



Citrix NetScaler 1000V Command Reference

Citrix NetScaler 10.1
October 3, 2013

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

 Citrix and other Citrix product names referenced herein are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. All other product names, company names, marks, logos, and symbols are trademarks of their respective owners.

© 2013 Cisco Systems, Inc. All rights reserved.

Contents

Command Reference	57
AAA Commands	57
aaa	57
stat aaa	57
aaa user	58
add aaa user	58
rm aaa user	58
set aaa user	59
bind aaa user	59
unbind aaa user	60
show aaa user	61
aaa group	61
add aaa group	61
rm aaa group	62
bind aaa group	62
unbind aaa group	63
show aaa group	64
aaa preauthenticationaction	64
add aaa preauthenticationaction	65
rm aaa preauthenticationaction	65
set aaa preauthenticationaction	66
unset aaa preauthenticationaction	66
show aaa preauthenticationaction	66
aaa preauthenticationpolicy	67
add aaa preauthenticationpolicy	67
rm aaa preauthenticationpolicy	67
set aaa preauthenticationpolicy	67
show aaa preauthenticationpolicy	68
aaa stats	68
show aaa stats	68
aaa session	68
show aaa session	69

Contents

kill aaa session.....	69
aaa radiusParams.....	70
set aaa radiusParams.....	70
unset aaa radiusParams.....	72
show aaa radiusParams.....	72
aaa ldapParams.....	73
set aaa ldapParams.....	73
unset aaa ldapParams.....	74
show aaa ldapParams.....	75
aaa tacacsParams.....	75
set aaa tacacsParams.....	75
unset aaa tacacsParams.....	76
show aaa tacacsParams.....	77
aaa certParams.....	77
set aaa certParams.....	77
unset aaa certParams.....	78
show aaa certParams.....	78
aaa parameter.....	78
set aaa parameter.....	78
unset aaa parameter.....	79
show aaa parameter.....	79
aaa preauthenticationparameter.....	80
set aaa preauthenticationparameter.....	80
unset aaa preauthenticationparameter.....	80
show aaa preauthenticationparameter.....	81
aaa global.....	81
bind aaa global.....	81
unbind aaa global.....	81
show aaa global.....	82
aaa kcdAccount.....	82
add aaa kcdAccount.....	82
rm aaa kcdAccount.....	83
set aaa kcdAccount.....	83
unset aaa kcdAccount.....	84
show aaa kcdAccount.....	84
Application Commands.....	85
import application.....	85
Synopsis.....	85
Description.....	85
Parameters.....	85

export application.....	86
Synopsis.....	86
Description.....	86
Parameters.....	86
rm application.....	86
Synopsis.....	86
Description.....	87
Parameters.....	87
AppFlow Commands.....	87
appflow.....	87
stat appflow.....	87
appflow collector.....	87
add appflow collector.....	88
rm appflow collector.....	88
rename appflow collector.....	89
show appflow collector.....	89
appflow action.....	90
add appflow action.....	90
rm appflow action.....	91
set appflow action.....	91
unset appflow action.....	92
rename appflow action.....	92
show appflow action.....	92
appflow policy.....	93
add appflow policy.....	93
rm appflow policy.....	94
set appflow policy.....	94
unset appflow policy.....	95
rename appflow policy.....	95
show appflow policy.....	96
appflow policylabel.....	96
add appflow policylabel.....	96
rm appflow policylabel.....	97
bind appflow policylabel.....	97
unbind appflow policylabel.....	98
rename appflow policylabel.....	98
show appflow policylabel.....	99
appflow param.....	99
set appflow param.....	99
unset appflow param.....	101

show appflow param.....	102
appflow global.....	102
bind appflow global.....	102
unbind appflow global.....	102
show appflow global.....	103
Application Firewall Commands.....	103
appfw.....	104
stat appfw.....	104
appfw fieldType.....	104
add appfw fieldType.....	105
rm appfw fieldType.....	105
set appfw fieldType.....	106
show appfw fieldType.....	106
appfw profile.....	106
add appfw profile.....	106
rm appfw profile.....	116
set appfw profile.....	117
unset appfw profile.....	126
bind appfw profile.....	127
unbind appfw profile.....	131
show appfw profile.....	133
stat appfw profile.....	133
archive appfw profile.....	133
restore appfw profile.....	134
appfw policy.....	134
add appfw policy.....	134
rm appfw policy.....	135
set appfw policy.....	135
unset appfw policy.....	136
show appfw policy.....	136
stat appfw policy.....	137
rename appfw policy.....	137
appfw policylabel.....	138
add appfw policylabel.....	138
rm appfw policylabel.....	138
bind appfw policylabel.....	139
unbind appfw policylabel.....	139
show appfw policylabel.....	140
stat appfw policylabel.....	141
rename appfw policylabel.....	141

appfw confidField.....	141
add appfw confidField.....	142
rm appfw confidField.....	142
set appfw confidField.....	143
unset appfw confidField.....	143
show appfw confidField.....	143
appfw stats.....	144
show appfw stats.....	144
appfw xmlerrorpage.....	144
rm appfw xmlerrorpage.....	144
show appfw xmlerrorpage.....	144
import appfw xmlerrorpage.....	145
update appfw xmlerrorpage.....	145
appfw htmlerrorpage.....	146
rm appfw htmlerrorpage.....	146
show appfw htmlerrorpage.....	146
import appfw htmlerrorpage.....	147
update appfw htmlerrorpage.....	147
appfw settings.....	148
set appfw settings.....	148
unset appfw settings.....	150
show appfw settings.....	150
appfw transactionRecords.....	150
show appfw transactionRecords.....	150
appfw global.....	150
bind appfw global.....	151
unbind appfw global.....	151
show appfw global.....	151
appfw learningsettings.....	152
set appfw learningsettings.....	152
unset appfw learningsettings.....	154
show appfw learningsettings.....	154
appfw learningdata.....	155
rm appfw learningdata.....	155
show appfw learningdata.....	156
reset appfw learningdata.....	156
export appfw learningdata.....	156
appfw JSONContentType.....	157
add appfw JSONContentType.....	157
rm appfw JSONContentType.....	157

show appfw JSONContentType.....	158
appfw wsdl.....	158
rm appfw wsdl.....	158
show appfw wsdl.....	158
import appfw wsdl.....	159
appfw signatures.....	159
rm appfw signatures.....	159
show appfw signatures.....	160
import appfw signatures.....	160
update appfw signatures.....	161
appfw xmlschema.....	161
rm appfw xmlschema.....	162
show appfw xmlschema.....	162
import appfw xmlschema.....	162
appfw XMLContentType.....	163
add appfw XMLContentType.....	163
rm appfw XMLContentType.....	163
show appfw XMLContentType.....	164
appfw archive.....	164
show appfw archive.....	164
export appfw archive.....	164
import appfw archive.....	165
rm appfw archive.....	165
APPQOE Commands.....	166
appqoe.....	166
stat appqoe.....	166
appqoe action.....	166
add appqoe action.....	166
rm appqoe action.....	168
set appqoe action.....	168
unset appqoe action.....	170
show appqoe action.....	170
appqoe policy.....	170
add appqoe policy.....	170
rm appqoe policy.....	171
set appqoe policy.....	171
show appqoe policy.....	171
stat appqoe policy.....	171
appqoe parameter.....	172
set appqoe parameter.....	172

unset appqoe parameter.....	173
show appqoe parameter.....	173
appqoe stats.....	173
show appqoe stats.....	173
Audit Commands.....	173
audit.....	174
stat audit.....	174
audit syslogAction.....	174
add audit syslogAction.....	174
rm audit syslogAction.....	176
set audit syslogAction.....	176
unset audit syslogAction.....	177
show audit syslogAction.....	177
audit syslogPolicy.....	178
add audit syslogPolicy.....	178
rm audit syslogPolicy.....	178
set audit syslogPolicy.....	179
show audit syslogPolicy.....	179
audit nslogAction.....	179
add audit nslogAction.....	180
rm audit nslogAction.....	181
set audit nslogAction.....	181
unset audit nslogAction.....	183
show audit nslogAction.....	183
audit nslogPolicy.....	183
add audit nslogPolicy.....	183
rm audit nslogPolicy.....	184
set audit nslogPolicy.....	184
show audit nslogPolicy.....	185
audit messageaction.....	185
add audit messageaction.....	185
rm audit messageaction.....	186
set audit messageaction.....	186
unset audit messageaction.....	187
show audit messageaction.....	187
audit stats.....	187
show audit stats.....	187
audit messages.....	187
show audit messages.....	188
audit syslogParams.....	188

set audit syslogParams.....	188
unset audit syslogParams.....	189
show audit syslogParams.....	190
audit nslogParams.....	190
set audit nslogParams.....	190
unset audit nslogParams.....	191
show audit nslogParams.....	191
Authentication Commands.....	192
authentication radiusAction.....	192
add authentication radiusAction.....	192
rm authentication radiusAction.....	194
set authentication radiusAction.....	194
unset authentication radiusAction.....	196
show authentication radiusAction.....	196
authentication ldapAction.....	197
add authentication ldapAction.....	197
rm authentication ldapAction.....	199
set authentication ldapAction.....	200
unset authentication ldapAction.....	202
show authentication ldapAction.....	202
authentication tacacsAction.....	202
add authentication tacacsAction.....	202
rm authentication tacacsAction.....	203
set authentication tacacsAction.....	204
unset authentication tacacsAction.....	205
show authentication tacacsAction.....	205
authentication negotiateAction.....	205
add authentication negotiateAction.....	205
rm authentication negotiateAction.....	206
set authentication negotiateAction.....	207
unset authentication negotiateAction.....	207
show authentication negotiateAction.....	207
authentication samlAction.....	208
add authentication samlAction.....	208
rm authentication samlAction.....	209
set authentication samlAction.....	209
unset authentication samlAction.....	210
show authentication samlAction.....	210
authentication certAction.....	210
add authentication certAction.....	211

rm authentication certAction.....	212
set authentication certAction.....	212
unset authentication certAction.....	213
show authentication certAction.....	213
authentication localPolicy.....	213
add authentication localPolicy.....	213
rm authentication localPolicy.....	214
set authentication localPolicy.....	214
unset authentication localPolicy.....	215
show authentication localPolicy.....	215
authentication radiusPolicy.....	215
add authentication radiusPolicy.....	215
rm authentication radiusPolicy.....	216
set authentication radiusPolicy.....	216
unset authentication radiusPolicy.....	216
show authentication radiusPolicy.....	217
authentication certPolicy.....	217
add authentication certPolicy.....	217
rm authentication certPolicy.....	218
set authentication certPolicy.....	218
unset authentication certPolicy.....	218
show authentication certPolicy.....	219
authentication ldapPolicy.....	219
add authentication ldapPolicy.....	219
rm authentication ldapPolicy.....	220
set authentication ldapPolicy.....	220
unset authentication ldapPolicy.....	220
show authentication ldapPolicy.....	220
authentication tacacsPolicy.....	221
add authentication tacacsPolicy.....	221
rm authentication tacacsPolicy.....	221
set authentication tacacsPolicy.....	222
unset authentication tacacsPolicy.....	222
show authentication tacacsPolicy.....	222
authentication negotiatePolicy.....	223
add authentication negotiatePolicy.....	223
rm authentication negotiatePolicy.....	223
set authentication negotiatePolicy.....	224
unset authentication negotiatePolicy.....	224
show authentication negotiatePolicy.....	224

authentication samlPolicy.....	225
add authentication samlPolicy.....	225
rm authentication samlPolicy.....	225
set authentication samlPolicy.....	226
unset authentication samlPolicy.....	226
show authentication samlPolicy.....	226
authentication vsrver.....	227
add authentication vsrver.....	227
rm authentication vsrver.....	228
set authentication vsrver.....	228
unset authentication vsrver.....	229
bind authentication vsrver.....	229
unbind authentication vsrver.....	230
enable authentication vsrver.....	230
disable authentication vsrver.....	231
show authentication vsrver.....	231
stat authentication vsrver.....	232
rename authentication vsrver.....	232
authentication authnProfile.....	233
add authentication authnProfile.....	233
rm authentication authnProfile.....	233
set authentication authnProfile.....	234
unset authentication authnProfile.....	234
show authentication authnProfile.....	234
Authorization Commands.....	235
authorization policy.....	235
add authorization policy.....	235
rm authorization policy.....	236
set authorization policy.....	236
rename authorization policy.....	236
show authorization policy.....	237
authorization policylabel.....	237
add authorization policylabel.....	237
rm authorization policylabel.....	238
bind authorization policylabel.....	238
unbind authorization policylabel.....	239
rename authorization policylabel.....	239
show authorization policylabel.....	240
stat authorization policylabel.....	240
authorization action.....	241

show authorization action.....	241
AUTOSCALE Commands.....	241
autoscale profile.....	241
add autoscale profile.....	241
rm autoscale profile.....	242
set autoscale profile.....	242
show autoscale profile.....	242
autoscale action.....	243
add autoscale action.....	243
rm autoscale action.....	243
set autoscale action.....	244
unset autoscale action.....	244
show autoscale action.....	244
autoscale policy.....	245
add autoscale policy.....	245
rm autoscale policy.....	245
set autoscale policy.....	246
unset autoscale policy.....	246
show autoscale policy.....	247
stat autoscale policy.....	247
rename autoscale policy.....	247
Basic Commands.....	248
location.....	249
add location.....	249
rm location.....	250
show location.....	250
locationFile.....	250
add locationFile.....	251
rm locationFile.....	251
show locationFile.....	251
server.....	252
add server.....	252
rm server.....	253
set server.....	254
unset server.....	254
enable server.....	255
disable server.....	255
show server.....	256
rename server.....	256
service.....	257

add service.....	257
rm service.....	261
set service.....	261
unset service.....	264
bind service.....	265
unbind service.....	265
enable service.....	266
disable service.....	266
show service.....	267
rename service.....	268
stat service.....	268
serviceGroup.....	269
add serviceGroup.....	269
rm serviceGroup.....	272
set serviceGroup.....	272
unset serviceGroup.....	275
bind serviceGroup.....	276
unbind serviceGroup.....	277
enable serviceGroup.....	277
disable serviceGroup.....	278
show serviceGroup.....	279
stat serviceGroup.....	279
rename serviceGroup.....	280
dbMonitors.....	280
restart dbMonitors.....	280
locationData.....	280
clear locationData.....	281
svcbindings.....	281
show svcbindings.....	281
servicegroupbindings.....	281
show servicegroupbindings.....	281
serviceGroupMember.....	281
stat serviceGroupMember.....	282
configstatus.....	282
show configstatus.....	282
locationParameter.....	282
set locationParameter.....	283
unset locationParameter.....	284
show locationParameter.....	284
vserver.....	284

show vserver.....	284
uiinternal.....	284
set uiinternal.....	285
unset uiinternal.....	285
show uiinternal.....	286
reporting.....	286
enable reporting.....	286
disable reporting.....	286
show reporting.....	287
nstrace.....	287
start nstrace.....	287
stop nstrace.....	289
show nstrace.....	290
Cache Commands.....	290
cache.....	290
stat cache.....	291
cache policy.....	291
add cache policy.....	291
rm cache policy.....	292
set cache policy.....	292
unset cache policy.....	293
show cache policy.....	294
stat cache policy.....	294
rename cache policy.....	295
cache policylabel.....	295
add cache policylabel.....	295
rm cache policylabel.....	296
bind cache policylabel.....	296
unbind cache policylabel.....	297
show cache policylabel.....	297
stat cache policylabel.....	298
rename cache policylabel.....	298
cache contentGroup.....	298
add cache contentGroup.....	299
rm cache contentGroup.....	302
set cache contentGroup.....	303
unset cache contentGroup.....	306
show cache contentGroup.....	306
expire cache contentGroup.....	307
flush cache contentGroup.....	307

save cache contentGroup.....	308
cache forwardProxy.....	308
add cache forwardProxy.....	308
rm cache forwardProxy.....	308
show cache forwardProxy.....	309
cache selector.....	309
add cache selector.....	309
rm cache selector.....	310
set cache selector.....	310
show cache selector.....	310
cache object.....	310
show cache object.....	311
expire cache object.....	312
flush cache object.....	312
save cache object.....	313
cache stats.....	313
show cache stats.....	313
cache global.....	313
bind cache global.....	314
unbind cache global.....	314
show cache global.....	314
cache parameter.....	315
set cache parameter.....	315
unset cache parameter.....	316
show cache parameter.....	316
CLI Commands.....	317
config.....	317
config.....	317
whoami.....	317
whoami.....	317
exit.....	318
exit.....	318
quit.....	318
quit.....	318
man.....	318
man.....	318
history.....	319
history.....	319
help.....	319
help.....	319

source.....	321
source.....	321
batch.....	321
batch.....	321
backup.....	322
backup.....	322
unalias.....	322
unalias.....	322
alias.....	323
alias.....	323
cls.....	323
cls.....	323
cli attribute.....	323
show cli attribute.....	324
cli prompt.....	324
clear cli prompt.....	324
set cli prompt.....	324
show cli prompt.....	325
cli mode.....	325
set cli mode.....	325
unset cli mode.....	326
show cli mode.....	326
Cluster Commands.....	326
cluster.....	327
join cluster.....	327
cluster instance.....	327
add cluster instance.....	327
rm cluster instance.....	328
set cluster instance.....	328
unset cluster instance.....	329
enable cluster instance.....	329
disable cluster instance.....	329
show cluster instance.....	330
stat cluster instance.....	331
cluster node.....	331
add cluster node.....	331
set cluster node.....	332
unset cluster node.....	333
rm cluster node.....	333
show cluster node.....	333

stat cluster node.....	334
cluster nodegroup.....	334
add cluster nodegroup.....	335
show cluster nodegroup.....	335
set cluster nodegroup.....	335
unset cluster nodegroup.....	336
bind cluster nodegroup.....	336
unbind cluster nodegroup.....	337
rm cluster nodegroup.....	338
cluster files.....	338
sync cluster files.....	338
cluster sync.....	339
force cluster sync.....	339
Compression Commands.....	339
cmp.....	339
stat cmp.....	340
cmp action.....	340
add cmp action.....	340
rm cmp action.....	341
show cmp action.....	341
rename cmp action.....	342
cmp policy.....	343
add cmp policy.....	343
rm cmp policy.....	344
set cmp policy.....	345
show cmp policy.....	346
stat cmp policy.....	347
rename cmp policy.....	347
cmp policylabel.....	348
add cmp policylabel.....	348
rm cmp policylabel.....	348
bind cmp policylabel.....	349
unbind cmp policylabel.....	349
show cmp policylabel.....	350
stat cmp policylabel.....	350
rename cmp policylabel.....	351
cmp stats.....	351
show cmp stats.....	351
cmp global.....	352
bind cmp global.....	352

unbind cmp global.....	353
show cmp global.....	353
cmp parameter.....	354
set cmp parameter.....	354
unset cmp parameter.....	356
show cmp parameter.....	356
CO Commands.....	356
co policy.....	356
unset co policy.....	356
co parameter.....	356
unset co parameter.....	357
Cache Redirection Commands.....	357
cr policy.....	357
add cr policy.....	357
rm cr policy.....	358
set cr policy.....	358
show cr policy.....	359
cr vserver.....	359
add cr vserver.....	359
rm cr vserver.....	363
set cr vserver.....	363
unset cr vserver.....	366
bind cr vserver.....	367
unbind cr vserver.....	367
enable cr vserver.....	368
disable cr vserver.....	368
show cr vserver.....	368
stat cr vserver.....	369
rename cr vserver.....	369
Content Switching Commands.....	370
cs policy.....	370
add cs policy.....	370
rm cs policy.....	372
set cs policy.....	372
unset cs policy.....	373
show cs policy.....	373
rename cs policy.....	373
cs policylabel.....	374
add cs policylabel.....	374
rm cs policylabel.....	375

bind cs policylabel.....	375
unbind cs policylabel.....	376
show cs policylabel.....	377
rename cs policylabel.....	377
cs vserver.....	378
add cs vserver.....	378
rm cs vserver.....	383
set cs vserver.....	384
unset cs vserver.....	389
bind cs vserver.....	389
unbind cs vserver.....	390
enable cs vserver.....	390
disable cs vserver.....	391
show cs vserver.....	391
stat cs vserver.....	392
rename cs vserver.....	392
cs parameter.....	393
set cs parameter.....	393
unset cs parameter.....	393
show cs parameter.....	393
cs action.....	394
add cs action.....	394
rm cs action.....	395
set cs action.....	395
unset cs action.....	396
show cs action.....	396
rename cs action.....	396
DB Commands.....	397
db user.....	397
add db user.....	397
rm db user.....	398
set db user.....	398
show db user.....	399
db dbProfile.....	399
add db dbProfile.....	399
rm db dbProfile.....	400
set db dbProfile.....	400
unset db dbProfile.....	401
show db dbProfile.....	401
DNS Commands.....	401

dns.....	402
stat dns.....	402
dns aaaaRec.....	403
add dns aaaaRec.....	403
rm dns aaaaRec.....	403
show dns aaaaRec.....	404
dns addRec.....	404
add dns addRec.....	404
rm dns addRec.....	405
show dns addRec.....	406
dns txtRec.....	406
add dns txtRec.....	406
rm dns txtRec.....	407
show dns txtRec.....	408
dns cnameRec.....	408
add dns cnameRec.....	408
rm dns cnameRec.....	409
show dns cnameRec.....	409
dns mxRec.....	410
add dns mxRec.....	410
rm dns mxRec.....	411
set dns mxRec.....	411
unset dns mxRec.....	412
show dns mxRec.....	412
dns nsRec.....	412
add dns nsRec.....	412
rm dns nsRec.....	413
show dns nsRec.....	413
dns ptrRec.....	414
add dns ptrRec.....	414
rm dns ptrRec.....	414
show dns ptrRec.....	415
dns srvRec.....	415
add dns srvRec.....	415
rm dns srvRec.....	416
set dns srvRec.....	417
unset dns srvRec.....	417
show dns srvRec.....	418
dns soaRec.....	418
add dns soaRec.....	418

rm dns soaRec.....	419
set dns soaRec.....	420
unset dns soaRec.....	421
show dns soaRec.....	421
dns suffix.....	421
add dns suffix.....	421
rm dns suffix.....	422
show dns suffix.....	422
dns nameServer.....	422
add dns nameServer.....	423
rm dns nameServer.....	424
enable dns nameServer.....	424
disable dns nameServer.....	425
show dns nameServer.....	425
dns view.....	425
add dns view.....	426
rm dns view.....	426
show dns view.....	426
dns policy.....	427
add dns policy.....	427
rm dns policy.....	428
set dns policy.....	428
show dns policy.....	429
dns action64.....	430
add dns action64.....	430
rm dns action64.....	431
set dns action64.....	431
unset dns action64.....	432
show dns action64.....	432
dns policy64.....	432
add dns policy64.....	432
rm dns policy64.....	433
set dns policy64.....	433
show dns policy64.....	434
dns zone.....	434
add dns zone.....	435
set dns zone.....	435
unset dns zone.....	436
rm dns zone.....	436
sign dns zone.....	436

unsign dns zone.....	437
show dns zone.....	437
dns key.....	438
add dns key.....	438
create dns key.....	439
set dns key.....	440
unset dns key.....	441
rm dns key.....	441
show dns key.....	441
dns proxyRecords.....	442
flush dns proxyRecords.....	442
dns records.....	442
stat dns records.....	442
dns stats.....	442
show dns stats.....	443
dns parameter.....	443
set dns parameter.....	443
unset dns parameter.....	445
show dns parameter.....	445
dns policylabel.....	445
add dns policylabel.....	445
rm dns policylabel.....	446
bind dns policylabel.....	446
unbind dns policylabel.....	447
show dns policylabel.....	447
stat dns policylabel.....	448
rename dns policylabel.....	448
dns global.....	449
bind dns global.....	449
unbind dns global.....	449
show dns global.....	449
dns action.....	450
add dns action.....	450
rm dns action.....	451
set dns action.....	451
unset dns action.....	452
show dns action.....	453
dns nsecRec.....	453
show dns nsecRec.....	453
DOS Commands.....	454

dos.....	454
stat dos.....	454
dos policy.....	454
add dos policy.....	454
rm dos policy.....	455
set dos policy.....	455
unset dos policy.....	456
show dos policy.....	456
stat dos policy.....	457
dos stats.....	457
show dos stats.....	457
Filter Commands.....	457
filter action.....	457
add filter action.....	458
rm filter action.....	459
set filter action.....	459
unset filter action.....	460
show filter action.....	460
filter htmlinjectionvariable.....	461
add filter htmlinjectionvariable.....	461
rm filter htmlinjectionvariable.....	462
set filter htmlinjectionvariable.....	462
unset filter htmlinjectionvariable.....	462
show filter htmlinjectionvariable.....	463
filter policy.....	463
add filter policy.....	463
rm filter policy.....	465
set filter policy.....	465
show filter policy.....	466
filter prebodyInjection.....	467
set filter prebodyInjection.....	467
unset filter prebodyInjection.....	468
show filter prebodyInjection.....	468
filter postbodyInjection.....	468
set filter postbodyInjection.....	468
unset filter postbodyInjection.....	469
show filter postbodyInjection.....	469
filter htmlinjectionparameter.....	469
set filter htmlinjectionparameter.....	469
unset filter htmlinjectionparameter.....	470

show filter htmlinjectionparameter.....	470
filter global.....	471
bind filter global.....	471
unbind filter global.....	471
show filter global.....	472
GSLB Commands.....	472
gslb site.....	473
add gslb site.....	473
rm gslb site.....	474
set gslb site.....	475
unset gslb site.....	476
show gslb site.....	476
stat gslb site.....	476
gslb service.....	477
add gslb service.....	477
rm gslb service.....	480
set gslb service.....	480
unset gslb service.....	482
bind gslb service.....	482
unbind gslb service.....	483
show gslb service.....	483
stat gslb service.....	484
rename gslb service.....	484
gslb vserver.....	485
add gslb vserver.....	485
rm gslb vserver.....	488
set gslb vserver.....	489
unset gslb vserver.....	492
bind gslb vserver.....	493
unbind gslb vserver.....	493
enable gslb vserver.....	494
disable gslb vserver.....	494
show gslb vserver.....	495
stat gslb vserver.....	495
rename gslb vserver.....	496
gslb runningConfig.....	496
show gslb runningConfig.....	496
gslb domain.....	496
stat gslb domain.....	497
gslb Idnsentries.....	497

clear gslb ldnentries.....	497
show gslb ldnentries.....	497
gslb parameter.....	498
set gslb parameter.....	498
unset gslb parameter.....	499
show gslb parameter.....	499
gslb ldnentry.....	499
rm gslb ldnentry.....	499
gslb config.....	500
sync gslb config.....	500
gslb syncStatus.....	501
show gslb syncStatus.....	501
HA Commands.....	501
HA node.....	501
add HA node.....	501
rm HA node.....	502
set HA node.....	502
unset HA node.....	504
bind HA node.....	504
unbind HA node.....	504
show HA node.....	505
stat HA node.....	505
HA sync.....	506
force HA sync.....	506
HA files.....	506
sync HA files.....	506
HA failover.....	507
force HA failover.....	507
IPSec Commands.....	507
ipsec profile.....	508
add ipsec profile.....	508
show ipsec profile.....	509
rm ipsec profile.....	509
ipsec parameter.....	509
set ipsec parameter.....	509
unset ipsec parameter.....	510
show ipsec parameter.....	510
ipsec counters.....	511
stat ipsec counters.....	511
LB Commands.....	511

lb monitor.....	512
add lb monitor.....	512
rm lb monitor.....	520
set lb monitor.....	521
unset lb monitor.....	530
enable lb monitor.....	530
disable lb monitor.....	531
bind lb monitor.....	532
unbind lb monitor.....	532
show lb monitor.....	533
lb route.....	534
add lb route.....	534
rm lb route.....	534
show lb route.....	535
lb route6.....	535
add lb route6.....	535
rm lb route6.....	535
show lb route6.....	536
lb vsrver.....	536
add lb vsrver.....	536
rm lb vsrver.....	546
set lb vsrver.....	546
unset lb vsrver.....	556
bind lb vsrver.....	556
unbind lb vsrver.....	557
enable lb vsrver.....	558
disable lb vsrver.....	558
show lb vsrver.....	559
stat lb vsrver.....	559
rename lb vsrver.....	560
lb metricTable.....	560
add lb metricTable.....	560
rm lb metricTable.....	561
set lb metricTable.....	561
bind lb metricTable.....	561
unbind lb metricTable.....	562
show lb metricTable.....	562
lb monbindings.....	563
show lb monbindings.....	563
lb persistentSessions.....	563

show lb persistentSessions.....	563
clear lb persistentSessions.....	564
lb group.....	564
set lb group.....	564
unset lb group.....	566
bind lb group.....	566
unbind lb group.....	567
show lb group.....	567
rename lb group.....	568
lb sipParameters.....	568
set lb sipParameters.....	568
unset lb sipParameters.....	569
show lb sipParameters.....	569
lb parameter.....	570
set lb parameter.....	570
unset lb parameter.....	571
show lb parameter.....	572
Networking Commands.....	572
arp.....	574
add arp.....	574
rm arp.....	574
send arp.....	575
show arp.....	575
channel.....	576
add channel.....	576
rm channel.....	578
set channel.....	578
unset channel.....	580
bind channel.....	580
unbind channel.....	581
show channel.....	581
fis.....	582
add fis.....	582
rm fis.....	582
bind fis.....	582
unbind fis.....	583
show fis.....	583
route.....	583
add route.....	584
clear route.....	585

rm route.....	585
set route.....	586
unset route.....	587
show route.....	587
vlan.....	588
add vlan.....	588
rm vlan.....	588
set vlan.....	589
unset vlan.....	589
bind vlan.....	590
unbind vlan.....	590
show vlan.....	591
stat vlan.....	591
vrID.....	592
add vrID.....	592
rm vrID.....	593
set vrID.....	593
unset vrID.....	594
bind vrID.....	595
unbind vrID.....	595
show vrID.....	596
vrID6.....	596
add vrID6.....	596
rm vrID6.....	597
bind vrID6.....	597
unbind vrID6.....	598
show vrID6.....	598
route6.....	598
add route6.....	599
clear route6.....	600
rm route6.....	600
set route6.....	601
unset route6.....	602
show route6.....	602
nd6.....	603
add nd6.....	603
clear nd6.....	603
rm nd6.....	604
show nd6.....	604
inat.....	605

add inat.....	605
rm inat.....	606
set inat.....	606
unset inat.....	607
stat inat.....	608
show inat.....	608
inatsession.....	609
stat inatsession.....	609
bridgegroup.....	609
add bridgegroup.....	609
rm bridgegroup.....	610
set bridgegroup.....	610
unset bridgegroup.....	611
bind bridgegroup.....	611
unbind bridgegroup.....	611
show bridgegroup.....	612
ipTunnel.....	612
add ipTunnel.....	612
rm ipTunnel.....	613
show ipTunnel.....	614
ip6Tunnel.....	615
add ip6Tunnel.....	615
rm ip6Tunnel.....	615
show ip6Tunnel.....	616
netbridge.....	617
add netbridge.....	617
rm netbridge.....	617
show netbridge.....	617
bind netbridge.....	618
unbind netbridge.....	618
ipset.....	619
add ipset.....	619
rm ipset.....	619
bind ipset.....	620
unbind ipset.....	620
show ipset.....	621
linkset.....	621
add linkset.....	621
rm linkset.....	622
bind linkset.....	622

unbind linkset.....	623
show linkset.....	623
netProfile.....	623
add netProfile.....	624
rm netProfile.....	624
set netProfile.....	625
unset netProfile.....	625
show netProfile.....	625
arpparam.....	626
set arpparam.....	626
unset arpparam.....	626
show arpparam.....	627
ci.....	627
show ci.....	627
interface.....	627
clear interface.....	627
set interface.....	628
unset interface.....	630
enable interface.....	631
disable interface.....	631
reset interface.....	631
show interface.....	632
stat interface.....	634
rnat.....	634
clear rnat.....	634
set rnat.....	635
unset rnat.....	635
stat rnat.....	635
show rnat.....	636
bridgetable.....	636
set bridgetable.....	636
unset bridgetable.....	637
show bridgetable.....	637
clear bridgetable.....	637
bridge.....	637
stat bridge.....	638
lacp.....	638
set lacp.....	638
show lacp.....	638
rnatparam.....	639

set rnatparam.....	639
unset rnatparam.....	639
show rnatparam.....	639
rnatip.....	640
stat rnatip.....	640
vrIDParam.....	640
set vrIDParam.....	640
unset vrIDParam.....	641
show vrIDParam.....	641
nd6RAvariables.....	641
set nd6RAvariables.....	641
unset nd6RAvariables.....	643
show nd6RAvariables.....	643
bind nd6RAvariables.....	643
unbind nd6RAvariables.....	644
onLinkIPv6Prefix.....	644
add onLinkIPv6Prefix.....	644
rm onLinkIPv6Prefix.....	645
set onLinkIPv6Prefix.....	645
unset onLinkIPv6Prefix.....	646
show onLinkIPv6Prefix.....	646
ipv6.....	647
set ipv6.....	647
unset ipv6.....	648
show ipv6.....	648
ipTunnelParam.....	648
set ipTunnelParam.....	648
unset ipTunnelParam.....	649
show ipTunnelParam.....	649
ip6TunnelParam.....	650
set ip6TunnelParam.....	650
unset ip6TunnelParam.....	651
show ip6TunnelParam.....	651
L2Param.....	651
set L2Param.....	651
unset L2Param.....	653
show L2Param.....	653
L3Param.....	653
set L3Param.....	653
unset L3Param.....	654

show L3Param.....	654
forwardingSession.....	655
add forwardingSession.....	655
set forwardingSession.....	656
rm forwardingSession.....	656
show forwardingSession.....	656
ptp.....	657
set ptp.....	657
show ptp.....	657
rnat6.....	657
add rnat6.....	657
bind rnat6.....	658
unbind rnat6.....	659
set rnat6.....	659
unset rnat6.....	659
clear rnat6.....	660
show rnat6.....	660
inatparam.....	660
set inatparam.....	660
unset inatparam.....	661
show inatparam.....	661
nat64.....	662
add nat64.....	662
set nat64.....	662
unset nat64.....	663
rm nat64.....	663
stat nat64.....	663
show nat64.....	664
rsskeytype.....	664
set rsskeytype.....	664
show rsskeytype.....	664
tunnelip.....	664
stat tunnelip.....	665
tunnelip6.....	665
stat tunnelip6.....	665
L4Param.....	665
set L4Param.....	666
unset L4Param.....	666
show L4Param.....	666
vpath.....	666

add vpath.....	666
rm vpath.....	667
show vpath.....	667
stat vpath.....	668
vPathParam.....	668
set vPathParam.....	668
unset vPathParam.....	669
show vPathParam.....	669
NS Commands.....	669
shutdown.....	671
shutdown.....	671
reboot.....	671
reboot.....	671
ns.....	672
config ns.....	672
stat ns.....	672
ns limitIdentifier.....	672
add ns limitIdentifier.....	672
rm ns limitIdentifier.....	674
set ns limitIdentifier.....	674
unset ns limitIdentifier.....	675
show ns limitIdentifier.....	676
stat ns limitIdentifier.....	676
ns acl.....	677
add ns acl.....	677
rm ns acl.....	679
set ns acl.....	680
unset ns acl.....	681
enable ns acl.....	682
disable ns acl.....	682
stat ns acl.....	683
rename ns acl.....	683
show ns acl.....	684
ns acl6.....	684
add ns acl6.....	685
rm ns acl6.....	687
set ns acl6.....	687
unset ns acl6.....	689
enable ns acl6.....	689
disable ns acl6.....	690

stat ns acl6.....	690
rename ns acl6.....	691
show ns acl6.....	691
ns ip6.....	692
add ns ip6.....	692
rm ns ip6.....	694
set ns ip6.....	695
unset ns ip6.....	696
show ns ip6.....	697
ns ip.....	697
add ns ip.....	697
rm ns ip.....	700
set ns ip.....	701
unset ns ip.....	703
enable ns ip.....	703
disable ns ip.....	704
show ns ip.....	704
ns simpleacl.....	705
add ns simpleacl.....	705
clear ns simpleacl.....	706
rm ns simpleacl.....	706
flush ns simpleacl.....	707
show ns simpleacl.....	707
stat ns simpleacl.....	707
ns simpleacl6.....	708
add ns simpleacl6.....	708
clear ns simpleacl6.....	709
flush ns simpleacl6.....	709
rm ns simpleacl6.....	710
show ns simpleacl6.....	710
stat ns simpleacl6.....	711
ns pbr.....	711
add ns pbr.....	711
rm ns pbr.....	713
set ns pbr.....	714
unset ns pbr.....	716
enable ns pbr.....	716
disable ns pbr.....	716
stat ns pbr.....	717
show ns pbr.....	717

ns xmlns:namespace.....	718
add ns xmlns:namespace.....	718
rm ns xmlns:namespace.....	719
set ns xmlns:namespace.....	719
unset ns xmlns:namespace.....	720
show ns xmlns:namespace.....	720
ns tcpProfile.....	720
add ns tcpProfile.....	720
rm ns tcpProfile.....	723
set ns tcpProfile.....	723
unset ns tcpProfile.....	726
show ns tcpProfile.....	726
ns httpProfile.....	727
add ns httpProfile.....	727
rm ns httpProfile.....	729
set ns httpProfile.....	729
unset ns httpProfile.....	731
show ns httpProfile.....	732
ns stats.....	732
show ns stats.....	732
clear ns stats.....	732
ns ns.conf.....	733
show ns ns.conf.....	733
ns savedConfig.....	733
show ns savedConfig.....	733
ns runningConfig.....	733
show ns runningConfig.....	733
ns acls.....	733
renumber ns acls.....	733
clear ns acls.....	734
apply ns acls.....	734
ns info.....	735
show ns info.....	735
ns license.....	736
show ns license.....	736
ns version.....	736
show ns version.....	736
ns config.....	736
clear ns config.....	736
set ns config.....	737

unset ns config.....	742
save ns config.....	742
show ns config.....	742
diff ns config.....	743
ns param.....	743
set ns param.....	743
unset ns param.....	749
show ns param.....	749
ns acls6.....	749
clear ns acls6.....	750
apply ns acls6.....	750
renumber ns acls6.....	750
ns pbrs.....	751
renumber ns pbrs.....	751
clear ns pbrs.....	751
apply ns pbrs.....	752
ns connectiontable.....	752
show ns connectiontable.....	752
ns limitSessions.....	753
show ns limitSessions.....	753
clear ns limitSessions.....	753
ns hostName.....	753
set ns hostName.....	754
show ns hostName.....	754
ns surgeQ.....	754
flush ns surgeQ.....	754
ns feature.....	755
enable ns feature.....	755
disable ns feature.....	756
show ns feature.....	756
ns mode.....	756
enable ns mode.....	756
disable ns mode.....	757
show ns mode.....	757
ns dhcpParams.....	757
set ns dhcpParams.....	757
unset ns dhcpParams.....	758
show ns dhcpParams.....	758
ns dhcpIp.....	758
release ns dhcpIp.....	758

ns spParams.....	758
set ns spParams.....	759
unset ns spParams.....	759
show ns spParams.....	759
ns tcpbufParam.....	760
set ns tcpbufParam.....	760
unset ns tcpbufParam.....	760
show ns tcpbufParam.....	760
ns tcpParam.....	761
set ns tcpParam.....	761
unset ns tcpParam.....	765
show ns tcpParam.....	765
ns httpParam.....	766
set ns httpParam.....	766
unset ns httpParam.....	767
show ns httpParam.....	767
ns weblogparam.....	767
set ns weblogparam.....	767
unset ns weblogparam.....	768
show ns weblogparam.....	768
ns diameter.....	768
set ns diameter.....	768
unset ns diameter.....	769
show ns diameter.....	769
ns rateControl.....	769
set ns rateControl.....	769
unset ns rateControl.....	770
show ns rateControl.....	770
ns rpcNode.....	771
set ns rpcNode.....	771
unset ns rpcNode.....	772
show ns rpcNode.....	772
ns timeout.....	773
set ns timeout.....	773
unset ns timeout.....	774
show ns timeout.....	775
ns hardware.....	775
show ns hardware.....	775
ns events.....	775
show ns events.....	775

ns encryptionParams.....	776
set ns encryptionParams.....	776
show ns encryptionParams.....	776
ns rollbackcmd.....	776
show ns rollbackcmd.....	777
ns memory.....	777
stat ns memory.....	777
ns pbr6.....	777
add ns pbr6.....	778
renumber ns pbr6.....	780
rm ns pbr6.....	780
set ns pbr6.....	781
unset ns pbr6.....	782
enable ns pbr6.....	783
disable ns pbr6.....	783
stat ns pbr6.....	784
show ns pbr6.....	784
clear ns pbr6.....	785
apply ns pbr6.....	785
ns trafficDomain.....	785
add ns trafficDomain.....	786
rm ns trafficDomain.....	786
clear ns trafficDomain.....	786
bind ns trafficDomain.....	787
unbind ns trafficDomain.....	787
enable ns trafficDomain.....	788
disable ns trafficDomain.....	788
show ns trafficDomain.....	789
stat ns trafficDomain.....	789
ns consoleloginprompt.....	790
set ns consoleloginprompt.....	790
unset ns consoleloginprompt.....	790
show ns consoleloginprompt.....	790
ns timer.....	791
add ns timer.....	791
rm ns timer.....	791
set ns timer.....	792
unset ns timer.....	792
bind ns timer.....	793
unbind ns timer.....	793

show ns timer.....	794
rename ns timer.....	794
ns aptlicense.....	794
show ns aptlicense.....	795
update ns aptlicense.....	795
NTP Commands.....	795
ntp server.....	796
add ntp server.....	796
rm ntp server.....	797
set ntp server.....	797
unset ntp server.....	798
show ntp server.....	798
ntp sync.....	798
enable ntp sync.....	798
disable ntp sync.....	799
show ntp sync.....	799
ntp status.....	799
show ntp status.....	799
ntp param.....	799
set ntp param.....	799
unset ntp param.....	800
show ntp param.....	800
Policy Commands.....	800
policy expression.....	801
add policy expression.....	801
rm policy expression.....	801
set policy expression.....	802
unset policy expression.....	802
show policy expression.....	803
policy map.....	803
add policy map.....	803
rm policy map.....	804
show policy map.....	805
policy patset.....	805
add policy patset.....	805
rm policy patset.....	806
bind policy patset.....	806
unbind policy patset.....	807
show policy patset.....	807
policy dataset.....	808

add policy dataset.....	808
rm policy dataset.....	808
bind policy dataset.....	809
unbind policy dataset.....	809
show policy dataset.....	809
policy httpCallout.....	810
add policy httpCallout.....	810
rm policy httpCallout.....	811
set policy httpCallout.....	811
unset policy httpCallout.....	813
show policy httpCallout.....	814
policy stringmap.....	814
add policy stringmap.....	814
rm policy stringmap.....	815
set policy stringmap.....	815
unset policy stringmap.....	816
bind policy stringmap.....	816
unbind policy stringmap.....	817
show policy stringmap.....	817
PQ Commands.....	818
pq.....	818
stat pq.....	818
pq policy.....	818
add pq policy.....	818
rm pq policy.....	819
set pq policy.....	820
unset pq policy.....	821
show pq policy.....	821
stat pq policy.....	821
pq stats.....	821
show pq stats.....	822
Protocol Commands.....	822
protocol tcp.....	822
stat protocol tcp.....	822
protocol http.....	822
stat protocol http.....	822
protocol icmp.....	823
stat protocol icmp.....	823
protocol ipv6.....	823
stat protocol ipv6.....	823

protocol icmpv6.....	823
stat protocol icmpv6.....	823
protocol ip.....	824
stat protocol ip.....	824
protocol udp.....	824
stat protocol udp.....	824
protocol httpBand.....	824
set protocol httpBand.....	824
unset protocol httpBand.....	825
show protocol httpBand.....	825
QOS Commands.....	826
qos.....	826
stat qos.....	826
qos stats.....	826
show qos stats.....	826
Responder Commands.....	826
responder policy.....	827
add responder policy.....	827
rm responder policy.....	828
set responder policy.....	828
unset responder policy.....	829
show responder policy.....	829
rename responder policy.....	830
stat responder policy.....	830
responder action.....	831
add responder action.....	831
rm responder action.....	832
set responder action.....	833
unset responder action.....	834
show responder action.....	834
rename responder action.....	834
responder policylabel.....	835
add responder policylabel.....	835
rm responder policylabel.....	836
bind responder policylabel.....	836
unbind responder policylabel.....	836
show responder policylabel.....	837
stat responder policylabel.....	838
rename responder policylabel.....	838
responder global.....	838

bind responder global.....	839
unbind responder global.....	839
show responder global.....	840
responder param.....	840
set responder param.....	840
unset responder param.....	841
show responder param.....	841
responder htmlpage.....	842
import responder htmlpage.....	842
rm responder htmlpage.....	842
update responder htmlpage.....	843
show responder htmlpage.....	843
Rewrite Commands.....	844
rewrite policy.....	844
add rewrite policy.....	844
rm rewrite policy.....	845
set rewrite policy.....	846
unset rewrite policy.....	847
show rewrite policy.....	847
stat rewrite policy.....	847
rename rewrite policy.....	848
rewrite action.....	849
add rewrite action.....	849
rm rewrite action.....	852
set rewrite action.....	852
unset rewrite action.....	854
show rewrite action.....	854
rename rewrite action.....	854
rewrite policylabel.....	855
add rewrite policylabel.....	855
rm rewrite policylabel.....	856
bind rewrite policylabel.....	856
unbind rewrite policylabel.....	857
show rewrite policylabel.....	857
stat rewrite policylabel.....	858
rename rewrite policylabel.....	858
rewrite global.....	859
bind rewrite global.....	859
unbind rewrite global.....	859
show rewrite global.....	860

rewrite param.....	860
set rewrite param.....	860
unset rewrite param.....	861
show rewrite param.....	861
Router Commands.....	862
vtysh.....	862
Synopsis.....	862
Description.....	862
SC Commands.....	862
sc.....	862
stat sc.....	862
sc policy.....	862
add sc policy.....	863
rm sc policy.....	864
set sc policy.....	864
unset sc policy.....	865
show sc policy.....	866
stat sc policy.....	866
sc stats.....	867
show sc stats.....	867
sc parameter.....	867
set sc parameter.....	867
unset sc parameter.....	868
show sc parameter.....	868
SNMP Commands.....	868
snmp.....	869
stat snmp.....	869
snmp community.....	869
add snmp community.....	869
rm snmp community.....	870
show snmp community.....	870
snmp manager.....	871
add snmp manager.....	871
rm snmp manager.....	872
set snmp manager.....	872
unset snmp manager.....	873
show snmp manager.....	873
snmp trap.....	874
add snmp trap.....	874
rm snmp trap.....	875

set snmp trap.....	875
unset snmp trap.....	877
show snmp trap.....	877
snmp group.....	877
add snmp group.....	877
rm snmp group.....	878
set snmp group.....	879
show snmp group.....	879
snmp view.....	880
add snmp view.....	880
rm snmp view.....	880
set snmp view.....	881
show snmp view.....	881
snmp user.....	882
add snmp user.....	882
rm snmp user.....	883
set snmp user.....	883
unset snmp user.....	884
show snmp user.....	884
snmp oid.....	884
show snmp oid.....	884
snmp stats.....	885
show snmp stats.....	885
snmp alarm.....	885
set snmp alarm.....	885
unset snmp alarm.....	888
enable snmp alarm.....	888
disable snmp alarm.....	889
show snmp alarm.....	890
snmp mib.....	891
set snmp mib.....	891
unset snmp mib.....	892
show snmp mib.....	892
snmp engineId.....	892
set snmp engineId.....	893
unset snmp engineId.....	893
show snmp engineId.....	893
snmp option.....	894
set snmp option.....	894
unset snmp option.....	894

show snmp option.....	894
SPILLOVER Commands.....	895
spillover policy.....	895
add spillover policy.....	895
rm spillover policy.....	895
set spillover policy.....	896
unset spillover policy.....	896
show spillover policy.....	897
rename spillover policy.....	897
stat spillover policy.....	897
spillover action.....	898
add spillover action.....	898
rm spillover action.....	898
show spillover action.....	899
rename spillover action.....	899
SSL Commands.....	899
ssl.....	900
stat ssl.....	900
ssl fipsKey.....	901
create ssl fipsKey.....	901
rm ssl fipsKey.....	901
show ssl fipsKey.....	902
import ssl fipsKey.....	903
export ssl fipsKey.....	904
ssl wrapkey.....	904
create ssl wrapkey.....	904
rm ssl wrapkey.....	905
show ssl wrapkey.....	905
ssl certKey.....	906
add ssl certKey.....	906
rm ssl certKey.....	907
set ssl certKey.....	908
unset ssl certKey.....	908
bind ssl certKey.....	908
unbind ssl certKey.....	909
link ssl certKey.....	910
unlink ssl certKey.....	911
show ssl certKey.....	911
update ssl certKey.....	912
ssl ciphersuite.....	913

show ssl ciphersuite.....	913
ssl cipher.....	914
add ssl cipher.....	914
bind ssl cipher.....	915
show ssl cipher.....	917
rm ssl cipher.....	918
unbind ssl cipher.....	918
ssl crt.....	919
add ssl crt.....	919
create ssl crt.....	921
rm ssl crt.....	922
set ssl crt.....	922
unset ssl crt.....	924
show ssl crt.....	924
ssl action.....	925
add ssl action.....	925
rm ssl action.....	927
show ssl action.....	927
ssl policy.....	928
add ssl policy.....	928
rm ssl policy.....	929
set ssl policy.....	930
unset ssl policy.....	931
show ssl policy.....	931
ssl policylabel.....	931
add ssl policylabel.....	932
rm ssl policylabel.....	932
bind ssl policylabel.....	933
unbind ssl policylabel.....	933
show ssl policylabel.....	934
ssl ocspResponder.....	934
add ssl ocspResponder.....	934
rm ssl ocspResponder.....	936
set ssl ocspResponder.....	936
unset ssl ocspResponder.....	938
show ssl ocspResponder.....	938
ssl rsakey.....	938
create ssl rsakey.....	938
ssl pkcs12.....	939
convert ssl pkcs12.....	939

ssl pkcs8.....	940
convert ssl pkcs8.....	940
ssl dhParam.....	941
create ssl dhParam.....	941
ssl dsaKey.....	942
create ssl dsaKey.....	942
ssl certLink.....	942
show ssl certLink.....	943
ssl certReq.....	943
create ssl certReq.....	943
ssl cert.....	945
create ssl cert.....	945
ssl stats.....	946
show ssl stats.....	947
ssl parameter.....	947
set ssl parameter.....	947
unset ssl parameter.....	949
show ssl parameter.....	949
ssl fips.....	949
set ssl fips.....	949
unset ssl fips.....	950
reset ssl fips.....	950
show ssl fips.....	951
update ssl fips.....	951
ssl service.....	951
set ssl service.....	952
unset ssl service.....	955
bind ssl service.....	955
unbind ssl service.....	956
show ssl service.....	956
ssl serviceGroup.....	957
set ssl serviceGroup.....	957
unset ssl serviceGroup.....	958
bind ssl serviceGroup.....	958
unbind ssl serviceGroup.....	959
show ssl serviceGroup.....	960
ssl vservice.....	960
set ssl vservice.....	960
unset ssl vservice.....	963
bind ssl vservice.....	963

unbind ssl vserver.....	964
show ssl vserver.....	965
ssl fipsSIMTarget.....	966
enable ssl fipsSIMTarget.....	966
init ssl fipsSIMTarget.....	967
ssl fipsSIMSource.....	967
enable ssl fipsSIMSource.....	967
init ssl fipsSIMSource.....	968
ssl global.....	968
bind ssl global.....	968
unbind ssl global.....	969
show ssl global.....	969
ssl dtlsProfile.....	970
add ssl dtlsProfile.....	970
rm ssl dtlsProfile.....	971
set ssl dtlsProfile.....	971
unset ssl dtlsProfile.....	972
show ssl dtlsProfile.....	972
Stream Commands.....	973
stream selector.....	973
add stream selector.....	973
set stream selector.....	974
rm stream selector.....	974
show stream selector.....	975
stream identifier.....	975
add stream identifier.....	975
set stream identifier.....	976
unset stream identifier.....	977
rm stream identifier.....	977
show stream identifier.....	978
stat stream identifier.....	978
stream session.....	979
clear stream session.....	979
System Commands.....	979
system.....	980
stat system.....	980
system cmdPolicy.....	981
add system cmdPolicy.....	981
rm system cmdPolicy.....	981
set system cmdPolicy.....	981

show system cmdPolicy.....	982
system user.....	982
add system user.....	982
rm system user.....	983
set system user.....	983
unset system user.....	984
bind system user.....	984
unbind system user.....	985
show system user.....	985
system group.....	985
add system group.....	985
rm system group.....	986
bind system group.....	986
unbind system group.....	987
show system group.....	987
set system group.....	987
unset system group.....	988
system session.....	988
show system session.....	988
kill system session.....	988
system cpu.....	989
stat system cpu.....	989
system memory.....	989
stat system memory.....	989
system entitydata.....	990
rm system entitydata.....	990
show system entitydata.....	990
system entity.....	991
show system entity.....	991
system globaldata.....	992
show system globaldata.....	992
system counters.....	993
show system counters.....	993
system countergroup.....	993
show system countergroup.....	993
system entitytype.....	993
show system entitytype.....	993
system eventhistory.....	994
show system eventhistory.....	994
system core.....	994

show system core.....	994
system dataSource.....	994
show system dataSource.....	994
system global.....	995
bind system global.....	995
unbind system global.....	995
show system global.....	995
system collectionparam.....	995
set system collectionparam.....	996
unset system collectionparam.....	996
show system collectionparam.....	996
system parameter.....	996
set system parameter.....	996
unset system parameter.....	997
show system parameter.....	997
system backup.....	998
create system backup.....	998
restore system backup.....	998
rm system backup.....	998
show system backup.....	999
TM Commands.....	999
tm sessionPolicy.....	999
add tm sessionPolicy.....	999
rm tm sessionPolicy.....	1000
set tm sessionPolicy.....	1000
unset tm sessionPolicy.....	1001
show tm sessionPolicy.....	1001
tm sessionAction.....	1002
add tm sessionAction.....	1002
rm tm sessionAction.....	1003
set tm sessionAction.....	1003
unset tm sessionAction.....	1004
show tm sessionAction.....	1005
tm trafficPolicy.....	1005
add tm trafficPolicy.....	1005
rm tm trafficPolicy.....	1006
set tm trafficPolicy.....	1006
unset tm trafficPolicy.....	1006
show tm trafficPolicy.....	1007
stat tm trafficPolicy.....	1007

tm formSSOAction.....	1007
add tm formSSOAction.....	1008
rm tm formSSOAction.....	1009
set tm formSSOAction.....	1009
unset tm formSSOAction.....	1010
show tm formSSOAction.....	1010
tm samlSSOProfile.....	1010
add tm samlSSOProfile.....	1011
rm tm samlSSOProfile.....	1011
set tm samlSSOProfile.....	1012
unset tm samlSSOProfile.....	1012
show tm samlSSOProfile.....	1013
tm trafficAction.....	1013
add tm trafficAction.....	1013
rm tm trafficAction.....	1014
set tm trafficAction.....	1014
unset tm trafficAction.....	1015
show tm trafficAction.....	1015
tm global.....	1016
bind tm global.....	1016
unbind tm global.....	1016
show tm global.....	1016
tm sessionParameter.....	1016
set tm sessionParameter.....	1017
unset tm sessionParameter.....	1018
show tm sessionParameter.....	1018
Transform Commands.....	1018
transform profile.....	1018
add transform profile.....	1018
rm transform profile.....	1019
set transform profile.....	1019
unset transform profile.....	1020
show transform profile.....	1020
transform action.....	1020
add transform action.....	1020
rm transform action.....	1021
set transform action.....	1021
unset transform action.....	1022
show transform action.....	1023
transform policy.....	1023

add transform policy.....	1023
rm transform policy.....	1024
set transform policy.....	1024
unset transform policy.....	1025
show transform policy.....	1025
stat transform policy.....	1026
rename transform policy.....	1026
transform policylabel.....	1027
add transform policylabel.....	1027
rm transform policylabel.....	1028
bind transform policylabel.....	1028
unbind transform policylabel.....	1029
show transform policylabel.....	1029
stat transform policylabel.....	1030
rename transform policylabel.....	1030
transform global.....	1031
bind transform global.....	1031
unbind transform global.....	1031
show transform global.....	1032
Tunnel Commands.....	1032
tunnel trafficPolicy.....	1033
add tunnel trafficPolicy.....	1033
rm tunnel trafficPolicy.....	1034
set tunnel trafficPolicy.....	1034
unset tunnel trafficPolicy.....	1035
show tunnel trafficPolicy.....	1035
tunnel global.....	1036
bind tunnel global.....	1036
unbind tunnel global.....	1037
show tunnel global.....	1037
Utility Commands.....	1038
nstrace.....	1038
nstrace.....	1038
scp.....	1039
scp.....	1039
shell.....	1040
shell.....	1040
install.....	1041
install.....	1041
grep.....	1041

grep.....	1041
traceroute6.....	1042
traceroute6.....	1042
traceroute.....	1043
traceroute.....	1043
ping6.....	1045
ping6.....	1045
ping.....	1046
ping.....	1046
techsupport.....	1047
show techsupport.....	1047
callhome.....	1047
show callhome.....	1047
set callhome.....	1048
unset callhome.....	1048
VPN Commands.....	1049
vpn.....	1049
stat vpn.....	1049
vpn vserver.....	1050
add vpn vserver.....	1050
rm vpn vserver.....	1052
set vpn vserver.....	1053
unset vpn vserver.....	1055
bind vpn vserver.....	1055
unbind vpn vserver.....	1056
enable vpn vserver.....	1056
disable vpn vserver.....	1057
show vpn vserver.....	1057
stat vpn vserver.....	1058
rename vpn vserver.....	1058
vpn intranetApplication.....	1059
add vpn intranetApplication.....	1059
rm vpn intranetApplication.....	1060
show vpn intranetApplication.....	1060
vpn nextHopServer.....	1060
add vpn nextHopServer.....	1060
rm vpn nextHopServer.....	1061
show vpn nextHopServer.....	1061
vpn trafficPolicy.....	1062
add vpn trafficPolicy.....	1062

rm vpn trafficPolicy.....	1063
set vpn trafficPolicy.....	1063
unset vpn trafficPolicy.....	1064
show vpn trafficPolicy.....	1064
vpn trafficAction.....	1064
add vpn trafficAction.....	1064
rm vpn trafficAction.....	1065
set vpn trafficAction.....	1065
unset vpn trafficAction.....	1066
show vpn trafficAction.....	1066
vpn formSSOAction.....	1067
add vpn formSSOAction.....	1067
rm vpn formSSOAction.....	1068
set vpn formSSOAction.....	1068
unset vpn formSSOAction.....	1069
show vpn formSSOAction.....	1069
vpn samlSSOProfile.....	1069
add vpn samlSSOProfile.....	1070
rm vpn samlSSOProfile.....	1070
set vpn samlSSOProfile.....	1071
unset vpn samlSSOProfile.....	1071
show vpn samlSSOProfile.....	1072
vpn url.....	1072
add vpn url.....	1072
rm vpn url.....	1073
set vpn url.....	1073
unset vpn url.....	1074
show vpn url.....	1074
vpn sessionPolicy.....	1074
add vpn sessionPolicy.....	1075
rm vpn sessionPolicy.....	1075
set vpn sessionPolicy.....	1075
unset vpn sessionPolicy.....	1076
show vpn sessionPolicy.....	1076
vpn sessionAction.....	1077
add vpn sessionAction.....	1077
rm vpn sessionAction.....	1083
set vpn sessionAction.....	1084
unset vpn sessionAction.....	1090
show vpn sessionAction.....	1091

Contents

vpn clientlessAccessPolicy.....	1091
add vpn clientlessAccessPolicy.....	1091
rm vpn clientlessAccessPolicy.....	1092
set vpn clientlessAccessPolicy.....	1092
show vpn clientlessAccessPolicy.....	1093
vpn clientlessAccessProfile.....	1093
add vpn clientlessAccessProfile.....	1093
rm vpn clientlessAccessProfile.....	1093
set vpn clientlessAccessProfile.....	1094
unset vpn clientlessAccessProfile.....	1095
show vpn clientlessAccessProfile.....	1095
vpn stats.....	1096
show vpn stats.....	1096
vpn icaConnection.....	1096
show vpn icaConnection.....	1096
vpn global.....	1096
bind vpn global.....	1096
unbind vpn global.....	1097
show vpn global.....	1098
vpn parameter.....	1098
set vpn parameter.....	1098
unset vpn parameter.....	1105
show vpn parameter.....	1106
WI Commands.....	1106
wi site.....	1106
add wi site.....	1106
rm wi site.....	1109
set wi site.....	1109
unset wi site.....	1112
bind wi site.....	1112
unbind wi site.....	1113
show wi site.....	1114
wi package.....	1114
install wi package.....	1115
uninstall wi package.....	1115

Command Reference

Provides basic information of the NetScaler command line interface and also provides the commands to configure and retrieve details of the appliance.

AAA Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [aaa](#)
- ♦ [aaa user](#)
- ♦ [aaa group](#)
- ♦ [aaa preauthenticationaction](#)
- ♦ [aaa preauthenticationpolicy](#)
- ♦ [aaa stats](#)
- ♦ [aaa session](#)
- ♦ [aaa radiusParams](#)
- ♦ [aaa ldapParams](#)
- ♦ [aaa tacacsParams](#)
- ♦ [aaa certParams](#)
- ♦ [aaa parameter](#)
- ♦ [aaa preauthenticationparameter](#)
- ♦ [aaa global](#)
- ♦ [aaa kcdAccount](#)

aaa

stat aaa

Synopsis

```
stat aaa [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]  
[-clearstats ( basic | full )]
```

Description

Display aaa statistics

Parameters

clearstats

Clear the statistics / counters Possible values: basic, full

aaa user

[[add](#) | [rm](#) | [set](#) | [bind](#) | [unbind](#) | [show](#)]

add aaa user

Synopsis

add aaa user <userName> {-password }

Description

Adds a local AAA user account and verifies the configuration to ensure that it is correct.

Parameters

userName

Name for the user. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space (), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the user is added. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my aaa user" or 'my aaa user').

password

Password with which the user logs on. Required for any user account that does not exist on an external authentication server. If you are not using an external authentication server, all user accounts must have a password. If you are using an external authentication server, you must provide a password for local user accounts that do not exist on the authentication server.

Example

```
add aaa user johndoe -password abcd
add aaa user johndoe -password
The above example adds user johndoe with password
abcd for first case, password supplied on prompt
for second case
```

[Top](#)

rm aaa user

Synopsis

rm aaa user <userName>

Description

Removes a local AAA user account and the associated configuration.

Parameters

userName

Name of the AAA user account to remove.

[Top](#)

set aaa user

Synopsis

set aaa user <userName>

Description

Configures the password for an existing local AAA user account. This command prompts you for a new password. NOTE: AAA does not request confirmation of the new password, so you might want to test the new password before sending it to the user.

Parameters

userName

Name of the local AAA user account.

password

Password with which the user logs on. Required for any user account that does not exist on an external authentication server. If you are not using an external authentication server, all user accounts must have a password. If you are using an external authentication server, you must provide a password for local user accounts that do not exist on the authentication server.

Example

```
set aaa user johndoe password abcd
The above command sets the password for johndoe to
abcd
```

[Top](#)

bind aaa user

Synopsis

bind aaa user <userName> [-policy <string> [-priority <positive_integer>]] [-intranetApplication <string>] [-urlName <string>] [-intranetIP <ip_addr> [<netmask>]]

Description

Binds a policy to the specified user account.

Parameters

userName

User account to which to bind the policy.

policy

Name for the policy that you are creating. Must begin with a letter, number, or the underscore character (_), and must consist only of letters, numbers, and the hyphen (-), period (.) pound (#), space (), at sign (@), equals (=), colon (:), and underscore characters. Cannot be changed after the policy is added. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or "my policy").

intranetApplication

Name of the intranet VPN application to which the policy applies.

urlName

URL of the intranet application to which you are binding the policy.

intranetIP

IP address of the intranet application to which you are binding the policy.

Example

```
To bind intranetip to the user joe:
bind aaa user joe -intranetip 10.102.1.123
```

[Top](#)

unbind aaa user

Synopsis

```
unbind aaa user <userName> [-policy <string>] [-intranetApplication <string>] [-urlName
<string>] [-intranetIP <ip_addr> [<netmask>]]
```

Description

Unbinds a policy from the specified user account.

Parameters

userName

Name of the user account from which to unbind the policy.

policy

Name of the policy to unbind.

intranetApplication

Name of the intranet VPN application from which you are unbinding the policy.

urlName

URL of the intranet application from which you are unbinding the policy.

intranetIP

Intranet IP address of the application from which you are unbinding the policy.

Example

```
unbind AAA user joe -intranetip 10.102.1.123
```

[Top](#)

show aaa user**Synopsis**

```
show aaa user [<userName>] [-loggedIn]
```

Description

Displays the current configuration of a AAA user account.

Parameters**userName**

Name of the user who has the account.

loggedIn

Show whether the user is logged in or not.

Example

```
Example
> show aaa user joe
      UserName: joe           IntranetIP:
10.102.1.123

      Bound to groups:
      GroupName: engg

Done
>
```

[Top](#)

aaa group

[[add](#) | [rm](#) | [bind](#) | [unbind](#) | [show](#)]

add aaa group**Synopsis**

```
add aaa group <groupName>
```

Description

Creates a AAA group and verifies the configuration to ensure that it is correct.

Parameters

groupName

Name for the group. Must begin with a letter, number, or the underscore character (_), and must consist only of letters, numbers, and the hyphen (-), period (.) pound (#), space (), at sign (@), equals (=), colon (:), and underscore characters. Cannot be changed after the group is added. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my aaa group" or 'my aaa group').

Example

```
add aaa group group_ad
```

[Top](#)

rm aaa group

Synopsis

```
rm aaa group <groupName>
```

Description

Removes the specified AAA group.

Parameters

groupName

Name of the group that you are removing.

[Top](#)

bind aaa group

Synopsis

```
bind aaa group <groupName> [-userName <string>] [-policy <string> [-priority  
<positive_integer>]] [-intranetApplication <string>] [-urlName <string>] [-intranetIP  
<ip_addr> <netmask>]
```

Description

Binds the specified AAA group to the specified resource. The resource can be a user, an Intranet IP address or range, a policy, or an Intranet application.

Parameters

groupName

Name of the group that you are binding.

userName

Bind a AAA group to the specified AAA user. If the specified user is bound to more than one group, the group expressions are evaluated, upon authorization, to determine the appropriate action.

policy

Bind a policy to the specified AAA group.

intranetApplication

Bind the group to the specified intranet VPN application.

urlName

Bind the group to the specified URL.

intranetIP

Bind the group to the specified IP address or IP block. Normally you would bind the group to an IP address or range that your users use to access intranet resources.

Example

```
To bind an Intranet IP to the group engg:
bind aaa group engg -intranetip 10.102.10.0
255.255.255.0
```

[Top](#)

unbind aaa group

Synopsis

```
unbind aaa group <groupName> [-userName <string> ...] [-policy <string>] [-
intranetApplication <string>] [-urlName <string>] [-intranetIP <ip_addr> <netmask>]
```

Description

Unbinds the specified AAA group from the specified resource. The resource can be a user, an intranet IP address or range, a policy, or an intranet application.

Parameters

groupName

Name of the group that you are unbinding.

userName

Unbind the specified AAA group from the specified AAA user.

policy

Unbind the specified policy from the specified AAA group.

intranetApplication

Unbind the specified group from the specified intranet VPN application.

urlName

Unbind the specified group from the specified URL.

intranetIP

Unbind the specified group from the specified IP address or IP block.

Example

```
unbind aaa group engg -intranetip 10.102.10.0
255.255.255.0
```

[Top](#)

show aaa group

Synopsis

show aaa group [<groupName>] [-loggedIn]

Description

Displays the current configuration of a AAA group.

Parameters

groupName

Name of the group.

loggedIn

Display only the group members who are currently logged in.

Example

```
> show aaa group engg
  GroupName: engg

  Bound AAA users:
  Username: joe
  Username: jane

  Intranetip IP: 10.102.10.0      Netmask:
255.255.255.0
  Done
>
```

[Top](#)

aaa preauthenticationaction

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add aaa preauthenticationaction

Synopsis

```
add aaa preauthenticationaction <name> [<preauthenticationaction>] [-killProcess <string>] [-deletefiles <string>]
```

Description

Adds an action (profile) for endpoint analysis (EPA) clients before authentication.

Parameters

name

Name for the preauthentication action. Must begin with a letter, number, or the underscore character (_), and must consist only of letters, numbers, and the hyphen (-), period (.) pound (#), space (), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after preauthentication action is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my aaa action" or 'my aaa action').

preauthenticationaction

Allow or deny logon after endpoint analysis (EPA) results. Possible values: ALLOW, DENY

killProcess

String specifying the name of a process to be terminated by the endpoint analysis (EPA) tool.

deletefiles

String specifying the path(s) and name(s) of the files to be deleted by the endpoint analysis (EPA) tool.

[Top](#)

rm aaa preauthenticationaction

Synopsis

```
rm aaa preauthenticationaction <name>
```

Description

Removes a preauthentication action. NOTE: A preauthentication action cannot be removed if it is bound to a policy.

Parameters

name

Name of the preauthentication action to remove.

[Top](#)

set aaa preauthenticationaction

Synopsis

```
set aaa preauthenticationaction <name> [<preauthenticationaction>] [-killProcess  
<string>] [-deletefiles <string>]
```

Description

Modifies an existing preauthentication action (profile).

Parameters

name

Name of the preauthentication action to modify.

preauthenticationaction

Allow or deny logon after endpoint analysis (EPA) results. Possible values: ALLOW, DENY

killProcess

String specifying the name of a process to be terminated by the endpoint analysis (EPA) tool.

deletefiles

String specifying the path(s) and name(s) of the files to be deleted by the endpoint analysis (EPA) tool.

[Top](#)

unset aaa preauthenticationaction

Synopsis

```
unset aaa preauthenticationaction <name> [-killProcess] [-deletefiles]
```

Description

Use this command to remove aaa preauthenticationaction settings. Refer to the set aaa preauthenticationaction command for meanings of the arguments.

[Top](#)

show aaa preauthenticationaction

Synopsis

```
show aaa preauthenticationaction [<name>]
```

Description

Displays details of the specified preauthentication action.

Parameters

name

Name of the preauthentication action.

[Top](#)

aaa preauthenticationpolicy

[[add](#) | [rm](#) | [set](#) | [show](#)]

add aaa preauthenticationpolicy

Synopsis

add aaa preauthenticationpolicy <name> <rule> [<reqAction>]

Description

Adds a preauthentication policy. The policy defines expressions to be evaluated by the endpoint analysis (EPA) tool.

Parameters

name

Name for the preauthentication policy. Must begin with a letter, number, or the underscore character (_), and must consist only of letters, numbers, and the hyphen (-), period (.), pound (#), space (), at sign (@), equals (=), colon (:), and underscore characters. Cannot be changed after the preauthentication policy is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy').

rule

Name of the NetScaler named rule, or a default syntax expression, defining connections that match the policy.

reqAction

Name of the action that the policy is to invoke when a connection matches the policy.

[Top](#)

rm aaa preauthenticationpolicy

Synopsis

rm aaa preauthenticationpolicy <name>

Description

Removes the specified preauthentication policy.

Parameters

name

Name of the preauthentication policy to remove.

[Top](#)

set aaa preauthenticationpolicy

Synopsis

set aaa preauthenticationpolicy <name> [-rule <expression>] [-reqAction <string>]

Description

Modifies the Request Action of a preauthentication policy.

Parameters

name

Name of the preauthentication policy to modify.

rule

The new rule to be associated with the policy.

reqAction

Name of the action that the policy is to invoke when a connection matches the policy.

[Top](#)

show aaa preauthenticationpolicy

Synopsis

show aaa preauthenticationpolicy [<name>]

Description

Displays the properties of either the specified preauthentication policy or (if none is specified) a list of all configured preauthentication policies.

Parameters

name

Name of the preauthentication policy whose properties you want to view.

[Top](#)

aaa stats

show aaa stats

Synopsis

show aaa stats - alias for 'stat aaa'

Description

show aaa stats is an alias for stat aaa

aaa session

[[show](#) | [kill](#)]

show aaa session

Synopsis

```
show aaa session [-userName <string>] [-groupName <string>] [-intranetIP <ip_addr|*>
[<netmask>]]
```

Description

Displays all AAA-TM/VPN connections that are bound to the specified user, group, IP address, or IP range.

Parameters

userName

Name of the AAA user.

groupName

Name of the AAA group.

intranetIP

IP address or the first address in the intranet IP range.

Example

```
> show aaa connection
      ClintIp (ClientPort)   ->
ServerIp (ServerPort)
      -----
User Name: Joe

      10.102.0.39           (2318 ) -> 10.102.4.245
(443 )
      10.102.0.39           (2320 ) -> 10.102.4.245
(443 )
      10.102.0.39           (2340 ) -> 10.102.4.245
(443 )

      Done
>
```

[Top](#)

kill aaa session

Synopsis

```
kill aaa session [-userName <string>] [-groupName <string>] [-intranetIP <ip_addr|*>
[<netmask>]] [-all]
```

Description

Terminates the specified AAA-TM/VPN session.

Parameters

userName

Terminate AAA-TM/VPN sessions that belong to the specified user.

groupName

Terminate AAA-TM/VPN sessions that belong to any user that is a member of the specified group.

intranetIP

Terminate AAA-TM/VPN sessions that are associated with the specified intranet IP address or with an address in the range specified by the address and subnet mask.

all

Terminate all active AAA-TM/VPN sessions.

Example

```
kill aaa session -user joe
```

[Top](#)

aaa radiusParams

[[set](#) | [unset](#) | [show](#)]

set aaa radiusParams

Synopsis

```
set aaa radiusParams [-serverIP <ip_addr|ipv6_addr|*>] [-serverPort <port>] [-authTimeout <positive_integer>] {-radKey } [-radNASip ( ENABLED | DISABLED )] [-radNASid <string>] [-radVendorID <positive_integer>] [-radAttributeType <positive_integer>] [-radGroupsPrefix <string>] [-radGroupSeparator <string>] [-passEncoding <passEncoding>] [-ipVendorID <positive_integer>] [-ipAttributeType <positive_integer>] [-accounting ( ON | OFF )] [-pwdVendorID <positive_integer>] [-pwdAttributeType <positive_integer>] [-defaultAuthenticationGroup <string>] [-callingstationid ( ENABLED | DISABLED )]
```

Description

Modifies the global configuration settings for the RADIUS server. The settings that you specify are used for all SSL-VPN virtual servers unless you use authentication policies to create a configuration for a specific SSL-VPN virtual server.

Parameters

serverIP

IP address of your RADIUS server.

serverPort

Port number on which the RADIUS server listens for connections. Default value: 1812
Minimum value: 1

authTimeout

Maximum number of seconds that the NetScaler appliance waits for a response from the RADIUS server. Default value: 3 Minimum value: 1

radKey

The key shared between the RADIUS server and clients. Required for allowing the NetScaler appliance to communicate with the RADIUS server.

radNASip

Send the NetScaler IP (NSIP) address to the RADIUS server as the Network Access Server IP (NASIP) part of the Radius protocol. Possible values: ENABLED, DISABLED

radNASid

Send the Network Access Server ID (NASID) for your NetScaler appliance to the RADIUS server as the nasid part of the Radius protocol.

radVendorID

Vendor ID for RADIUS group extraction. Minimum value: 1

radAttributeType

Attribute type for RADIUS group extraction. Minimum value: 1

radGroupsPrefix

Prefix string that precedes group names within a RADIUS attribute for RADIUS group extraction.

radGroupSeparator

Group separator string that delimits group names within a RADIUS attribute for RADIUS group extraction.

passEncoding

Enable password encoding in RADIUS packets that the NetScaler appliance sends to the RADIUS server. Possible values: pap, chap, mschapv1, mschapv2 Default value: AAA_PAP

ipVendorID

Vendor ID attribute in the RADIUS response. If the attribute is not vendor-encoded, it is set to 0.

ipAttributeType

IP attribute type in the RADIUS response. Minimum value: 1

accounting

Configure the RADIUS server state to accept or refuse accounting messages. Possible values: ON, OFF

pwdVendorID

Vendor ID of the password in the RADIUS response. Used to extract the user password. Minimum value: 1

defaultAuthenticationGroup

This is the default group that is chosen when the authentication succeeds in addition to extracted groups. Maximum value: 64

callingstationid

Send Calling-Station-ID of the client to the RADIUS server. IP Address of the client is sent as its Calling-Station-ID. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

```
To configure the default RADIUS parameters:
set aaa radiusparams -serverip 192.30.1.2 -radkey
sslvpn
```

[Top](#)

unset aaa radiusParams

Synopsis

```
unset aaa radiusParams [-serverIP] [-serverPort] [-authTimeout] [-radNASip] [-radNASid]
[-radVendorID] [-radAttributeType] [-radGroupsPrefix] [-radGroupSeparator] [-
passEncoding] [-ipVendorID] [-ipAttributeType] [-accounting] [-pwdVendorID] [-
pwdAttributeType] [-defaultAuthenticationGroup] [-callingstationid]
```

Description

Use this command to remove aaa radiusParams settings. Refer to the set aaa radiusParams command for meanings of the arguments.

[Top](#)

show aaa radiusParams

Synopsis

```
show aaa radiusParams
```

Description

Displays the current RADIUS configuration on the NetScaler appliance.

Example

```
> show aaa radiusparams
Configured RADIUS parameters
      Server IP: 127.0.0.2      Port: 1812
      key: secret      Timeout: 10
Done
>
```

[Top](#)

aaa ldapParams

[[set](#) | [unset](#) | [show](#)]

set aaa ldapParams

Synopsis

```
set aaa ldapParams [-serverIP <ip_addr|ipv6_addr|*>] [-serverPort <port>] [-authTimeout <positive_integer>] [-ldapBase <string>] [-ldapBindDn <string>] {-ldapBindDnPassword } [-ldapLoginName <string>] [-searchFilter <string>] [-groupAttrName <string>] [-subAttributeName <string>] [-secType <secType>] [-svrType ( AD | NDS )] [-ssoNameAttribute <string>] [-passwdChange ( ENABLED | DISABLED )] [-nestedGroupExtraction ( ON | OFF )] [-maxNestingLevel <positive_integer>] [-groupNameIdentifier <string>] [-groupSearchAttribute <string>] [-groupSearchSubAttribute <string>] [-groupSearchFilter <string>] [-defaultAuthenticationGroup <string>]
```

Description

Modifies the global configuration settings for the LDAP server. The settings that you specify are used for all SSL-VPN virtual servers unless you use authentication policies to create a configuration for a specific SSL-VPN virtual server.

Parameters

serverIP

IP address of your LDAP server.

serverPort

Port number on which the LDAP server listens for connections. Default value: 389
Minimum value: 1

authTimeout

Maximum number of seconds that the NetScaler appliance waits for a response from the LDAP server. Default value: 3 Minimum value: 1

ldapBase

Base (the server and location) from which LDAP search commands should start. If the LDAP server is running locally, the default value of base is dc=netscaler, dc=com.

ldapBindDn

Complete distinguished name (DN) string used for binding to the LDAP server.

ldapBindDnPassword

Password for binding to the LDAP server.

ldapLoginName

Name attribute that the NetScaler appliance uses to query the external LDAP server or an Active Directory.

searchFilter

String to be combined with the default LDAP user search string to form the value to use when executing an LDAP search. For example, the following values:
vpnallowed=true, ldaploginname=""samaccount"" when combined with the user-

supplied username `""bob""`, yield the following LDAP search string:
`""(&(vpnallowed=true)(samaccount=bob))""`

groupAttrName

Attribute name used for group extraction from the LDAP server.

subAttributeName

Subattribute name used for group extraction from the LDAP server.

secType

Type of security used for communications between the NetScaler appliance and the LDAP server. For the PLAINTEXT setting, no encryption is required. Possible values: PLAINTEXT, TLS, SSL Default value: AAA_LDAP_PLAINTEXT

svrType

The type of LDAP server. Possible values: AD, NDS Default value: AAA_LDAP_SERVER_TYPE_DEFAULT

ssoNameAttribute

Attribute used by the NetScaler appliance to query an external LDAP server or Active Directory for an alternative username. This alternative username is then used for single sign-on (SSO).

passwdChange

Accept password change requests. Possible values: ENABLED, DISABLED Default value: DISABLED

nestedGroupExtraction

Queries the external LDAP server to determine whether the specified group belongs to another group. Possible values: ON, OFF Default value: OFF

defaultAuthenticationGroup

This is the default group that is chosen when the authentication succeeds in addition to extracted groups. Maximum value: 64

Example

```
To configure authentication in the LDAP server
running at 192.40.1.2:
set aaa ldapparams -serverip 192.40.1.2 -ldapbase
"dc=netScaler,dc=com" -ldapbindDN
"cn=Manager,dc=netScaler,dc=com" -
ldapbindDnPassword secret -ldaploginname uid
```

[Top](#)

unset aaa ldapParams

Synopsis

```
unset aaa ldapParams [-serverIP] [-serverPort] [-authTimeout] [-ldapBase] [-
ldapBindDn] [-ldapBindDnPassword] [-ldapLoginName] [-searchFilter] [-groupAttrName]
[-subAttributeName] [-secType] [-svrType] [-ssoNameAttribute] [-passwdChange] [-
nestedGroupExtraction] [-maxNestingLevel] [-groupNameIdentifier] [-
```

groupSearchAttribute] [-groupSearchSubAttribute] [-groupSearchFilter] [-defaultAuthenticationGroup]

Description

Use this command to remove aaa ldapParams settings. Refer to the set aaa ldapParams command for meanings of the arguments.

[Top](#)

show aaa ldapParams

Synopsis

show aaa ldapParams

Description

Displays the current LDAP configuration on the NetScaler appliance.

Example

```
> show aaa ldapparams
Configured LDAP parameters
  Server IP: 127.0.0.1      Port: 389
  Timeout: 1      BindDn:
cn=Manager,dc=florazel,dc=com
  login: uid      Base: dc=florazel,dc=com
  Secure Type: PLAINTEXT
Done
>
```

[Top](#)

aaa tacacsParams

[[set](#) | [unset](#) | [show](#)]

set aaa tacacsParams

Synopsis

set aaa tacacsParams [-serverIP <ip_addr|ipv6_addr|*>] [-serverPort <port>] [-authTimeout <positive_integer>] {-tacacsSecret } [-authorization (ON | OFF)] [-accounting (ON | OFF)] [-auditFailedCmds (ON | OFF)] [-defaultAuthenticationGroup <string>]

Description

Modifies the global configuration settings for the TACACS+ server. The settings that you specify are used for all SSL-VPN virtual servers unless you use authentication policies to create a configuration for a specific SSL-VPN virtual server.

Parameters

serverIP

IP address of your TACACS+ server.

serverPort

Port number on which the TACACS+ server listens for connections. Default value: 49
Minimum value: 1

authTimeout

Maximum number of seconds that the NetScaler appliance waits for a response from the TACACS+ server. Default value: 3 Minimum value: 1

tacacsSecret

Key shared between the TACACS+ server and clients. Required for allowing the NetScaler appliance to communicate with the TACACS+ server.

authorization

Use streaming authorization on the TACACS+ server. Possible values: ON, OFF

accounting

Send accounting messages to the TACACS+ server. Possible values: ON, OFF

auditFailedCmds

The option for sending accounting messages to the TACACS+ server. Possible values: ON, OFF

defaultAuthenticationGroup

This is the default group that is chosen when the authentication succeeds in addition to extracted groups. Maximum value: 64

Example

```
To configure a TACACS+ server running at
192.168.1.20
    set aaa tacacsparams -serverip 192.168.1.20 -
tacacssecret secret
```

[Top](#)

unset aaa tacacsParams

Synopsis

```
unset aaa tacacsParams [-serverIP] [-serverPort] [-authTimeout] [-tacacsSecret] [-
authorization] [-accounting] [-auditFailedCmds] [-defaultAuthenticationGroup]
```

Description

Use this command to remove aaa tacacsParams settings. Refer to the set aaa tacacsParams command for meanings of the arguments.

[Top](#)

show aaa tacacsParams

Synopsis

show aaa tacacsParams

Description

Displays the NetScaler appliance's current AAA TACACS+ configuration.

Example

```
> sh aaa tacacsparams
Configured TACACS parameter
      Server IP: 192.168.1.20 Port: 49
      Timeout: 1 secs
Done
```

[Top](#)

aaa certParams

[[set](#) | [unset](#) | [show](#)]

set aaa certParams

Synopsis

set aaa certParams [-userNameField <string>] [-groupNameField <string>] [-defaultAuthenticationGroup <string>]

Description

Modifies the global configuration settings for certificate policies. The settings that you specify are used for all SSL-VPN virtual servers unless you use authentication policies to create a configuration for a specific SSL-VPN virtual server.

Parameters

userNameField

Client certificate field that contains the username, in the format <field>:<subfield>.

groupNameField

Client certificate field that specifies the group, in the format <field>:<subfield>.

defaultAuthenticationGroup

This is the default group that is chosen when the authentication succeeds in addition to extracted groups. Maximum value: 64

Example

```
To configure the default certificate parameters:
  set aaa certparams -userNameField "Subject:CN"
  -groupNameField "Subject:OU"
```

[Top](#)

unset aaa certParams

Synopsis

```
unset aaa certParams [-userNameField] [-groupNameField] [-
defaultAuthenticationGroup]
```

Description

Use this command to remove aaa certParams settings. Refer to the set aaa certParams command for meanings of the arguments.

[Top](#)

show aaa certParams

Synopsis

```
show aaa certParams
```

Description

Displays the current client certificate configuration on the NetScaler appliance.

[Top](#)

aaa parameter

[[set](#) | [unset](#) | [show](#)]

set aaa parameter

Synopsis

```
set aaa parameter [-enableStaticPageCaching ( YES | NO )] [-
enableEnhancedAuthFeedback ( YES | NO )] [-defaultAuthType <defaultAuthType>] [-
maxAAAUUsers <positive_integer>] [-maxLoginAttempts <positive_integer>] [-
failedLoginTimeout <positive_integer>]] [-aaadnatlp <ip_addr|*>]
```

Description

Sets the global AAA configuration. Any configuration settings made at this level overrides configuration settings for the authentication server.

Parameters

enableStaticPageCaching

The default state of VPN Static Page caching. If nothing is specified, the default value is set to ON. Possible values: YES, NO Default value: STATIC_PAGE_CACHING_ENABLED

enableEnhancedAuthFeedback

Enhanced auth feedback provides more information to the end user about the reason for an authentication failure. The default value is set to ON. Possible values: YES, NO Default value: ENHANCED_AUTH_FEEDBACK_DISABLED

defaultAuthType

The default authentication server type. Possible values: LOCAL, LDAP, RADIUS, TACACS, CERT Default value: LOCAL_AUTH

maxAAAUUsers

Maximum number of concurrent users allowed to log on to VPN simultaneously. Minimum value: 1

maxLoginAttempts

Maximum Number of login Attempts Minimum value: 1

aaadnatIp

Source IP address to use for traffic that is sent to the authentication server.

Example

```
set aaa parameter -defaultAuthType RADIUS -
maxAAAUUsers 100
```

[Top](#)

unset aaa parameter

Synopsis

```
unset aaa parameter [-enableStaticPageCaching] [-enableEnhancedAuthFeedback] [-
defaultAuthType] [-maxAAAUUsers] [-aaadnatIp] [-maxLoginAttempts]
```

Description

Resets the global AAA parameter settings on the NetScaler appliance. Attributes for which a default value is available revert to their default values. See the set aaa parameter command for descriptions of the parameters..Refer to the set aaa parameter command for meanings of the arguments.

[Top](#)

show aaa parameter

Synopsis

```
show aaa parameter
```

Description

Displays the current AAA global configuration.

Example

```
> show aaa parameter
Configured AAA parameters
      DefaultAuthType: LDAP      MaxAAUsers: 5
Done
>
```

[Top](#)

aaa preauthenticationparameter

[[set](#) | [unset](#) | [show](#)]

set aaa preauthenticationparameter

Synopsis

```
set aaa preauthenticationparameter [-preauthenticationaction ( ALLOW | DENY )] [-
rule <expression>] [-killProcess <string>] [-deletefiles <string>]
```

Description

Configures the default end point analysis (EPA) parameters that are applied before authentication.

Parameters

preauthenticationaction

Deny or allow login on the basis of end point analysis results. Possible values: ALLOW, DENY

rule

Name of the NetScaler named rule, or a default syntax expression, to be evaluated by the EPA tool.

killProcess

String specifying the name of a process to be terminated by the EPA tool.

deletefiles

String specifying the path(s) to and name(s) of the files to be deleted by the EPA tool, as a string of between 1 and 1023 characters.

[Top](#)

unset aaa preauthenticationparameter

Synopsis

```
unset aaa preauthenticationparameter [-rule] [-preauthenticationaction] [-killProcess]
[-deletefiles]
```


Description

Resets the default end point analysis(EPA) configuration settings on the NetScaler appliance. Attributes for which a default value is available revert to their default values. See the set aaa preauthenticationparameter command for descriptions of the parameters..Refer to the set aaa preauthenticationparameter command for meanings of the arguments.

[Top](#)

show aaa preauthenticationparameter

Synopsis

show aaa preauthenticationparameter

Description

Displays the current preauthentication configuration.

[Top](#)

aaa global

[[bind](#) | [unbind](#) | [show](#)]

bind aaa global

Synopsis

bind aaa global [-policy <string> [-priority <positive_integer>]] [-windowsProfile <string>]

Description

Binds a policy globally.

Parameters

policy

Name of the policy to bind globally.

windowsProfile

Name of the negotiate profile to bind globally.

Example

```
bind aaa global -pol pol1
```

[Top](#)

unbind aaa global

Synopsis

unbind aaa global [-policy <string>] [-windowsProfile <string>]

Description

Unbind the policy from the global bind point.

Parameters

policy

Name of the policy to be unbound.

windowsProfile

Name of the negotiate profile to be bound.

[Top](#)

show aaa global

Synopsis

```
show aaa global
```

Description

Displays a list of policies that are currently bound to Global on the NetScaler appliance.

[Top](#)

aaa kcdAccount

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add aaa kcdAccount

Synopsis

```
add aaa kcdAccount <kcdAccount> {-keytab <string>} {-realmStr <string>} {-delegatedUser <string>} {-kcdPassword} {-usercert <string>} {-cacert <string>}
```

Description

Add a Kerberos constrained delegation account.

Parameters

kcdAccount

The name of the KCD account.

keytab

The path to the keytab file. If specified other parameters in this command need not be given

realmStr

Kerberos Realm.

delegatedUser

Username that can perform kerberos constrained delegation.

kcdPassword

Password for Delegated User.

usercert

SSL Cert (including private key) for Delegated User.

cacert

CA Cert for UserCert or when doing PKINIT backchannel.

Example

```
add aaa kcdaccount my_kcd_acct -keytab /var/
mykcd.keytab
add aaa kcdaccount my_kcd_acct -keytab
The above example adds a Kerberos constrained
delegation account
my_kcd_acct, with the keytab file located at /var/
mykcd.keytab
```

[Top](#)

rm aaa kcdAccount**Synopsis**

```
rm aaa kcdAccount <kcdAccount>
```

Description

Remove the KCD account.

Parameters**kcdAccount**

The KCD account name.

[Top](#)

set aaa kcdAccount**Synopsis**

```
set aaa kcdAccount <kcdAccount> [-keytab <string>] [-realmStr <string>] [-
delegatedUser <string>] [-kcdPassword ] [-usercert <string>] [-cacert <string>]
```

Description

Set the KCD account information.

Parameters**kcdAccount**

The name of the KCD account.

keytab

The path to the keytab file. If specified other parameters in this command need not be given

realmStr

Kerberos Realm.

delegatedUser

Username that can perform kerberos constrained delegation.

kcdPassword

Password for Delegated User.

usercert

SSL Cert (including private key) for Delegated User.

cacert

CA Cert for UserCert or when doing PKINIT backchannel.

Example

```
set aaa kcdaccount my_kcd_acct -keytab /var/
hiskcd.keytab
The above command sets the keytab location for KCD
account
my_kcd_acct to /var/hiskcd.keytab
```

[Top](#)

unset aaa kcdAccount

Synopsis

```
unset aaa kcdAccount <kcdAccount> [-usercert <string>] [-cacert <string>]
```

Description

Unset the KCD account information..Refer to the set aaa kcdAccount command for meanings of the arguments.

[Top](#)

show aaa kcdAccount

Synopsis

```
show aaa kcdAccount [<kcdAccount>]
```

Description

Display KCD accounts.

Parameters

kcdAccount

The KCD account name.

Example

```

Example
> show aaa kcdaccount my_kcd_acct
      KcdAccount: my_kcd_acct
Keytab: /var/mykcd.keytab
Done
>

```

[Top](#)

Application Commands

[\[import | export | rm \]](#)

import application

Synopsis

```
import application <apptemplateFilename> [-appname <string>] [-deploymentFilename
<input_filename>]
```

Description

Imports application configuration information from an AppExpert application template file. You can specify a deployment file along with the template file. A template file contains application and variable definitions. A deployment file contains information about the services, service groups, endpoints, and variables that were in the AppExpert application configuration at the time the template file was created. Before you use template and deployment files, make sure that they are present in the /nsconfig/nstemplates/applications/ and /nsconfig/nstemplates/applications/deployment_files directories, respectively. You can transfer the files from your local drive to those directories on the NetScaler appliance by using either FTP or the NetScaler configuration utility. In the configuration utility, you can also import the files and create the application by using a single wizard (AppExpert > Applications > Import > AppExpert Template Wizard).

Parameters

apptemplateFilename

Name of the AppExpert application template file.

appname

Name to assign to the application on the NetScaler appliance. If you do not provide a name, the appliance assigns the application the name of the template file.

deploymentFilename

Name of the deployment file.

Example

```
import app application sampleapp -  
apptemplatefilename sampleapp.xml -  
deploymentfilename deploy.xml
```

[Top](#)

export application

Synopsis

```
export application <appname> [-apptemplateFilename <input_filename>] [-  
deploymentFilename <input_filename>]
```

Description

Exports application configuration information to an AppExpert application template file. A deployment file is created along with the template file. The template file contains application and variable definitions. The deployment file contains information about the services, service groups, endpoints, and variables that are in the AppExpert application configuration. The template and deployment files are exported to the /nsconfig/nstemplates/applications/ and /nsconfig/nstemplates/applications/deployment_files directories, respectively. If you use the configuration utility, you can also export an application to your local hard drive.

Parameters

appname

Name of the AppExpert application whose configuration you want to export to a template file.

apptemplateFilename

Name with which to save the template file. If you do not specify a name, the template file is saved with the name of the application.

deploymentFilename

Name with which to save the deployment file. If you do not specify a name, a string consisting of an underscore and "deployment" (_deployment) is automatically appended to the name of the template file to create the name of the deployment file.

[Top](#)

rm application

Synopsis

```
rm application <appname>
```

Description

Remove application configuration information from a netscaler device. You can specify an application name as input. All the configuration belonging to the specified application will be removed from the device.

Parameters

appname

Name of the AppExpert application whose configuration you want to remove from the Netscaler appliance.

[Top](#)

AppFlow Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [appflow](#)
- ♦ [appflow collector](#)
- ♦ [appflow action](#)
- ♦ [appflow policy](#)
- ♦ [appflow policylabel](#)
- ♦ [appflow param](#)
- ♦ [appflow global](#)

appflow

stat appflow

Synopsis

```
stat appflow [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile  
<input_filename>] [-clearstats ( basic | full )]
```

Description

Display AppFlow statistics.

Parameters

clearstats

Clear the statistics / counters Possible values: basic, full

appflow collector

[[add](#) | [rm](#) | [rename](#) | [show](#)]

add appflow collector

Synopsis

add appflow collector <name> -IPAddress <ip_addr> [-port <port>] [-netProfile <string>]

Description

Adds a new AppFlow collector. A collector receives the flow records generated by the NetScaler appliance. You can add only four AppFlow collectors to the NetScaler appliance.

Parameters

name

Name for the collector. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Only four collectors can be configured. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my appflow collector" or 'my appflow collector').

IPAddress

IPv4 address of the collector.

port

UDP port on which the collector listens. Default value: 4739

netProfile

Netprofile to associate with the collector. The IP address defined in the profile is used as the source IP address for AppFlow traffic for this collector. If you do not set this parameter, the NetScaler IP (NSIP) address is used as the source IP address.

Example

```
add appflow collector collector1 -IPAddress
192.168.1.40 -port 2055
```

[Top](#)

rm appflow collector

Synopsis

rm appflow collector <name>

Description

Removes an AppFlow collector. You cannot remove a collector if it is associated with an AppFlow action.

Parameters

name

Name of the collector to remove.

Example

```
rm appflow collector collector1
```

[Top](#)

rename appflow collector

Synopsis

```
rename appflow collector <name>@ <newName>@
```

Description

Renames an AppFlow collector.

Parameters

name

Existing name of the collector.

newName

New name for the collector. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at(@), equals (=), and hyphen (-) characters. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my appflow coll" or 'my appflow coll').

Example

```
rename appflow collector old_name new_name
```

[Top](#)

show appflow collector

Synopsis

```
show appflow collector [<name>]
```

Description

Displays information about all configured AppFlow collectors, or about the specified collector.

Parameters

name

Name of the collector about which to display information.

Example

```
show appflow collector collector1
```

[Top](#)

appflow action

[[add](#) | [rm](#) | [set](#) | [unset](#) | [rename](#) | [show](#)]

add appflow action

Synopsis

add appflow action <name> -collectors <string> ... [-comment <string>]

Description

Creates an AppFlow action. The action can be associated with an AppFlow policy by using the add appflow policy command.

Parameters

name

Name for the action. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my appflow action" or 'my appflow action').

collectors

Name(s) of collector(s) to be associated with the AppFlow action.

comment

Any comments about this action. In the CLI, if including spaces between words, enclose the comment in quotation marks. (The quotation marks are not required in the configuration utility.)

Example

```
add appflow action appflow_action_1 -collectors  
col1 col2
```

[Top](#)

rm appflow action

Synopsis

rm appflow action <name>

Description

Removes a configured AppFlow action. You cannot remove an action that is associated with an AppFlow policy.

Parameters

name

Name of the action to be removed.

Example

```
rm appflow action appflow_action_1
```

[Top](#)

set appflow action

Synopsis

set appflow action <name> [-collectors <string> ...] [-comment <string>]

Description

Modifies the specified parameters of an AppFlow action.

Parameters

name

Name of the action to be modified.

collectors

Name(s) of collector(s) to be associated with the AppFlow action.

comment

Any comments about this action. In the CLI, if including spaces between words, enclose the comment in quotation marks. (The quotation marks are not required in the configuration utility.)

Example

```
set appflow action appflow_action_1 -collectors  
col1 col2 col3
```

[Top](#)

unset appflow action

Synopsis

unset appflow action <name> -comment

Description

Use this command to remove appflow action settings. Refer to the set appflow action command for meanings of the arguments.

[Top](#)

rename appflow action

Synopsis

rename appflow action <name>@ <newName>@

Description

Renames an AppFlow action.

Parameters

name

Existing name of the action.

newName

New name for the AppFlow action. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my appflow action" or 'my appflow action').

Example

```
rename appflow action old_name new_name
```

[Top](#)

show appflow action

Synopsis

show appflow action [<name>]

Description

Displays information about AppFlow action(s), or about the specified AppFlow action.

Parameters

name

Name of the action about which to display information.

Example

```
1. show appflow action
2. show appflow action appflow_action_1
```

[Top](#)

appflow policy

[[add](#) | [rm](#) | [set](#) | [unset](#) | [rename](#) | [show](#)]

add appflow policy

Synopsis

add appflow policy <name> <rule> <action> [-comment <string>]

Description

Adds an Appflow policy. The policy specifies the rule based on which the traffic is evaluated, and the action to be taken if the rule returns "TRUE".

Parameters

name

Name for the policy. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my appflow policy" or 'my appflow policy').

rule

Expression or other value against which the traffic is evaluated. Must be a Boolean, default syntax expression. Note: Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>". The following requirements apply only to the NetScaler CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action

Name of the action to be associated with this policy.

comment

Any comments about this policy.

Example

```
add appflow policy appflow_pol "HTTP.REQ.HEADER(\
\"header\\").CONTAINS(\\\"qh3\\\")" appflow_act
```

[Top](#)

rm appflow policy

Synopsis

rm appflow policy <name>

Description

Removes an AppFlow policy. (Cannot remove a policy that is bound to a policy label.)

Parameters

name

Name of the policy to be removed.

Example

```
rm appflow policy appflow_policy_1
```

[Top](#)

set appflow policy

Synopsis

set appflow policy <name> [-rule <expression>] [-action <string>] [-comment <string>]

Description

Modifies the rule and/or action for an existing AppFlow policy. The rule for flow type can be changed only if the associated action is of NEUTRAL flow type.

Parameters

name

Name of the policy to modify.

rule

Expression or other value against which the traffic is evaluated. Must be a Boolean, default syntax expression. Note: Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>" The following requirements apply only to the NetScaler CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the \ character. * Alternatively, you

can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action

Name of the action to be associated with this policy.

comment

Any comments about this policy.

Example

```
set appflow policy appflow_policy -rule
"HTTP.REQ.HEADER(\\\"header\\\") .CONTAINS (\\\"qh2\\\") "
```

[Top](#)

unset appflow policy

Synopsis

```
unset appflow policy <name> -comment
```

Description

Use this command to remove appflow policy settings. Refer to the set appflow policy command for meanings of the arguments.

[Top](#)

rename appflow policy

Synopsis

```
rename appflow policy <name>@ <newName>@
```

Description

Renames an AppFlow policy.

Parameters

name

Existing name of the policy.

newName

New name for the policy. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my appflow policy" or 'my appflow policy').

Example

```
rename appflow policy old_name new_name
```

[Top](#)

show appflow policy

Synopsis

```
show appflow policy [<name>]
```

Description

Displays information about all configured AppFlow policies, or detailed information about the specified policy.

Parameters

name

Name of the policy about which to display detailed information.

Example

```
show appflow policy
```

[Top](#)

appflow policylabel

[[add](#) | [rm](#) | [bind](#) | [unbind](#) | [rename](#) | [show](#)]

add appflow policylabel

Synopsis

```
add appflow policylabel <labelName> [-policylabeltype ( HTTP | OTHERTCP )]
```

Description

Creates a user-defined AppFlow policy label. You can bind AppFlow policies to the AppFlow policy label.

Parameters

labelName

Name of the AppFlow policy label. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my appflow policylabel" or 'my appflow policylabel').

policylabeltype

Type of traffic evaluated by the policies bound to the policy label. Possible values: HTTP, OTHERTCP Default value: NS_PLTMAP_APPFLOW_REQ

Example

```
add appflow policylabel appflow_pol_label
```

[Top](#)**rm appflow policylabel****Synopsis**

```
rm appflow policylabel <labelName>
```

Description

Removes an AppFlow policy label.

Parameters

labelName

Name of the policy label to be removed.

Example

```
rm appflow policylabel appflow_pol_label
```

[Top](#)**bind appflow policylabel****Synopsis**

```
bind appflow policylabel <labelName> -policyName <string> -priority <positive_integer> [-gotoPriorityExpression <expression>] [-invoke (<labelType> <labelName>)]
```

Description

Binds an AppFlow policy to an AppFlow policy label.

Parameters

labelName

Name of the policy label to which to bind the policy.

policyName

Name of the policy to bind to the policy label.

Example

```
bind appflow policylabel appflow_pol_label -  
policyName appflow_pol -priority 1
```

[Top](#)

unbind appflow policylabel

Synopsis

unbind appflow policylabel <labelName> <policyName> [-priority <positive_integer>]

Description

Unbinds an AppFlow policy from an AppFlow policy label.

Parameters

labelName

Name of the policy label from which to unbind a policy.

policyName

Name of the policy to unbind.

Example

```
unbind appflow policylabel appflow_pol_label  
appflow_pol
```

[Top](#)

rename appflow policylabel

Synopsis

rename appflow policylabel <labelName>@ <newName>@

Description

Renames an AppFlow policy label.

Parameters

labelName

Existing name of the policylabel.

newName

New name for the policy label. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my appflow policylabel" or 'my appflow policylabel')

Example

```
rename appflow policylabel old_name new_name
```

[Top](#)**show appflow policylabel****Synopsis**

```
show appflow policylabel [<labelName>]
```

Description

Displays information about all AppFlow policy labels, or detailed information about the specified policy label.

Parameters

labelName

Name of the policy label about which to display detailed information.

Example

```
i)    show appflow policylabel appflow_pol_label
ii)   show appflow policylabel
```

[Top](#)**appflow param**

[[set](#) | [unset](#) | [show](#)]

set appflow param**Synopsis**

```
set appflow param [-templateRefresh <secs>] [-appnameRefresh <secs>] [-flowRecordInterval <secs>] [-udpPmtu <positive_integer>] [-httpUrl ( ENABLED | DISABLED )] [-AAAUUserName ( ENABLED | DISABLED )] [-httpCookie ( ENABLED | DISABLED )] [-httpReferer ( ENABLED | DISABLED )] [-httpMethod ( ENABLED | DISABLED )] [-httpHost ( ENABLED | DISABLED )] [-httpUserAgent ( ENABLED | DISABLED )] [-clientTrafficOnly ( YES | NO )] [-httpContentType ( ENABLED | DISABLED )] [-httpAuthorization ( ENABLED | DISABLED )] [-httpVia ( ENABLED | DISABLED )] [-httpXForwardedFor ( ENABLED | DISABLED )] [-httpLocation ( ENABLED | DISABLED )] [-httpSetCookie ( ENABLED | DISABLED )] [-httpSetCookie2 ( ENABLED | DISABLED )] [-connectionChaining ( ENABLED | DISABLED )]
```

Description

Configures AppFlow parameters.

Parameters

templateRefresh

Refresh interval, in seconds, at which to export the template data. Because data transmission is in UDP, the templates must be resent at regular intervals. Default value: 600 Minimum value: 60 Maximum value: 3600

appnameRefresh

Interval, in seconds, at which to send Appnames to the configured collectors. Appname refers to the name of an entity (virtual server, service, or service group) in the NetScaler appliance. Default value: 600 Minimum value: 60 Maximum value: 3600

flowRecordInterval

Interval, in seconds, at which to send flow records to the configured collectors. Default value: 60 Minimum value: 60 Maximum value: 3600

udpPmtu

MTU, in bytes, for IPFIX UDP packets. Default value: 1472 Minimum value: 128 Maximum value: 1472

httpUrl

Include the http URL that the NetScaler appliance received from the client. Possible values: ENABLED, DISABLED Default value: DISABLED

AAAUserName

Enable AppFlow AAA Username logging. Possible values: ENABLED, DISABLED Default value: DISABLED

httpCookie

Include the cookie that was in the HTTP request the appliance received from the client. Possible values: ENABLED, DISABLED Default value: DISABLED

httpReferer

Include the web page that was last visited by the client. Possible values: ENABLED, DISABLED Default value: DISABLED

httpMethod

Include the method that was specified in the HTTP request that the appliance received from the client. Possible values: ENABLED, DISABLED Default value: DISABLED

httpHost

Include the host identified in the HTTP request that the appliance received from the client. Possible values: ENABLED, DISABLED Default value: DISABLED

httpUserAgent

Include the client application through which the HTTP request was received by the NetScaler appliance. Possible values: ENABLED, DISABLED Default value: DISABLED

clientTrafficOnly

Generate AppFlow records for only the traffic from the client. Possible values: YES, NO Default value: NO

httpContentType

Include the HTTP Content-Type header sent from the server to the client to determine the type of the content sent. Possible values: ENABLED, DISABLED Default value: DISABLED

httpAuthorization

Include the HTTP Authorization header information. Possible values: ENABLED, DISABLED Default value: DISABLED

httpVia

Include the httpVia header which contains the IP address of proxy server through which the client accessed the server. Possible values: ENABLED, DISABLED Default value: DISABLED

httpXForwardedFor

Include the httpXForwardedFor header, which contains the original IP Address of the client using a proxy server to access the server. Possible values: ENABLED, DISABLED Default value: DISABLED

httpLocation

Include the HTTP location headers returned from the HTTP responses. Possible values: ENABLED, DISABLED Default value: DISABLED

httpSetCookie

Include the Set-cookie header sent from the server to the client in response to a HTTP request. Possible values: ENABLED, DISABLED Default value: DISABLED

httpSetCookie2

Include the Set-cookie header sent from the server to the client in response to a HTTP request. Possible values: ENABLED, DISABLED Default value: DISABLED

connectionChaining

Enable connection chaining so that the client server flows of a connection are linked. Also the connection chain ID is propagated across NetScalers, so that in a multi-hop environment the flows belonging to the same logical connection are linked. This id is also logged as part of appflow record Possible values: ENABLED, DISABLED Default value: DISABLED

Example

```
set appflow param -templateRefresh 240
```

[Top](#)

unset appflow param**Synopsis**

```
unset appflow param [-templateRefresh] [-appnameRefresh] [-flowRecordInterval] [-udpPmtu] [-httpUrl] [-AAAUserName] [-httpCookie] [-httpReferer] [-httpMethod] [-httpHost] [-httpUserAgent] [-clientTrafficOnly] [-httpContentType] [-httpAuthorization] [-httpVia] [-httpXForwardedFor] [-httpLocation] [-httpSetCookie] [-httpSetCookie2] [-connectionChaining]
```

Description

Use this command to remove appflow param settings. Refer to the set appflow param command for meanings of the arguments.

[Top](#)

show appflow param

Synopsis

show appflow param

Description

Displays AppFlow parameters.

[Top](#)

appflow global

[[bind](#) | [unbind](#) | [show](#)]

bind appflow global

Synopsis

bind appflow global <policyName> <priority> [<gotoPriorityExpression>] [-type <type>]
[-invoke (<labelType> <labelName>)]

Description

Binds the AppFlow policy to one of the two global lists of AppFlow policies. A policy becomes active only after it is bound.

Parameters

policyName

Name of the AppFlow policy to be bound.

Example

```
i)      bind appflow global pol9 9
ii)     bind appflow global pol9 9 120
iii)    bind appflow global pol9 9
"HTTP.REQ.HEADER(\\\"qh3\
\").TYPECAST_NUM_T(DECIMAL) "
```

[Top](#)

unbind appflow global

Synopsis

unbind appflow global (<policyName> [-type <type>] [-priority <positive_integer>])

Description

Unbinds entities from an AppFlow global bind point.

Parameters

policyName

Name of the policy to be unbound.

Example

```
unbind appflow global pol9
```

[Top](#)

show appflow global

Synopsis

show appflow global [-type <type>]

Description

Displays the AppFlow global bind points and the number of policies bound to each global bind point, or more detailed information about the specified bind point.

Parameters

type

Global bind point for which to show detailed information about the policies bound to the bind point. Possible values: REQ_OVERRIDE, REQ_DEFAULT, OVERRIDE, DEFAULT, OTHERTCP_REQ_OVERRIDE, OTHERTCP_REQ_DEFAULT, MSSQL_REQ_OVERRIDE, MSSQL_REQ_DEFAULT, MYSQL_REQ_OVERRIDE, MYSQL_REQ_DEFAULT, ICA_REQ_OVERRIDE, ICA_REQ_DEFAULT, ORACLE_REQ_OVERRIDE, ORACLE_REQ_DEFAULT

Example

```
show appflow global
```

[Top](#)

Application Firewall Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [appfw](#)
- ♦ [appfw fieldType](#)
- ♦ [appfw profile](#)

- ♦ [appfw policy](#)
- ♦ [appfw policylabel](#)
- ♦ [appfw confidField](#)
- ♦ [appfw stats](#)
- ♦ [appfw xmlerrorpage](#)
- ♦ [appfw htmlerrorpage](#)
- ♦ [appfw settings](#)
- ♦ [appfw transactionRecords](#)
- ♦ [appfw global](#)
- ♦ [appfw learningsettings](#)
- ♦ [appfw learningdata](#)
- ♦ [appfw JSONContentType](#)
- ♦ [appfw wsdl](#)
- ♦ [appfw signatures](#)
- ♦ [appfw xmlschema](#)
- ♦ [appfw XMLContentType](#)
- ♦ [appfw archive](#)

appfw

stat appfw

Synopsis

```
stat appfw [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile  
<input_filename>] [-clearstats ( basic | full )]
```

Description

Displays application firewall statistics.

Parameters

clearstats

Clear the statistics / counters Possible values: basic, full

appfw fieldType

[[add](#) | [rm](#) | [set](#) | [show](#)]

add appfw fieldType

Synopsis

add appfw fieldType <name> <regex> <priority> [-comment <string>]

Description

Adds a field type to the list of field types used by the field format security check. A field type is a regular expression defining the type of data that can appear in a web form field. The Learning engine also uses the field types list to generate appropriate field type assignments for the field formats check.

Parameters

name

Name for the field type. Must begin with a letter, number, or the underscore character \(_ \), and must contain only letters, numbers, and the hyphen \(- \), period \(. \), pound \(\# \), space \(\ \), at \(@ \), equals \(= \), colon \(: \), and underscore characters. Cannot be changed after the field type is added. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks \("my field type" or 'my field type' \).

regex

PCRE - format regular expression defining the characters and length allowed for this field type.

priority

Positive integer specifying the priority of the field type. A lower number specified a higher priority. Field types are checked in the order of their priority numbers.
Maximum value: 64000

comment

Comment describing the type of field that this field type is intended to match.

[Top](#)

rm appfw fieldType

Synopsis

rm appfw fieldType <name>

Description

Removes an application firewall field type.

Parameters

name

Name of the field type.

[Top](#)

set appfw fieldType

Synopsis

set appfw fieldType <name> <regex> <priority> [-comment <string>]

Description

Modifies the properties of the specified application firewall field type.

Parameters

name

Name for the field type. Must begin with a letter, number, or the underscore character \(_\\), and must contain only letters, numbers, and the hyphen \(-\\), period \(.\\) pound \(\#\\), space \(\ \\), at \(\@\\), equals \(\=\\), colon \(:\\), and underscore characters. Cannot be changed after the field type is added. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks \("my field type" or 'my field type'\\).

regex

PCRE - format regular expression defining the characters and length allowed for this field type.

[Top](#)

show appfw fieldType

Synopsis

show appfw fieldType [<name>]

Description

Displays the regular expression that defines the specified field type and its priority. If no field type is specified, displays all form field types currently configured on the NetScaler appliance.

Parameters

name

Name of the field type.

[Top](#)

appfw profile

[[add](#) | [rm](#) | [set](#) | [unset](#) | [bind](#) | [unbind](#) | [show](#) | [stat](#) | [archive](#) | [restore](#)]

add appfw profile

Synopsis

add appfw profile <name> [-defaults (basic | advanced)] [-startURLAction <startURLAction> ...] [-startURLClosure (ON | OFF)] [-denyURLAction <denyURLAction> ...] [-RefererHeaderCheck <RefererHeaderCheck>] [-

```

cookieConsistencyAction <cookieConsistencyAction> ...] [-cookieTransforms ( ON |
OFF )] [-cookieEncryption <cookieEncryption>] [-cookieProxying ( none | sessionOnly )]
[-addCookieFlags <addCookieFlags>] [-fieldConsistencyAction
<fieldConsistencyAction> ...] [-CSRFtagAction <CSRFtagAction> ...] [-
crossSiteScriptingAction <crossSiteScriptingAction> ...] [-
crossSiteScriptingTransformUnsafeHTML ( ON | OFF )] [-
crossSiteScriptingCheckCompleteURLs ( ON | OFF )] [-SQLInjectionAction
<SQLInjectionAction> ...] [-SQLInjectionTransformSpecialChars ( ON | OFF )] [-
SQLInjectionOnlyCheckFieldsWithSQLChars ( ON | OFF )] [-fieldFormatAction
<fieldFormatAction> ...] [-defaultFieldFormatType <string>] [-
defaultFieldFormatMinLength <positive_integer>] [-defaultFieldFormatMaxLength
<positive_integer>] [-bufferOverflowAction <bufferOverflowAction> ...] [-
bufferOverflowMaxURLLength <positive_integer>] [-bufferOverflowMaxHeaderLength
<positive_integer>] [-bufferOverflowMaxCookieLength <positive_integer>] [-
creditCardAction <creditCardAction> ...] [-creditCard <creditCard> ...] [-
creditCardMaxAllowed <positive_integer>] [-creditCardXOut ( ON | OFF )] [-
requestContentType <string>] [-responseContentType <string>] [-XMLDoSAction
<XMLDoSAction> ...] [-XMLFormatAction <XMLFormatAction> ...] [-
XMLSQLInjectionAction <XMLSQLInjectionAction> ...] [-
XMLSQLInjectionOnlyCheckFieldsWithSQLChars ( ON | OFF )] [-
XMLSQLInjectionParseComments <XMLSQLInjectionParseComments>] [-XMLXSSAction
<XMLXSSAction> ...] [-XMLWSIAction <XMLWSIAction> ...] [-XMLAttachmentAction
<XMLAttachmentAction> ...] [-XMLValidationAction <XMLValidationAction> ...] [-
XMLErrorObject <string>] [-signatures <string>] [-XMLSOAPFaultAction
<XMLSOAPFaultAction> ...] [-useHTMLErrorObject ( ON | OFF )] [-errorURL
<expression>] [-HTMLErrorObject <string>] [-logEveryPolicyHit ( ON | OFF )] [-
stripHtmlComments <stripHtmlComments>] [-stripXmlComments ( none | all )] [-
exemptClosureURLsFromSecurityChecks ( ON | OFF )] [-defaultCharSet <string>] [-
postBodyLimit <positive_integer>] [-fileUploadMaxNum <positive_integer>] [-
canonicalizeHTMLResponse ( ON | OFF )] [-enableFormTagging ( ON | OFF )] [-
sessionlessFieldConsistency <sessionlessFieldConsistency>] [-sessionlessURLClosure ( ON
| OFF )] [-semicolonFieldSeparator ( ON | OFF )] [-excludeFileUploadFromChecks ( ON |
OFF )] [-SQLInjectionParseComments <SQLInjectionParseComments>] [-
invalidPercentHandling <invalidPercentHandling>] [-type ( HTML | XML ) ...] [-
checkRequestHeaders ( ON | OFF )] [-comment <string>]

```

Description

Creates an application firewall profile, which specifies how the application firewall should protect a given type of web content. (A profile is equivalent to an action in other NetScaler features.)

Parameters

name

Name for the profile. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.), pound (#), space (), at (@), equals (=), colon (:), and underscore (_) characters. Cannot be changed after the profile is added. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my profile" or 'my profile').

defaults

Default configuration to apply to the profile. Basic defaults are intended for standard content that requires little further configuration, such as static web site content. Advanced defaults are intended for specialized content that requires significant specialized configuration, such as heavily scripted or dynamic content. CLI users: When adding an application firewall profile, you can set either the defaults or the type, but not both. To set both options, create the profile by using the add appfw profile command, and then use the set appfw profile command to configure the other option. Possible values: basic, advanced

builtin

Indicates that a profile is a built-in entity.

builtinType

Type of built-in profile. Determines which security checks and settings are used for the profile. (The type specified by the HTML XML setting is also called "Web 2.0.") CLI users: When adding an application firewall profile, you can set either the defaults or the type, but not both. To set both options, create the profile by using the add appfw profile command, and then use the set appfw profile command to configure the other option. Possible values: APPFW_NOT_BUILTIN, APPFW_BYPASS, APPFW_BLOCK, APPFW_RESET, APPFW_DROP

startURLAction

One or more Start URL actions. Available settings function as follows: * Block - Block connections that violate this security check. * Learn - Use the learning engine to generate a list of exceptions to this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -startURLAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -startURLAction none". Default value: AS_DEFAULT_DISPOSITION

startURLClosure

Toggle the state of Start URL Closure. Possible values: ON, OFF Default value: OFF

denyURLAction

One or more Deny URL actions. Available settings function as follows: * Block - Block connections that violate this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. NOTE: The Deny URL check takes precedence over the Start URL check. If you enable blocking for the Deny URL check, the application firewall blocks any URL that is explicitly blocked by a Deny URL, even if the same URL would otherwise be allowed by the Start URL check. CLI users: To enable one or more actions, type "set appfw profile -denyURLAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -denyURLAction none". Default value: AS_DEFAULT_DISPOSITION

RefererHeaderCheck

Enable validation of Referer headers. Referer validation ensures that a web form that a user sends to your web site originally came from your web site, not an outside attacker. Although this parameter is part of the Start URL check, referer validation

protects against cross-site request forgery (CSRF) attacks, not Start URL attacks.
Possible values: OFF, if_present, always Default value: AS_HEADER_CHECK_OFF

cookieConsistencyAction

One or more Cookie Consistency actions. Available settings function as follows: * Block - Block connections that violate this security check. * Learn - Use the learning engine to generate a list of exceptions to this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -cookieConsistencyAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -cookieConsistencyAction none". Default value: AS_NONE

cookieTransforms

Perform the specified type of cookie transformation. Available settings function as follows: * Encryption - Encrypt cookies. * Proxying - Mask contents of server cookies by sending proxy cookie to users. * Cookie flags - Flag cookies as HTTP only to prevent scripts on user's browser from accessing and possibly modifying them. CAUTION: Make sure that this parameter is set to ON if you are configuring any cookie transformations. If it is set to OFF, no cookie transformations are performed regardless of any other settings. Possible values: ON, OFF Default value: OFF

cookieEncryption

Type of cookie encryption. Available settings function as follows: * None - Do not encrypt cookies. * Decrypt Only - Decrypt encrypted cookies, but do not encrypt cookies. * Encrypt Session Only - Encrypt session cookies, but not permanent cookies. * Encrypt All - Encrypt all cookies. Possible values: none, decryptOnly, encryptSessionOnly, encryptAll Default value: AS_CKI_ENCRYPT_NONE

cookieProxying

Cookie proxy setting. Available settings function as follows: * None - Do not proxy cookies. * Session Only - Proxy session cookies by using the NetScaler session ID, but do not proxy permanent cookies. Possible values: none, sessionOnly Default value: AS_CKI_PROXY_NONE

addCookieFlags

Add the specified flags to cookies. Available settings function as follows: * None - Do not add flags to cookies. * HTTP Only - Add the HTTP Only flag to cookies, which prevents scripts from accessing cookies. * Secure - Add Secure flag to cookies. * All - Add both HTTPOnly and Secure flags to cookies. Possible values: none, httpOnly, secure, all Default value: AS_ADD_CKI_FLAGS_NONE

fieldConsistencyAction

One or more Form Field Consistency actions. Available settings function as follows: * Block - Block connections that violate this security check. * Learn - Use the learning engine to generate a list of exceptions to this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -fieldConsistencyaction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -fieldConsistencyAction none". Default value: AS_NONE

CSRFtagAction

One or more Cross-Site Request Forgery (CSRF) Tagging actions. Available settings function as follows: * Block - Block connections that violate this security check. * Learn - Use the learning engine to generate a list of exceptions to this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -CSRFtagAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -CSRFtagAction none". Default value: AS_NONE

crossSiteScriptingAction

One or more Cross-Site Scripting (XSS) actions. Available settings function as follows: * Block - Block connections that violate this security check. * Learn - Use the learning engine to generate a list of exceptions to this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -crossSiteScriptingAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -crossSiteScriptingAction none". Default value: AS_DEFAULT_DISPOSITION

crossSiteScriptingTransformUnsafeHTML

Transform cross-site scripts. This setting configures the application firewall to disable dangerous HTML instead of blocking the request. CAUTION: Make sure that this parameter is set to ON if you are configuring any cross-site scripting transformations. If it is set to OFF, no cross-site scripting transformations are performed regardless of any other settings. Possible values: ON, OFF Default value: OFF

crossSiteScriptingCheckCompleteURLs

Check complete URLs for cross-site scripts, instead of just the query portions of URLs. Possible values: ON, OFF Default value: OFF

SQLInjectionAction

One or more HTML SQL Injection actions. Available settings function as follows: * Block - Block connections that violate this security check. * Learn - Use the learning engine to generate a list of exceptions to this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -SQLInjectionAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -SQLInjectionAction none". Default value: AS_DEFAULT_DISPOSITION

SQLInjectionTransformSpecialChars

Transform injected SQL code. This setting configures the application firewall to disable SQL special strings instead of blocking the request. Since most SQL servers require a special string to activate an SQL keyword, in most cases a request that contains injected SQL code is safe if special strings are disabled. CAUTION: Make sure that this parameter is set to ON if you are configuring any SQL injection transformations. If it is set to OFF, no SQL injection transformations are performed regardless of any other settings. Possible values: ON, OFF Default value: OFF

SQLInjectionOnlyCheckFieldsWithSQLChars

Check only form fields that contain SQL special strings (characters) for injected SQL code. Most SQL servers require a special string to activate an SQL request, so SQL

code without a special string is harmless to most SQL servers. Possible values: ON, OFF Default value: ON

fieldFormatAction

One or more Field Format actions. Available settings function as follows: * Block - Block connections that violate this security check. * Learn - Use the learning engine to generate a list of suggested web form fields and field format assignments. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -fieldFormatAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -fieldFormatAction none". Default value: AS_DEFAULT_DISPOSITION

defaultFieldFormatType

Designate a default field type to be applied to web form fields that do not have a field type explicitly assigned to them.

defaultFieldFormatMinLength

Minimum length, in characters, for data entered into a field that is assigned the default field type. To disable the minimum and maximum length settings and allow data of any length to be entered into the field, set this parameter to zero (0). Default value: AS_DEFAULTFIELDFORMAT_DEFAULT_MIN_LEN Minimum value: 0 Maximum value: 65535

defaultFieldFormatMaxLength

Maximum length, in characters, for data entered into a field that is assigned the default field type. Default value: AS_DEFAULTFIELDFORMAT_DEFAULT_MAX_LEN Minimum value: 1 Maximum value: 65535

bufferOverflowAction

One or more Buffer Overflow actions. Available settings function as follows: * Block - Block connections that violate this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -bufferOverflowAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -bufferOverflowAction none". Default value: AS_DEFAULT_DISPOSITION

bufferOverflowMaxURLLength

Maximum length, in characters, for URLs on your protected web sites. Requests with longer URLs are blocked. Default value: AS_BUFFEROVERFLOW_DEFAULT_MAX_URL_LEN Minimum value: 0 Maximum value: 65535

bufferOverflowMaxHeaderLength

Maximum length, in characters, for HTTP headers in requests sent to your protected web sites. Requests with longer headers are blocked. Default value: AS_BUFFEROVERFLOW_DEFAULT_MAX_HDR_LEN Minimum value: 0 Maximum value: 65535

bufferOverflowMaxCookieLength

Maximum length, in characters, for cookies sent to your protected web sites. Requests with longer cookies are blocked. Default value:

AS_BUFFEROVERFLOW_DEFAULT_MAX_COOKIE_LEN Minimum value: 0 Maximum value: 65535

creditCardAction

One or more Credit Card actions. Available settings function as follows: * Block - Block connections that violate this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -creditCardAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -creditCardAction none". Default value: AS_NONE

creditCard

Credit card types that the application firewall should protect. Default value: AS_CCARD_DEFAULT_CARD_TYPE

creditCardMaxAllowed

Maximum number of credit card numbers that can appear on a web page served by your protected web sites. Pages that contain more credit card numbers are blocked, or the credit card numbers are masked. Maximum value: 255

creditCardXOut

Mask any credit card number detected in a response by replacing each digit, except the digits in the final group, with the letter "X." Possible values: ON, OFF Default value: OFF

requestContentType

Default Content-Type header for requests. A Content-Type header can contain 0-255 letters, numbers, and the hyphen (-) and underscore (_) characters. Default value: NS_S_AS_DEFAULT_REQUEST_CONTENT_TYPE

responseContentType

Default Content-Type header for responses. A Content-Type header can contain 0-255 letters, numbers, and the hyphen (-) and underscore (_) characters. Default value: NS_S_AS_DEFAULT_RESPONSE_CONTENT_TYPE

XMLDoSAction

One or more XML Denial-of-Service (XDoS) actions. Available settings function as follows: * Block - Block connections that violate this security check. * Learn - Use the learning engine to generate a list of exceptions to this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -XMLDoSAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLDoSAction none". Default value: AS_DEFAULT_DISPOSITION

XMLFormatAction

One or more XML Format actions. Available settings function as follows: * Block - Block connections that violate this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -XMLFormatAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLFormatAction none". Default value: AS_DEFAULT_DISPOSITION

XMLSQLInjectionAction

One or more XML SQL Injection actions. Available settings function as follows: * Block - Block connections that violate this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -XMLSQLInjectionAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLSQLInjectionAction none". Default value: AS_DEFAULT_DISPOSITION

XMLSQLInjectionOnlyCheckFieldsWithSQLChars

Check only form fields that contain SQL special characters, which most SQL servers require before accepting an SQL command, for injected SQL. Possible values: ON, OFF Default value: ON

XMLSQLInjectionParseComments

Parse comments in XML Data and exempt those sections of the request that are from the XML SQL Injection check. You must configure the type of comments that the application firewall is to detect and exempt from this security check. Available settings function as follows: * Check all - Check all content. * ANSI - Exempt content that is part of an ANSI (Mozilla-style) comment. * Nested - Exempt content that is part of a nested (Microsoft-style) comment. * ANSI Nested - Exempt content that is part of any type of comment. Possible values: checkall, ansi, nested, ansinested Default value: AS_CHECKALL

XMLXSSAction

One or more XML Cross-Site Scripting actions. Available settings function as follows: * Block - Block connections that violate this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -XMLXSSAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLXSSAction none". Default value: AS_DEFAULT_DISPOSITION

XMLWSIAction

One or more Web Services Interoperability (WSI) actions. Available settings function as follows: * Block - Block connections that violate this security check. * Learn - Use the learning engine to generate a list of exceptions to this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -XMLWSIAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLWSIAction none". Default value: AS_DEFAULT_DISPOSITION

XMLAttachmentAction

One or more XML Attachment actions. Available settings function as follows: * Block - Block connections that violate this security check. * Learn - Use the learning engine to generate a list of exceptions to this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -XMLAttachmentAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLAttachmentAction none". Default value: AS_DEFAULT_DISPOSITION

XMLValidationAction

One or more XML Validation actions. Available settings function as follows: * Block - Block connections that violate this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -XMLValidationAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLValidationAction none". Default value: AS_DEFAULT_DISPOSITION

XMLErrorObject

Name to assign to the XML Error Object, which the application firewall displays when a user request is blocked. Must begin with a letter, number, or the underscore character \(_\), and must contain only letters, numbers, and the hyphen \(-\), period \(.\) pound \(\#\), space \(\), at \(@\), equals \(\=\), colon \(:\) and underscore characters. Cannot be changed after the XML error object is added. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks \("my XML error object" or 'my XML error object'\). Default value: NS_S_AS_ERROR_OBJECT_DEFAULT

customSettings

Object name for custom settings. This check is applicable to Profile Type: HTML, XML. Default value: NS_S_AS_CUSTOM_OBJECT_DEFAULT

signatures

Object name for signatures. This check is applicable to Profile Type: HTML, XML. Default value: NS_S_AS_CUSTOM_OBJECT_DEFAULT

XMLSOAPFaultAction

One or more XML SOAP Fault Filtering actions. Available settings function as follows: * Block - Block connections that violate this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. * Remove - Remove all violations for this security check. CLI users: To enable one or more actions, type "set appfw profile -XMLSOAPFaultAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLSOAPFaultAction none". Default value: AS_DEFAULT_DISPOSITION

useHTMLErrorObject

Send an imported HTML Error object to a user when a request is blocked, instead of redirecting the user to the designated Error URL. Possible values: ON, OFF Default value: OFF

errorURL

URL that application firewall uses as the Error URL. Default value: NS_S_AS_ERROR_URL_DEFAULT

HTMLErrorObject

Name to assign to the HTML Error Object. Must begin with a letter, number, or the underscore character \(_\), and must contain only letters, numbers, and the hyphen \(-\), period \(.\) pound \(\#\), space \(\), at \(@\), equals \(\=\), colon \(:\) and underscore characters. Cannot be changed after the HTML error object is added. The following requirement applies only to the NetScaler CLI: If the name includes one or

more spaces, enclose the name in double or single quotation marks \ (for example, "my HTML error object" or 'my HTML error object\'). Default value:
NS_S_AS_ERROR_OBJECT_DEFAULT

logEveryPolicyHit

Log every profile match, regardless of security checks results. Possible values: ON, OFF Default value: OFF

stripComments

Strip HTML comments. This check is applicable to Profile Type: HTML. Possible values: ON, OFF Default value: OFF

stripHtmlComments

Strip HTML comments before forwarding a web page sent by a protected web site in response to a user request. Possible values: none, all, exclude_script_tag Default value: AS_STRIP_COMMENT_NONE

stripXmlComments

Exempt URLs that pass the Start URL closure check from additional security checks. Possible values: none, all Default value: AS_STRIP_COMMENT_NONE

exemptClosureURLsFromSecurityChecks

Exempt URLs that pass the Start URL closure check from additional security checks. Possible values: ON, OFF Default value: ON

defaultCharSet

Default character set for protected web pages. Web pages sent by your protected web sites in response to user requests are assigned this character set if the page does not already specify a character set. The character sets supported by the application firewall are: * iso-8859-1 (English US) * big5 (Chinese Traditional) * gb2312 (Chinese Simplified) * sjis (Japanese Shift-JIS) * euc-jp (Japanese EUC-JP) * iso-8859-9 (Turkish) * utf-8 (Unicode) * euc-kr (Korean) Default value:
NS_S_AS_CHARSET_DEFAULT Maximum value: 31

postBodyLimit

Maximum allowed HTTP post body size, in bytes. Default value:
AS_DEFAULT_POSTBODYLIMIT Maximum value: 1000000000

fileUploadMaxNum

Maximum allowed number of file uploads per form-submission request. The maximum setting (65535) allows an unlimited number of uploads. Default value:
AS_DEFAULT_MAX_FILE_UPLOADS Maximum value: 65535

canonicalizeHTMLResponse

Perform HTML entity encoding for any special characters in responses sent by your protected web sites. Possible values: ON, OFF Default value: ON

enableFormTagging

Enable tagging of web form fields for use by the Form Field Consistency and CSRF Form Tagging checks. Possible values: ON, OFF Default value: ON

sessionlessFieldConsistency

Perform sessionless Field Consistency Checks. Possible values: OFF, ON, postOnly Default value: AS_OFF

sessionlessURLClosure

Enable session less URL Closure Checks. This check is applicable to Profile Type: HTML. Possible values: ON, OFF Default value: OFF

semicolonFieldSeparator

Allow ';' as a form field separator in URL queries and POST form bodies. Possible values: ON, OFF Default value: OFF

excludeFileUploadFromChecks

Exclude uploaded files from Form checks. Possible values: ON, OFF Default value: OFF

SQLInjectionParseComments

Parse HTML comments and exempt them from the HTML SQL Injection check. You must specify the type of comments that the application firewall is to detect and exempt from this security check. Available settings function as follows: * Check all - Check all content. * ANSI - Exempt content that is part of an ANSI (Mozilla-style) comment. * Nested - Exempt content that is part of a nested (Microsoft-style) comment. * ANSI Nested - Exempt content that is part of any type of comment. Possible values: checkall, ansi, nested, ansinested Default value: AS_DEFAULT_SQLINJECTIONPARSECOMMENTS

invalidPercentHandling

Configure the method that the application firewall uses to handle percent-encoded names and values. Available settings function as follows: * apache_mode - Apache format. * asp_mode - Microsoft ASP format. * secure_mode - Secure format. Possible values: apache_mode, asp_mode, secure_mode Default value: AS_PERCENT_DECODE_SECURE_MODE

type

Application firewall profile type, which controls which security checks and settings are applied to content that is filtered with the profile. Available settings function as follows: * HTML - HTML-based web sites. * XML - XML-based web sites and services. * HTML XML (Web 2.0) - Sites that contain both HTML and XML content, such as ATOM feeds, blogs, and RSS feeds. Default value: AF_PROFILE_TYPE_HTML

checkRequestHeaders

Check request headers as well as web forms for injected SQL and cross-site scripts. Possible values: ON, OFF Default value: OFF

comment

Any comments about the purpose of profile, or other useful information about the profile.

[Top](#)

rm appfw profile

Synopsis

rm appfw profile <name>

Description

Removes the specified application firewall profile.

Parameters

name

Name of the profile.

[Top](#)

set appfw profile

Synopsis

```
set appfw profile <name> [-startURLAction <startURLAction> ...] [-startURLClosure ( ON
| OFF )] [-denyURLAction <denyURLAction> ...] [-RefererHeaderCheck
<RefererHeaderCheck>] [-cookieConsistencyAction <cookieConsistencyAction> ...] [-
cookieTransforms ( ON | OFF )] [-cookieEncryption <cookieEncryption>] [-
cookieProxying ( none | sessionOnly )] [-addCookieFlags <addCookieFlags>] [-
fieldConsistencyAction <fieldConsistencyAction> ...] [-CSRFtagAction
<CSRFtagAction> ...] [-crossSiteScriptingAction <crossSiteScriptingAction> ...] [-
crossSiteScriptingTransformUnsafeHTML ( ON | OFF )] [-
crossSiteScriptingCheckCompleteURLs ( ON | OFF )] [-SQLInjectionAction
<SQLInjectionAction> ...] [-SQLInjectionTransformSpecialChars ( ON | OFF )] [-
SQLInjectionOnlyCheckFieldsWithSQLChars ( ON | OFF )] [-fieldFormatAction
<fieldFormatAction> ...] [-defaultFieldFormatType <string>] [-
defaultFieldFormatMinLength <positive_integer>] [-defaultFieldFormatMaxLength
<positive_integer>] [-bufferOverflowAction <bufferOverflowAction> ...] [-
bufferOverflowMaxURLLength <positive_integer>] [-bufferOverflowMaxHeaderLength
<positive_integer>] [-bufferOverflowMaxCookieLength <positive_integer>] [-
creditCardAction <creditCardAction> ...] [-creditCard <creditCard> ...] [-
creditCardMaxAllowed <positive_integer>] [-creditCardXOut ( ON | OFF )] [-
requestContentType <string>] [-responseContentType <string>] [-XMLDoSAction
<XMLDoSAction> ...] [-XMLFormatAction <XMLFormatAction> ...] [-
XMLSQLInjectionAction <XMLSQLInjectionAction> ...] [-
XMLSQLInjectionOnlyCheckFieldsWithSQLChars ( ON | OFF )] [-
XMLSQLInjectionParseComments <XMLSQLInjectionParseComments>] [-XMLXSSAction
<XMLXSSAction> ...] [-XMLWSIAction <XMLWSIAction> ...] [-XMLAttachmentAction
<XMLAttachmentAction> ...] [-XMLValidationAction <XMLValidationAction> ...] [-
XMLErrorObject <string>] [-signatures <string>] [-XMLSOAPFaultAction
<XMLSOAPFaultAction> ...] [-useHTMLErrorObject ( ON | OFF )] [-errorURL
<expression>] [-HTMLErrorObject <string>] [-logEveryPolicyHit ( ON | OFF )] [-
stripHtmlComments <stripHtmlComments>] [-stripXmlComments ( none | all )] [-
exemptClosureURLsFromSecurityChecks ( ON | OFF )] [-defaultCharSet <string>] [-
postBodyLimit <positive_integer>] [-fileUploadMaxNum <positive_integer>] [-
canonicalizeHTMLResponse ( ON | OFF )] [-enableFormTagging ( ON | OFF )] [-
sessionlessFieldConsistency <sessionlessFieldConsistency>] [-sessionlessURLClosure ( ON
| OFF )] [-semicolonFieldSeparator ( ON | OFF )] [-excludeFileUploadFromChecks ( ON |
OFF )] [-SQLInjectionParseComments <SQLInjectionParseComments>] [-
invalidPercentHandling <invalidPercentHandling>] [-type ( HTML | XML ) ...] [-
checkRequestHeaders ( ON | OFF )] [-comment <string>]
```

Description

Modifies the specified parameters of the specified application firewall profile.

Parameters

name

Name of the profile that you want to modify.

startURLAction

One or more Start URL actions. Available settings function as follows: * Block - Block connections that violate this security check. * Learn - Use the learning engine to generate a list of exceptions to this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -startURLAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -startURLAction none". Default value: AS_DEFAULT_DISPOSITION

startURLClosure

Toggle the state of Start URL Closure. Possible values: ON, OFF Default value: OFF

denyURLAction

One or more Deny URL actions. Available settings function as follows: * Block - Block connections that violate this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. NOTE: The Deny URL check takes precedence over the Start URL check. If you enable blocking for the Deny URL check, the application firewall blocks any URL that is explicitly blocked by a Deny URL, even if the same URL would otherwise be allowed by the Start URL check. CLI users: To enable one or more actions, type "set appfw profile -denyURLAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -denyURLAction none". Default value: AS_DEFAULT_DISPOSITION

RefererHeaderCheck

Enable validation of Referer headers. Referer validation ensures that a web form that a user sends to your web site originally came from your web site, not an outside attacker. Although this parameter is part of the Start URL check, referer validation protects against cross-site request forgery (CSRF) attacks, not Start URL attacks. Possible values: OFF, if_present, always Default value: AS_HEADER_CHECK_OFF

cookieConsistencyAction

One or more Cookie Consistency actions. Available settings function as follows: * Block - Block connections that violate this security check. * Learn - Use the learning engine to generate a list of exceptions to this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -cookieConsistencyAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -cookieConsistencyAction none". Default value: AS_NONE

cookieTransforms

Perform the specified type of cookie transformation. Available settings function as follows: * Encryption - Encrypt cookies. * Proxying - Mask contents of server cookies by sending proxy cookie to users. * Cookie flags - Flag cookies as HTTP only to prevent scripts on user's browser from accessing and possibly modifying them. CAUTION: Make sure that this parameter is set to ON if you are configuring any

cookie transformations. If it is set to OFF, no cookie transformations are performed regardless of any other settings. Possible values: ON, OFF

cookieEncryption

Type of cookie encryption. Available settings function as follows: * None - Do not encrypt cookies. * Decrypt Only - Decrypt encrypted cookies, but do not encrypt cookies. * Encrypt Session Only - Encrypt session cookies, but not permanent cookies. * Encrypt All - Encrypt all cookies. Possible values: none, decryptOnly, encryptSessionOnly, encryptAll Default value: AS_CKI_ENCRYPT_NONE

cookieProxying

Cookie proxy setting. Available settings function as follows: * None - Do not proxy cookies. * Session Only - Proxy session cookies by using the NetScaler session ID, but do not proxy permanent cookies. Possible values: none, sessionOnly Default value: AS_CKI_PROXY_NONE

addCookieFlags

Add HttpOnly and Secure flags to cookies Possible values: none, httpOnly, secure, all Default value: AS_ADD_CKI_FLAGS_NONE

fieldConsistencyAction

One or more Form Field Consistency actions. Available settings function as follows: * Block - Block connections that violate this security check. * Learn - Use the learning engine to generate a list of exceptions to this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -fieldConsistencyaction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -fieldConsistencyAction none". Default value: AS_NONE

CSRFtagAction

One or more Cross-Site Request Forgery (CSRF) Tagging actions. Available settings function as follows: * Block - Block connections that violate this security check. * Learn - Use the learning engine to generate a list of exceptions to this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -CSRFtagAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -CSRFtagAction none". Default value: AS_NONE

crossSiteScriptingAction

One or more Cross-Site Scripting (XSS) actions. Available settings function as follows: * Block - Block connections that violate this security check. * Learn - Use the learning engine to generate a list of exceptions to this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -crossSiteScriptingAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -crossSiteScriptingAction none". Default value: AS_DEFAULT_DISPOSITION

crossSiteScriptingTransformUnsafeHTML

Transform cross-site scripts. This setting configures the application firewall to disable dangerous HTML instead of blocking the request. CAUTION: Make sure that this

parameter is set to ON if you are configuring any cross-site scripting transformations. If it is set to OFF, no cross-site scripting transformations are performed regardless of any other settings. Possible values: ON, OFF

crossSiteScriptingCheckCompleteURLs

Check complete URLs for cross-site scripts, instead of just the query portions of URLs. Possible values: ON, OFF

SQLInjectionAction

One or more HTML SQL Injection actions. Available settings function as follows: * Block - Block connections that violate this security check. * Learn - Use the learning engine to generate a list of exceptions to this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -SQLInjectionAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -SQLInjectionAction none". Default value: AS_DEFAULT_DISPOSITION

SQLInjectionTransformSpecialChars

Transform injected SQL code. This setting configures the application firewall to disable SQL special strings instead of blocking the request. Since most SQL servers require a special string to activate an SQL keyword, in most cases a request that contains injected SQL code is safe if special strings are disabled. CAUTION: Make sure that this parameter is set to ON if you are configuring any SQL injection transformations. If it is set to OFF, no SQL injection transformations are performed regardless of any other settings. Possible values: ON, OFF

SQLInjectionOnlyCheckFieldsWithSQLChars

Check only form fields that contain SQL special strings (characters) for injected SQL code. Most SQL servers require a special string to activate an SQL request, so SQL code without a special string is harmless to most SQL servers. Possible values: ON, OFF

fieldFormatAction

One or more Field Format actions. Available settings function as follows: * Block - Block connections that violate this security check. * Learn - Use the learning engine to generate a list of suggested web form fields and field format assignments. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -fieldFormatAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -fieldFormatAction none". Default value: AS_DEFAULT_DISPOSITION

defaultFieldFormatType

Designate a default field type to be applied to web form fields that do not have a field type explicitly assigned to them.

defaultFieldFormatMinLength

Minimum length, in characters, for data entered into a field that is assigned the default field type. To disable the minimum and maximum length settings and allow data of any length to be entered into the field, set this parameter to zero (0). Default value: AS_DEFAULTFIELDFORMAT_DEFAULT_MIN_LEN Minimum value: 0 Maximum value: 65535

defaultFieldFormatMaxLength

Maximum length, in characters, for data entered into a field that is assigned the default field type. Default value: AS_DEFAULTFIELDFORMAT_DEFAULT_MAX_LEN
Minimum value: 1 Maximum value: 65535

bufferOverflowAction

One or more Buffer Overflow actions. Available settings function as follows: * Block - Block connections that violate this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -bufferOverflowAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -bufferOverflowAction none". Default value: AS_DEFAULT_DISPOSITION

bufferOverflowMaxURLLength

Maximum length, in characters, for URLs on your protected web sites. Requests with longer URLs are blocked. Default value:
AS_BUFFEROVERFLOW_DEFAULT_MAX_URL_LEN Minimum value: 0 Maximum value: 65535

bufferOverflowMaxHeaderLength

Maximum length, in characters, for HTTP headers in requests sent to your protected web sites. Requests with longer headers are blocked. Default value:
AS_BUFFEROVERFLOW_DEFAULT_MAX_HDR_LEN Minimum value: 0 Maximum value: 65535

bufferOverflowMaxCookieLength

Maximum length, in characters, for cookies sent to your protected web sites. Requests with longer cookies are blocked. Default value:
AS_BUFFEROVERFLOW_DEFAULT_MAX_COOKIE_LEN Minimum value: 0 Maximum value: 65535

creditCardAction

One or more Credit Card actions. Available settings function as follows: * Block - Block connections that violate this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -creditCardAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -creditCardAction none". Default value: AS_NONE

creditCard

Credit card types that the application firewall should protect. Default value:
AS_CCARD_DEFAULT_CARD_TYPE

creditCardMaxAllowed

Maximum number of credit card numbers that can appear on a web page served by your protected web sites. Pages that contain more credit card numbers are blocked, or the credit card numbers are masked. Maximum value: 255

creditCardXOut

Mask any credit card number detected in a response by replacing each digit, except the digits in the final group, with the letter "X." Possible values: ON, OFF

requestContentType

Default Content-Type header for requests. A Content-Type header can contain 0-255 letters, numbers, and the hyphen (-) and underscore (_) characters. Default value: NS_S_AS_DEFAULT_REQUEST_CONTENT_TYPE

responseContentType

Default Content-Type header for responses. A Content-Type header can contain 0-255 letters, numbers, and the hyphen (-) and underscore (_) characters. Default value: NS_S_AS_DEFAULT_RESPONSE_CONTENT_TYPE

XMLDoSAction

One or more XML Denial-of-Service (XDoS) actions. Available settings function as follows: * Block - Block connections that violate this security check. * Learn - Use the learning engine to generate a list of exceptions to this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -XMLDoSAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLDoSAction none". Default value: AS_DEFAULT_DISPOSITION

XMLFormatAction

One or more XML Format actions. Available settings function as follows: * Block - Block connections that violate this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -XMLFormatAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLFormatAction none". Default value: AS_DEFAULT_DISPOSITION

XMLSQLInjectionAction

One or more XML SQL Injection actions. Available settings function as follows: * Block - Block connections that violate this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -XMLSQLInjectionAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLSQLInjectionAction none". Default value: AS_DEFAULT_DISPOSITION

XMLSQLInjectionOnlyCheckFieldsWithSQLChars

Check only form fields that contain SQL special characters, which most SQL servers require before accepting an SQL command, for injected SQL. Possible values: ON, OFF

XMLSQLInjectionParseComments

Parse comments in XML Data and exempt those sections of the request that are from the XML SQL Injection check. You must configure the type of comments that the application firewall is to detect and exempt from this security check. Available settings function as follows: * Check all - Check all content. * ANSI - Exempt content that is part of an ANSI (Mozilla-style) comment. * Nested - Exempt content that is part of a nested (Microsoft-style) comment. * ANSI Nested - Exempt content that is part of any type of comment. Possible values: checkall, ansi, nested, ansinested. Default value: AS_CHECKALL

XMLXSSAction

One or more XML Cross-Site Scripting actions. Available settings function as follows: * Block - Block connections that violate this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -XMLXSSAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLXSSAction none". Default value: AS_DEFAULT_DISPOSITION

XMLWSIAction

One or more Web Services Interoperability (WSI) actions. Available settings function as follows: * Block - Block connections that violate this security check. * Learn - Use the learning engine to generate a list of exceptions to this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -XMLWSIAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLWSIAction none". Default value: AS_DEFAULT_DISPOSITION

XMLAttachmentAction

One or more XML Attachment actions. Available settings function as follows: * Block - Block connections that violate this security check. * Learn - Use the learning engine to generate a list of exceptions to this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -XMLAttachmentAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLAttachmentAction none". Default value: AS_DEFAULT_DISPOSITION

XMLValidationAction

One or more XML Validation actions. Available settings function as follows: * Block - Block connections that violate this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -XMLValidationAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLValidationAction none". Default value: AS_DEFAULT_DISPOSITION

XMLErrorObject

Name to assign to the XML Error Object, which the application firewall displays when a user request is blocked. Must begin with a letter, number, or the underscore character \(_), and must contain only letters, numbers, and the hyphen \(-), period \(.), pound \(\#), space \(\), at (@), equals \(\=), colon \(:), and underscore characters. Cannot be changed after the XML error object is added. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks \('for example, "my XML error object" or 'my XML error object'). Default value: NS_S_AS_ERROR_OBJECT_DEFAULT

customSettings

Object name for custom settings. This check is applicable to Profile Type: HTML, XML. Default value: NS_S_AS_CUSTOM_OBJECT_DEFAULT

signatures

Object name for signatures. This check is applicable to Profile Type: HTML, XML.
Default value: NS_S_AS_CUSTOM_OBJECT_DEFAULT

XMLSOAPFaultAction

One or more XML SOAP Fault Filtering actions. Available settings function as follows:
* Block - Block connections that violate this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. * Remove - Remove all violations for this security check. CLI users: To enable one or more actions, type "set appfw profile - XMLSOAPFaultAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLSOAPFaultAction none". Default value: AS_DEFAULT_DISPOSITION

useHTMLErrorObject

Send an imported HTML Error object to a user when a request is blocked, instead of redirecting the user to the designated Error URL. Possible values: ON, OFF

errorURL

URL that application firewall uses as the Error URL. Default value: NS_S_AS_ERROR_URL_DEFAULT

HTMLErrorObject

Name to assign to the HTML Error Object. Must begin with a letter, number, or the underscore character \(_\), and must contain only letters, numbers, and the hyphen \(-\), period \(.\) pound \(\#\), space \(\), at \(@\), equals \(\=\), colon \(:\) and underscore characters. Cannot be changed after the HTML error object is added. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks \(''for example, "my HTML error object" or 'my HTML error object'\). Default value: NS_S_AS_ERROR_OBJECT_DEFAULT

logEveryPolicyHit

Log every profile match, regardless of security checks results. Possible values: ON, OFF

stripComments

Strip HTML comments. This check is applicable to Profile Type: HTML. Possible values: ON, OFF

stripHtmlComments

Strip HTML comments before forwarding a web page sent by a protected web site in response to a user request. Possible values: none, all, exclude_script_tag

stripXmlComments

Exempt URLs that pass the Start URL closure check from additional security checks. Possible values: none, all

exemptClosureURLsFromSecurityChecks

Exempt URLs that pass the Start URL closure check from additional security checks. Possible values: ON, OFF

defaultCharSet

Default character set for protected web pages. Web pages sent by your protected web sites in response to user requests are assigned this character set if the page

does not already specify a character set. The character sets supported by the application firewall are: * iso-8859-1 (English US) * big5 (Chinese Traditional) * gb2312 (Chinese Simplified) * sjis (Japanese Shift-JIS) * euc-jp (Japanese EUC-JP) * iso-8859-9 (Turkish) * utf-8 (Unicode) * euc-kr (Korean) Default value: NS_S_AS_CHARSET_DEFAULT Maximum value: 31

postBodyLimit

Maximum allowed HTTP post body size, in bytes. Default value: AS_DEFAULT_POSTBODYLIMIT Maximum value: 1000000000

fileUploadMaxNum

Maximum allowed number of file uploads per form-submission request. The maximum setting (65535) allows an unlimited number of uploads. Default value: AS_DEFAULT_MAX_FILE_UPLOADS Maximum value: 65535

canonicalizeHTMLResponse

Perform HTML entity encoding for any special characters in responses sent by your protected web sites. Possible values: ON, OFF Default value: ON

enableFormTagging

Enable tagging of web form fields for use by the Form Field Consistency and CSRF Form Tagging checks. Possible values: ON, OFF Default value: ON

sessionlessFieldConsistency

Perform sessionless Field Consistency Checks. Possible values: OFF, ON, postOnly Default value: AS_OFF

sessionlessURLClosure

Enable session less URL Closure Checks. This check is applicable to Profile Type: HTML. Possible values: ON, OFF Default value: OFF

semicolonFieldSeparator

Allow ';' as a form field separator in URL queries and POST form bodies. Possible values: ON, OFF Default value: OFF

excludeFileUploadFromChecks

Exclude uploaded files from Form checks. Possible values: ON, OFF Default value: OFF

SQLInjectionParseComments

Parse HTML comments and exempt them from the HTML SQL Injection check. You must specify the type of comments that the application firewall is to detect and exempt from this security check. Available settings function as follows: * Check all - Check all content. * ANSI - Exempt content that is part of an ANSI (Mozilla-style) comment. * Nested - Exempt content that is part of a nested (Microsoft-style) comment. * ANSI Nested - Exempt content that is part of any type of comment. Possible values: checkall, ansi, nested, ansinested Default value: AS_DEFAULT_SQLINJECTIONPARSECOMMENTS

invalidPercentHandling

Configure the method that the application firewall uses to handle percent-encoded names and values. Available settings function as follows: * apache_mode - Apache format. * asp_mode - Microsoft ASP format. * secure_mode - Secure format. Possible

values: apache_mode, asp_mode, secure_mode Default value:
AS_PERCENT_DECODE_SECURE_MODE

type

Application firewall profile type, which controls which security checks and settings are applied to content that is filtered with the profile. Available settings function as follows: * HTML - HTML-based web sites. * XML - XML-based web sites and services. * HTML XML (Web 2.0) - Sites that contain both HTML and XML content, such as ATOM feeds, blogs, and RSS feeds. Default value: AF_PROFILE_TYPE_HTML

checkRequestHeaders

Check request headers as well as web forms for injected SQL and cross-site scripts. Possible values: ON, OFF Default value: OFF

comment

Any comments about the purpose of profile, or other useful information about the profile.

[Top](#)

unset appfw profile

Synopsis

```
unset appfw profile <name> [-startURLAction] [-startURLClosure] [-denyURLAction] [-
RefererHeaderCheck] [-cookieConsistencyAction] [-cookieTransforms] [-
cookieEncryption] [-cookieProxying] [-addCookieFlags] [-fieldConsistencyAction] [-
CSRFTagAction] [-crossSiteScriptingAction] [-crossSiteScriptingTransformUnsafeHTML] [-
crossSiteScriptingCheckCompleteURLs] [-SQLInjectionAction] [-
SQLInjectionTransformSpecialChars] [-SQLInjectionOnlyCheckFieldsWithSQLChars] [-
fieldFormatAction] [-defaultFieldFormatType] [-defaultFieldFormatMinLength] [-
defaultFieldFormatMaxLength] [-bufferOverflowAction] [-
bufferOverflowMaxURLLength] [-bufferOverflowMaxHeaderLength] [-
bufferOverflowMaxCookieLength] [-creditCardAction] [-creditCard] [-
creditCardMaxAllowed] [-creditCardXOut] [-requestContentType] [-
responseContentType] [-XMLDoSAction] [-XMLFormatAction] [-XMLSQLInjectionAction] [-
XMLSQLInjectionOnlyCheckFieldsWithSQLChars] [-XMLSQLInjectionParseComments] [-
XMLXSSAction] [-XMLWSIAction] [-XMLAttachmentAction] [-XMLValidationAction] [-
XMLErrorObject] [-signatures] [-XMLSOAPFaultAction] [-useHTMLErrorObject] [-
errorURL] [-HTMLErrorObject] [-logEveryPolicyHit] [-stripHtmlComments] [-
stripXmlComments] [-exemptClosureURLsFromSecurityChecks] [-defaultCharSet] [-
postBodyLimit] [-fileUploadMaxNum] [-canonicalizeHTMLResponse] [-
enableFormTagging] [-sessionlessFieldConsistency] [-sessionlessURLClosure] [-
semicolonFieldSeparator] [-excludeFileUploadFromChecks] [-
SQLInjectionParseComments] [-invalidPercentHandling] [-type] [-checkRequestHeaders]
[-comment]
```

Description

Use this command to remove appfw profile settings. Refer to the set appfw profile command for meanings of the arguments.

[Top](#)

bind appfw profile

Synopsis

```
bind appfw profile <name> (-startURL <expression> | -denyURL <expression> | (-
fieldConsistency <string> <formActionURL> [-isRegex ( REGEX | NOTREGEX )]) | (-
cookieConsistency <string> [-isRegex ( REGEX | NOTREGEX )]) | (-SQLInjection <string>
<formActionURL> [-isRegex ( REGEX | NOTREGEX )] [-location <location>]) | (-CSRFTag
<expression> <CSRFFormActionURL>) | (-crossSiteScripting <string> <formActionURL> [-
isRegex ( REGEX | NOTREGEX )] [-location <location>]) | (-fieldFormat <string>
<formActionURL> <fieldType> [-fieldFormatMinLength <positive_integer>] [-
fieldFormatMaxLength <positive_integer>] [-isRegex ( REGEX | NOTREGEX )]) | (-
safeObject <string> <expression> <maxMatchLength> [-action <action> ...]) | -
trustedLearningClients <ip_addr[/prefix]|ipv6_addr[/prefix]|*> | (-XMLDoSURL
<expression> [-XMLMaxElementDepthCheck ( ON | OFF ) [-XMLMaxElementDepth
<positive_integer>]] [-XMLMaxElementNameLengthCheck ( ON | OFF ) [-
XMLMaxElementNameLength <positive_integer>]] [-XMLMaxElementsCheck ( ON | OFF )
[-XMLMaxElements <positive_integer>]] [-XMLMaxElementChildrenCheck ( ON | OFF ) [-
XMLMaxElementChildren <positive_integer>]] [-XMLMaxAttributesCheck ( ON | OFF ) [-
XMLMaxAttributes <positive_integer>]] [-XMLMaxAttributeNameLengthCheck ( ON |
OFF ) [-XMLMaxAttributeNameLength <positive_integer>]] [-
XMLMaxAttributeValueLengthCheck ( ON | OFF ) [-XMLMaxAttributeValueLength
<positive_integer>]] [-XMLMaxCharDATALengthCheck ( ON | OFF ) [-
XMLMaxCharDATALength <positive_integer>]] [-XMLMaxFileSizeCheck ( ON | OFF ) [-
XMLMaxFileSize <positive_integer>]] [-XMLMinFileSizeCheck ( ON | OFF ) [-
XMLMinFileSize <positive_integer>]] [-XMLBlockPI ( ON | OFF )] [-XMLBlockDTD ( ON |
OFF )] [-XMLBlockExternalEntities ( ON | OFF )] [-XMLMaxEntityExpansionsCheck ( ON |
OFF ) [-XMLMaxEntityExpansions <positive_integer>]] [-
XMLMaxEntityExpansionDepthCheck ( ON | OFF ) [-XMLMaxEntityExpansionDepth
<positive_integer>]] [-XMLMaxNamespacesCheck ( ON | OFF ) [-XMLMaxNamespaces
<positive_integer>]] [-XMLMaxNamespaceUriLengthCheck ( ON | OFF ) [-
XMLMaxNamespaceUriLength <positive_integer>]] [-XMLSOAPArrayCheck ( ON | OFF ) [-
XMLMaxSOAPArraySize <positive_integer>] [-XMLMaxSOAPArrayRank
<positive_integer>]]) | (-XMLWSIURL <expression> [-XMLWSIChecks <string>]) | (-
XMLValidationURL <expression> (-XMLRequestSchema <string> | (-XMLWSDL <string> [-
XMLAdditionalSOAPHeaders ( ON | OFF )] [-XMLEndPointCheck ( ABSOLUTE |
RELATIVE )]) | -XMLValidateSOAPEnvelope ( ON | OFF )] [-XMLResponseSchema <string>]
[-XMLValidateResponse ( ON | OFF )]) | (-XMLAttachmentURL <expression> [-
XMLMaxAttachmentSizeCheck ( ON | OFF ) [-XMLMaxAttachmentSize
<positive_integer>]] [-XMLAttachmentContentTypeCheck ( ON | OFF ) [-
XMLAttachmentContentType <expression>]]) | (-XMLSQLInjection <string> [-isRegex
( REGEX | NOTREGEX )] [-location ( ELEMENT | ATTRIBUTE )]) | (-XMLXSS <string> [-
isRegex ( REGEX | NOTREGEX )] [-location ( ELEMENT | ATTRIBUTE )]) | -contentType
<expression> | -excludeResContentType <expression>) [-comment <string>] [-state
( ENABLED | DISABLED )]
```

Description

Binds the specified exemption (relaxation) or rule to the specified application firewall profile. NOTE: You should not attempt to bind more than one exemption or rule at a time by using this command.

Parameters

name

Name of the profile to which to bind an exemption or rule.

startURL

Add the specified URL to the start URL list. Enclose URLs in double quotes to ensure preservation of any embedded spaces or non-alphanumeric characters.

denyURL

Add the specified URL to the deny URL list. Enclose URLs in double quotes to ensure preservation of any embedded spaces or non-alphanumeric characters.

fieldConsistency

Exempt the specified web form field and form action URL from the form field consistency check, or exempt the specified cookie from the cookie consistency check. A form field consistency exemption (relaxation) consists of the following items: * Web form field name. Name of the form field to exempt from this check. * Form action URL. Action URL for the web form. * IsRegex flag. The IsRegex flag, followed by YES if the form action URL is a regular expression, or NO if it is a literal string.

cookieConsistency

A cookie consistency exemption (relaxation) consists of the following items: * Cookie name. Name of the cookie to exempt from this check. * IsRegex flag. The IsRegex flag, followed by YES if the cookie name is a regular expression, or NO if it is a literal string.

SQLInjection

Exempt the specified HTTP header, web form field and the form action URL, or cookie from the SQL injection check. An SQL injection exemption (relaxation) consists of the following items: *Item name. Name of the web form field, cookie, or HTTP header to exempt from this check. * Form action URL. If the item to be exempted is a web form field, the action URL for the web form. * IsRegex flag. The IsRegex flag, followed by YES if the name or form action URL is a regular expression, or NO if it is a literal string. * Location. Location that should be examined by the SQL injection check, either FORMFIELD for web form field, HEADER for HTTP header, or COOKIE for cookie.

CSRFTag

Exempt the specified form field and web form from the cross-site request forgery (CSRF tagging) check. A CSRF tagging exemption (relaxation) consists of the following items: * Web form field name. Regular expression that describes the web form field to exempt from this check. * Form action URL. The action URL for the web form.

crossSiteScripting

Exempt the specified string, found in the specified HTTP header, cookie, or web form, from the cross-site scripting check. A cross-site scripting check exemption (relaxation) consists of the following items: * HTML to exempt. The string to exempt from the cross-site scripting check. * URL. The URL to exempt. * IsRegex flag. The IsRegex flag, followed by YES if the URL is a regular expression, or NO if it is a literal string. * location. Location which should be examined by the cross-site scripting

check, either FORMFIELD for web form field, HEADER for HTTP header, or COOKIE for cookie.

fieldFormat

Impose the specified format on content returned by users in the specified web form field. A field format rule consists of the following items: * Form field name. The name of the form field. * Form action URL. The form action URL for the web form. * Field type. The field type (format) to enforce on the specified web form field. * Field format minimum length. The minimum length allowed for data in the specified field. If 0, field can be left blank. * Field format maximum length. The maximum length allowed for data in the specified field. * IsRegex flag. The IsRegex flag, followed by YES if the URL is a regular expression, or NO if it is a literal string.

safeObject

Protect web sites from exposing sensitive private information such as social security numbers, credit card numbers, driver's license numbers, passport numbers, and any other type of private information that can be described by a regular expression. A safe object consists of the following items: * Name. A name that describes the type of information that the safe object is to protect. * Expression. PCRE-format regular expression that describes the information to be protected. * Maximum match length. Maximum length of a matched string. * Action. "X-Out" to mask blocked information with the letter X, or "Remove" to remove the information.

trustedLearningClients

Trusted host/network learning IP. This binding is applicable to profile Type: HTML, XML.

comment

Any comments about the purpose of profile, or other useful information about the profile.

state

Enabled. Possible values: ENABLED, DISABLED Default value: ENABLED

XMLDoSURL

Exempt the specified URL from the specified XML denial-of-service (XDoS) attack protections. An XDoS exemption (relaxation) consists of the following items: * URL. PCRE-format regular expression for the URL or URLs to be exempted. * Maximum-element-depth-check toggle. ON to enable this check, OFF to disable it. * Maximum-element-depth-check toggle. ON to enable, OFF to disable. * Maximum-element-depth-check level. Positive integer representing the maximum allowed depth of nested XML elements. * Maximum-element-name-length-check toggle. ON to enable, OFF to disable. * Maximum element name length. Positive integer representing the maximum allowed length of XML element names. * Maximum-number-of-elements-check toggle. ON to enable, OFF to disable. * Maximum number of elements. Positive integer representing the maximum allowed number of XML elements. * Maximum-number-of-element-children-check toggle. ON to enable, OFF to disable. * Maximum number of element children. Positive integer representing the maximum allowed number of XML element children. * Maximum-number-of-attributes-check toggle. ON to enable, OFF to disable. * Maximum number of attributes. Positive integer representing the maximum allowed number of XML attributes. * Maximum-attribute-name-length-check toggle. ON to enable, OFF to disable. * Maximum attribute name length. Positive integer representing the maximum allowed length of XML attribute

names. * Maximum-attribute-value-length-check toggle. ON to enable, OFF to disable. * Maximum attribute value length. Positive integer representing the maximum allowed length of XML attribute values. * Maximum-character-data-length-check toggle. ON to enable, OFF to disable. * Maximum character-data length. Positive integer representing the maximum allowed length of XML character data. * Maximum-file-size-check toggle. ON to enable, OFF to disable. * Maximum file size. Positive integer representing the maximum allowed size, in bytes, of attached or uploaded files. * Minimum-file-size-check toggle. ON to enable, OFF to disable. * Minimum file size. Positive integer representing the minimum allowed size, in bytes, of attached or uploaded files. * Maximum-number-of-entity-expansions-check toggle. ON to enable, OFF to disable. * Maximum number of entity expansions. Positive integer representing the maximum allowed number of XML entity expansions. * Maximum-number-of XML-namespaces-check toggle. ON to enable, OFF to disable. * Maximum number of XML namespaces. Positive integer representing the maximum allowed number of XML namespaces. * Maximum-XML-namespace-URI-length-check toggle. ON to enable, OFF to disable. * MaximumXML-namespace URI length. Positive integer representing the maximum allowed length of XML namespace URIs. * Block-processing-instructions toggle. Block XML processing instructions. ON to enable, OFF to disable. * Block-DTD toggle. Block design type documents (DTDs). ON to enable, OFF to disable. * Block-external-XML-entitites toggle. ON to enable, OFF to disable. * Maximum-SOAP-array-check toggle. ON to enable, OFF to disable. * Maximum SOAP-array size. Positive integer representing the maximum allowed size of XML SOAP arrays. * Maximum SOAP-array rank. Positive integer representing the maximum rank (dimensions) of any single XML SOAP array.

XMLWSIURL

Exempt the specified URL from the web services interoperability (WS-I) check. The URL is specified as a PCRE-format regular expression, which can match one or more URLs.

XMLValidationURL

Exempt the specified URL from the XML message validation check. An XML message validation exemption (relaxation) consists of the following items: * URL. PCRE-format regular expression that matches the URL(s) to be exempted. * XML-request-schema toggle. Use the specified XML schema to validate requests. ON to enable, OFF to disable. * XML request schema. XML schema to use for validating requests. * XML-response-schema toggle. Use the specified XML schema to validate responses. ON to enable, OFF to disable. * XML response schema. XML schema to use for validating responses. * WSDL toggle. Use the specified WSDL to validate. ON to enable, OFF to disable. * WSDL. WSDL to use for validation. * SOAP-envelope toggle. Validate against the SOAP envelope. ON to enable, OFF to disable. * Additional-SOAP-headers toggle. Validate against the extended list of SOAP headers. ON to enable, OFF to disable. * XML-end-point check. ABSOLUTE to use an absolute end point, RELATIVE to use a relative end point.

XMLAttachmentURL

Exempt the specified URL from the XML attachment check. An XML attachment exemption (relaxation) consists of the following items: * URL. PCRE-format regular expression that matches the URL(s) to be exempted. * Maximum-attachment-size-check toggle. ON to enable, OFF to disable. * Maximum attachment size. Positive integer representing the maximum allowed size in bytes for each XML attachment. * Attachment-content-type-check toggle. ON to enable, OFF to disable. * Attachment

content type. PCRE-format regular expression that specifies the list of MIME content types allowed for XML attachments.

XMLSQLInjection

Exempt the specified URL from the XML SQL injection check. An XML attachment exemption (relaxation) consists of the following items: * URL. URL to exempt, as a string or a PCRE-format regular expression. * ISREGEX flag. REGEX if URL is a regular expression, NOTREGEX if URL is a fixed string. * Location. ELEMENT if the attachment is located in an XML element, ATTRIBUTE if located in an XML attribute.

XMLXSS

Exempt the specified URL from the XML cross-site scripting (XSS) check. An XML cross-site scripting exemption (relaxation) consists of the following items: * URL. URL to exempt, as a string or a PCRE-format regular expression. * ISREGEX flag. REGEX if URL is a regular expression, NOTREGEX if URL is a fixed string. * Location. ELEMENT if the attachment is located in an XML element, ATTRIBUTE if located in an XML attribute.

contentType

Add the specified content-type to the content-type list. Enclose content-type in double quotes to ensure preservation of any embedded spaces or non-alphanumeric characters.

excludeResContentType

Add the specified content-type to the response content-type list that are to be excluded from inspection. Enclose content-type in double quotes to ensure preservation of any embedded spaces or non-alphanumeric characters.

[Top](#)

unbind appfw profile

Synopsis

```
unbind appfw profile <name> (-startURL <expression> | -denyURL <expression> | (-
fieldConsistency <string> <formActionURL>) | -cookieConsistency <string> | (-
SQLInjection <string> <formActionURL> [-location <location>]) | (-CSRFtag <string>
<CSRFFormActionURL>) | (-crossSiteScripting <string> <formActionURL> [-location
<location>]) | (-fieldFormat <string> <formActionURL>) | -safeObject <string> | -
trustedLearningClients <ip_addr[/prefix]|ipv6_addr[/prefix]|*> | -XMLDoSURL
<expression> | -XMLWSIURL <expression> | -XMLValidationURL <expression> | -
XMLAttachmentURL <expression> | (-XMLSQLInjection <string> [-location ( ELEMENT |
ATTRIBUTE )]) | (-XMLXSS <string> [-location ( ELEMENT | ATTRIBUTE )]) | -contentType
<expression> | -excludeResContentType <expression>)
```

Description

Unbinds the specified exemption (relaxation) or rule from the specified application firewall profile. See the bind appfw profile command for a description of the parameters.

Parameters

name

Name of the exemption (relaxation) or rule that you want to unbind.

startURL

Start URL regular expression.

denyURL

Deny URL regular expression.

fieldConsistency

Form field name.

cookieConsistency

Cookie name.

SQLInjection

Form field, header or cookie name.

CSRFTag

CSRF Form origin URL. This binding is applicable to Profile Type: HTML.

crossSiteScripting

Form field, header or cookie name.

fieldFormat

Field format name.

safeObject

Safe Object name.

trustedLearningClients

Trusted learning Clients IP

XMLDoSURL

XML DoS URL regular expression.

XMLWSIURL

XML WS-I URL regular expression.

XMLValidationURL

XML Message URL regular expression.

XMLAttachmentURL

XML Attachment URL regular expression.

XMLSQLInjection

Exempt the specified URL from the XML SQL injection check. An XML attachment exemption (relaxation) consists of the following items: * URL. URL to exempt, as a string or a PCRE-format regular expression. * ISREGEX flag. REGEX if URL is a regular expression, NOTREGEX if URL is a fixed string. * Location. ELEMENT if the attachment is located in an XML element, ATTRIBUTE if located in an XML attribute.

XMLXSS

Exempt the specified URL from the XML cross-site scripting (XSS) check. An XML cross-site scripting exemption (relaxation) consists of the following items: * URL. URL to exempt, as a string or a PCRE-format regular expression. * ISREGEX flag. REGEX if URL is a regular expression, NOTREGEX if URL is a fixed string. * Location. ELEMENT if the attachment is located in an XML element, ATTRIBUTE if located in an XML attribute.

contentType

content-type regular expression.

excludeResContentType

Response content type regular expression that are to be excluded from inspection.

[Top](#)

show appfw profile

Synopsis

show appfw profile [<name>]

Description

Displays details of the specified application firewall profile. If no profile is specified, displays a list of all application firewall profiles on the NetScaler appliance.

Parameters

name

Name of the application firewall profile.

[Top](#)

stat appfw profile

Synopsis

stat appfw profile [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-clearstats (basic | full)]

Description

Displays statistics for the specified application firewall profile. If no profile is specified, displays abbreviated statistics for all profiles.

Parameters

name

Name of the application firewall profile.

clearstats

Clear the statistics / counters Possible values: basic, full

Example

```
stat appfw profile
```

[Top](#)

archive appfw profile

Synopsis

archive appfw profile <name> <archivename> [-comment <string>]

Description

Create archive for the profile.

Parameters

name

Name for the profile. Must begin with a letter, number, or the underscore character (`_`), and must contain only letters, numbers, and the hyphen (`-`), period (`.`), pound (`#`), space (), at (`@`), equals (`=`), colon (`:`), and underscore (`_`) characters. Cannot be changed after the profile is added. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my profile" or 'my profile').

archivename

Source for tar archive.

comment

Any comments about the purpose of profile, or other useful information about the profile.

[Top](#)

restore appfw profile

Synopsis

restore appfw profile <archivename>

Description

Restore configuration from archive file

Parameters

archivename

Source for tar archive.

[Top](#)

appfw policy

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#) | [stat](#) | [rename](#)]

add appfw policy

Synopsis

add appfw policy <name> <rule> <profileName> [-comment <string>] [-logAction <string>]

Description

Creates an application firewall policy.

Parameters

name

Name for the policy. Must begin with a letter, number, or the underscore character \(_), and must contain only letters, numbers, and the hyphen \(-\), period \(.), pound \(\#), space \(\), at \(@), equals \(\=), colon \(:), and underscore characters. Can be changed after the policy is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks \("my policy" or 'my policy').

rule

Name of the NetScaler named rule, or a NetScaler default syntax expression, that the policy uses to determine whether to filter the connection through the application firewall with the designated profile.

profileName

Name of the application firewall profile to use if the policy matches.

comment

Any comments to preserve information about the policy for later reference.

logAction

Where to log information for connections that match this policy.

[Top](#)

rm appfw policy

Synopsis

```
rm appfw policy <name>
```

Description

Removes an application firewall policy.

Parameters

name

Name of the policy to remove.

[Top](#)

set appfw policy

Synopsis

```
set appfw policy <name> [-rule <expression>] [-profileName <string>] [-comment <string>] [-logAction <string>]
```

Description

Modifies the specified parameters of an application firewall policy.

Parameters

name

Name of the policy to modify.

rule

Name of the NetScaler named rule, or a NetScaler default syntax expression, that the policy uses to determine whether to filter the connection through the application firewall with the designated profile.

profileName

Name of the application firewall profile to use if the policy matches.

comment

Any comments to preserve information about the policy for later reference.

logAction

Where to log information for connections that match this policy.

Example

```
set transform policy pol9 -rule "HTTP.REQ.HEADER(\
\"header\\").CONTAINS(\\\"qh2\\\") "
```

[Top](#)

unset appfw policy

Synopsis

```
unset appfw policy <name> [-comment] [-logAction]
```

Description

Removes the settings of an existing application firewall policy. Attributes for which a default value is available revert to their default values. See the `set appfw policy` command for a description of the parameters..Refer to the `set appfw policy` command for meanings of the arguments.

Example

```
unset transform policy pol9 -undefAction
```

[Top](#)

show appfw policy

Synopsis

```
show appfw policy [<name>]
```

Description

Displays the current settings for the specified application firewall policy. If no policy name is provided, displays a list of all application firewall policies currently configured on the NetScaler appliance.

Parameters

name

Name of the policy.

[Top](#)

stat appfw policy

Synopsis

```
stat appfw policy [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile  
<input_filename>] [-clearstats ( basic | full )]
```

Description

Displays statistics for the specified application firewall policy. If no application firewall policy is specified, displays abbreviated statistics for all application firewall policies.

Parameters

name

Name of the application firewall policy.

clearstats

Clear the statistics / counters Possible values: basic, full

Example

```
stat appfw policy
```

[Top](#)

rename appfw policy

Synopsis

```
rename appfw policy <name>@ <newName>@
```

Description

Renames an application firewall policy.

Parameters

name

Existing name of the application firewall policy.

newName

New name for the policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.), pound (#), space (), at (@), equals (=), colon (:), and underscore characters. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy').

Example

```
rename appfw policy oldname newname
```

[Top](#)

appfw policylabel

[[add](#) | [rm](#) | [bind](#) | [unbind](#) | [show](#) | [stat](#) | [rename](#)]

add appfw policylabel

Synopsis

add appfw policylabel <labelName> <policylabeltype>

Description

Creates a user-defined application firewall policy label.

Parameters**labelName**

Name for the policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.), pound (#), space (), at (@), equals (=), colon (:), and underscore characters. Can be changed after the policy label is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy label" or 'my policy label').

policylabeltype

Type of transformations allowed by the policies bound to the label. Always http_req for application firewall policy labels. Possible values: http_req

Example

```
add appfw policylabel appfw_label http_req
```

[Top](#)

rm appfw policylabel

Synopsis

rm appfw policylabel <labelName>

Description

Removes the specified application firewall policy label.

Parameters

labelName

Name of the application firewall policy label to remove.

Example

```
rm appfw policylabel appfw_label
```

[Top](#)

bind appfw policylabel

Synopsis

```
bind appfw policylabel <labelName> <policyName> <priority> [<gotoPriorityExpression>]
[-invoke (<labelType> <labelName>)]
```

Description

Binds the specified application firewall policy to the specified policy label.

Parameters

labelName

Name of the application firewall policy label.

policyName

Name of the application firewall policy to bind to the policy label.

Example

```
i)    bind appfw policylabel trans_http_url pol_1
1 2 -invoke reqvserver CURRENT
      ii)    bind appfw policylabel trans_http_url
pol_2 2
```

[Top](#)

unbind appfw policylabel

Synopsis

```
unbind appfw policylabel <labelName> <policyName> [-priority <positive_integer>]
```

Description

Unbinds the specified application firewall policy from the specified policy label. See the bind appfw policylabel command for descriptions of the parameters.

Parameters

labelName

Name for the policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.), pound (#), space (), at (@), equals (=), colon (:), and underscore characters. Can be changed after the policy label is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy label" or 'my policy label').

policyName

Name of the application firewall policy to bind to the policy label.

priority

Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

```
unbind appfw policylabel appfw_label
```

[Top](#)

show appfw policylabel

Synopsis

```
show appfw policylabel [<labelName>]
```

Description

Displays the current settings for the specified application firewall policy label. If no policy label is specified, displays a list of all application firewall policy labels currently configured on the NetScaler appliance.

Parameters

labelName

Name of the application firewall policy label.

Example

```
i)    show appfw policylabel appfw_label
ii)   show appfw policylabel
```

[Top](#)

stat appfw policylabel

Synopsis

```
stat appfw policylabel [<labelName>] [-detail] [-fullValues] [-ntimes <positive_integer>]
[-logFile <input_filename>] [-clearstats ( basic | full )]
```

Description

Displays statistics for the specified application firewall policy label. If no application firewall policy label is specified, displays abbreviated statistics for all application firewall policy labels.

Parameters

labelName

Name of the application firewall policy label.

clearstats

Clear the statistics / counters Possible values: basic, full

[Top](#)

rename appfw policylabel

Synopsis

```
rename appfw policylabel <labelName>@ <newName>@
```

Description

Renames an application firewall policy label.

Parameters

labelName

Existing name of the application firewall policy label.

newName

The new name of the application firewall policylabel.

Example

```
rename appfw policylabel oldname newname
```

[Top](#)

appfw confidField

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add appfw confidField

Synopsis

```
add appfw confidField <fieldName> <url> [-isRegex ( REGEX | NOTREGEX )] [-comment  
<string>] [-state ( ENABLED | DISABLED )]
```

Description

Defines the specified web form field as confidential. Form fields designated as confidential have the information that is provided in those fields x'd out in the audit logs.

Parameters

fieldName

Name of the form field to designate as confidential.

url

URL of the web page that contains the web form.

isRegex

Method of specifying the form field name. Available settings function as follows: * REGEX. Form field is a regular expression. * NOTREGEX. Form field is a literal string. Possible values: REGEX, NOTREGEX Default value: NS_NOTREGEX

comment

Any comments to preserve information about the form field designation.

state

Enable or disable the confidential field designation. Possible values: ENABLED, DISABLED Default value: ENABLED

[Top](#)

rm appfw confidField

Synopsis

```
rm appfw confidField <fieldName> <url>
```

Description

Removes a confidential field designation.

Parameters

fieldName

Name of the web form field.

url

URL of the web page that contains the web form in which the field appears.

[Top](#)

set appfw confidField

Synopsis

```
set appfw confidField <fieldName> <url> [-comment <string>] [-state ( ENABLED |
DISABLED )]
```

Description

Modifies the specified parameters of a confidential field setting. Form fields designated as confidential have the information that is provided in those fields x'd out in the audit logs.

Parameters

fieldName

Name of the field to modify.

url

URL of the web page that contains the web form.

comment

Any comments to preserve information about the form field designation.

state

Enable or disable the confidential field designation. Possible values: ENABLED, DISABLED Default value: ENABLED

[Top](#)

unset appfw confidField

Synopsis

```
unset appfw confidField <fieldName> <url> [-comment] [-state]
```

Description

Use this command to remove appfw confidField settings. Refer to the set appfw confidField command for meanings of the arguments.

[Top](#)

show appfw confidField

Synopsis

```
show appfw confidField [<fieldName> <url>]
```

Description

Displays the current settings for the specified application firewall confidential field designation. If no confidential field designation is specified, displays a list of all application firewall confidential field designations on the NetScaler appliance.

Parameters

fieldName

Name of the web form field.

url

URL of the web page that contains the web form with the form field.

[Top](#)

appfw stats

show appfw stats

Synopsis

show appfw stats - alias for 'stat appfw'

Description

show appfw stats is an alias for stat appfw

appfw xmlerrorpage

[[rm](#) | [show](#) | [import](#) | [update](#)]

rm appfw xmlerrorpage

Synopsis

rm appfw xmlerrorpage <name>

Description

Removes the object imported by import xmlerrorpage.

Parameters

name

Indicates name of the imported xml error page to be removed.

Example

```
rm xmlerrorpage <name>
```

[Top](#)

show appfw xmlerrorpage

Synopsis

show appfw xmlerrorpage [<name>]

Description

Displays the specified XML error object. If no XML error page object is specified, displays a list of all XML error objects on the NetScaler appliance.

Parameters

name

Name of the XML error object.

Example

```
show appfw xmlerrorpage
```

[Top](#)

import appfw xmlerrorpage

Synopsis

```
import appfw xmlerrorpage <src> <name> [-comment <string>] [-overwrite]
```

Description

Imports the specified XML error page to the NetScaler appliance and assigns it the specified name.

Parameters

src

URL (protocol, host, path, and name) for the location at which to store the imported XML error object. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

name

Name to assign to the XML error object on the NetScaler appliance.

comment

Any comments to preserve information about the XML error object.

overwrite

Overwrite any existing XML error object of the same name.

Example

```
import xmlerrorpage http://www.example.com/
errorpage.xml my-xml-error-page
```

[Top](#)

update appfw xmlerrorpage

Synopsis

```
update appfw xmlerrorpage <name>
```

Description

Updates the specified XML error object from the source.

Parameters

name

Name of the XML error object.

Example

```
update xmlerrorpage my-xml-error-page
```

[Top](#)

appfw htmlerrorpage

[[rm](#) | [show](#) | [import](#) | [update](#)]

rm appfw htmlerrorpage

Synopsis

rm appfw htmlerrorpage <name>

Description

Removes the specified XML error object.

Parameters

name

Name of the XML error object to remove.

Example

```
rm htmlerrorpage <name>
```

[Top](#)

show appfw htmlerrorpage

Synopsis

show appfw htmlerrorpage [<name>]

Description

Displays the specified HTML error object. If no HTML error object is specified, lists all HTML error objects on the NetScaler appliance.

Parameters

name

Name of the HTML error object.

Example

```
show appfw htmlerrorpage
```

[Top](#)

import appfw htmlerrorpage

Synopsis

```
import appfw htmlerrorpage <src> <name> [-comment <string>] [-overwrite]
```

Description

Imports the specified HTML error page to the NetScaler appliance and assigns it the specified name.

Parameters

src

URL (protocol, host, path, and name) for the location at which to store the imported HTML error object. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

name

Name to assign to the HTML error object on the NetScaler appliance.

comment

Any comments to preserve information about the HTML error object.

overwrite

Overwrite any existing HTML error object of the same name.

Example

```
import htmlerrorpage http://www.example.com/  
errorpage.html my-html-error-page
```

[Top](#)

update appfw htmlerrorpage

Synopsis

```
update appfw htmlerrorpage <name>
```

Description

Updates the specified HTML error page object from the source.

Parameters

name

Name of the HTML error page object to update.

Example

```
update htmlerrorpage my-html-error-page
```

[Top](#)

appfw settings

[[set](#) | [unset](#) | [show](#)]

set appfw settings

Synopsis

```
set appfw settings [-defaultProfile <string>] [-undefAction <string>] [-sessionTimeout  
<positive_integer>] [-learnRateLimit <positive_integer>] [-sessionLifetime  
<positive_integer>] [-sessionCookieName <string>] [-clientIPLoggingHeader <string>] [-  
importSizeLimit <positive_integer>] [-signatureAutoUpdate ( ON | OFF )] [-signatureUrl  
<expression>] [-cookiePostEncryptPrefix <string>] [-logMalformedReq ( ON | OFF )] [-  
CEFLogging ( ON | OFF )] [-entityDecoding ( ON | OFF )] [-useConfigurableSecretKey  
( ON | OFF )]
```

Description

Modifies the global application firewall settings. The global settings apply to all application firewall profiles.

Parameters

defaultProfile

Profile to use when a connection does not match any policy. Default setting is APPFW_BYPASS, which sends unmatched connections back to the NetScaler appliance without attempting to filter them further. Default value: AS_ENGINESETTINGS_DEFAULT_PROF_DEFAULT

undefAction

Profile to use when an application firewall policy evaluates to undefined (UNDEF). An UNDEF event indicates an internal error condition. The APPFW_BLOCK built-in profile is the default setting. You can specify a different built-in or user-created profile as the UNDEF profile. Default value: AS_ENGINESETTINGS_UNDEF_PROF_DEFAULT

sessionTimeout

Timeout, in seconds, after which a user session is terminated. Before continuing to use the protected web site, the user must establish a new session by opening a

designated start URL. Default value: AS_ENGISETTINGS_SESSIONTIMEOUT_DEFAULT
Minimum value: 1 Maximum value: 65535

learnRateLimit

Maximum number of connections per second that the application firewall learning engine examines to generate new relaxations for learning-enabled security checks. The application firewall drops any connections above this limit from the list of connections used by the learning engine. Default value:
AS_ENGISETTINGS_LEARN_RATE_LIMIT_DEFAULT Minimum value: 1 Maximum value: 1000

sessionLifetime

Maximum amount of time (in seconds) that the application firewall allows a user session to remain active, regardless of user activity. After this time, the user session is terminated. Before continuing to use the protected web site, the user must establish a new session by opening a designated start URL. Default value:
AS_ENGISETTINGS_SESSIONLIFETIME_DEFAULT Maximum value: 2147483647

sessionCookieName

Name of the session cookie that the application firewall uses to track user sessions. Must begin with a letter or number, and can consist of from 1 to 31 letters, numbers, and the hyphen (-) and underscore (_) symbols. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cookie name" or 'my cookie name'). Default value: NS_S_AS_DEFAULT_COOKIE_NAME

clientIPLoggingHeader

Name of an HTTP header that contains the IP address that the client used to connect to the protected web site or service.

importSizeLimit

Cumulative total maximum number of bytes in web forms imported to a protected web site. If a user attempts to upload files with a total byte count higher than the specified limit, the application firewall blocks the request. Default value:
AS_ENGISETTINGS_IMPORTSIZELIMIT_DEFAULT Minimum value: 1 Maximum value: 134217728

signatureAutoUpdate

Flag used to enable/disable auto update signatures Possible values: ON, OFF Default value: OFF

signatureUrl

URL to download the mapping file from server Default value:
AS_ENGISETTINGS_SIGNATURES_UPDATE_URL

cookiePostEncryptPrefix

String that is prepended to all encrypted cookie values. Default value:
NS_S_AS_DEFAULT_CKI_POST_ENCRYPT_PREFIX

logMalformedReq

Log requests that are so malformed that application firewall parsing doesn't occur. Possible values: ON, OFF Default value: ON

CEFLogging

Enable CEF format logs. Possible values: ON, OFF Default value: OFF

entityDecoding

Transform multibyte (double- or half-width) characters to single width characters.
Possible values: ON, OFF Default value: OFF

useConfigurableSecretKey

Use configurable secret key in AppFw operations Possible values: ON, OFF Default value: OFF

[Top](#)

unset appfw settings

Synopsis

```
unset appfw settings [-defaultProfile] [-undefAction] [-sessionTimeout] [-learnRateLimit] [-sessionLifetime] [-sessionCookieName] [-clientIPLoggingHeader] [-importSizeLimit] [-signatureAutoUpdate] [-signatureUrl] [-cookiePostEncryptPrefix] [-logMalformedReq] [-CEFLogging] [-entityDecoding] [-useConfigurableSecretKey]
```

Description

Use this command to remove appfw settings settings. Refer to the set appfw settings command for meanings of the arguments.

[Top](#)

show appfw settings

Synopsis

```
show appfw settings
```

Description

Displays the current application firewall global settings.

[Top](#)

appfw transactionRecords

show appfw transactionRecords

Synopsis

```
show appfw transactionRecords
```

Description

Display an application firewall transaction record.

appfw global

[[bind](#) | [unbind](#) | [show](#)]

bind appfw global

Synopsis

```
bind appfw global <policyName> <priority> [-state ( ENABLED | DISABLED )]  
[<gotoPriorityExpression>] [-type <type>] [-invoke (<labelType> <labelName>)]
```

Description

Activates an application firewall policy.

Parameters

policyName
Name of the policy.

[Top](#)

unbind appfw global

Synopsis

```
unbind appfw global <policyName> [-type <type>] [-priority <positive_integer>]
```

Description

Deactivates the specified application firewall policy. See the bind appfw policy command for descriptions of the parameters.

Parameters

policyName
Application Firewall policy name.

priority
Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value:
2147483647

[Top](#)

show appfw global

Synopsis

```
show appfw global [-type <type>]
```

Description

Displays a list of application firewall policies that are bound to the specified bind point. If no bind point is specified, displays a list of all application firewall policies

Parameters

type
Bind point to which to policy is bound. Possible values: REQ_OVERRIDE,
REQ_DEFAULT, NONE

[Top](#)

appfw learningsettings

[[set](#) | [unset](#) | [show](#)]

set appfw learningsettings

Synopsis

```
set appfw learningsettings <profileName> [-startURLMinThreshold <positive_integer>] [-startURLPercentThreshold <positive_integer>] [-cookieConsistencyMinThreshold <positive_integer>] [-cookieConsistencyPercentThreshold <positive_integer>] [-CSRFtagMinThreshold <positive_integer>] [-CSRFtagPercentThreshold <positive_integer>] [-fieldConsistencyMinThreshold <positive_integer>] [-fieldConsistencyPercentThreshold <positive_integer>] [-crossSiteScriptingMinThreshold <positive_integer>] [-crossSiteScriptingPercentThreshold <positive_integer>] [-SQLInjectionMinThreshold <positive_integer>] [-SQLInjectionPercentThreshold <positive_integer>] [-fieldFormatMinThreshold <positive_integer>] [-fieldFormatPercentThreshold <positive_integer>] [-XMLWSIMinThreshold <positive_integer>] [-XMLWSIPercentThreshold <positive_integer>] [-XMLAttachmentMinThreshold <positive_integer>] [-XMLAttachmentPercentThreshold <positive_integer>]
```

Description

Configures the application firewall learning settings for the specified profile.

Parameters

profileName

Name of the profile.

startURLMinThreshold

Minimum number of application firewall sessions that the learning engine must observe to learn start URLs. Default value:

AS_LEARNINGSETTINGS_DEFAULT_MINTHRESHOLD Minimum value: 1

startURLPercentThreshold

Minimum percentage of application firewall sessions that must contain a particular start URL pattern for the learning engine to learn that start URL. Default value:

AS_LEARNINGSETTINGS_DEFAULT_PERCENTTHRESHOLD Maximum value: 100

cookieConsistencyMinThreshold

Minimum number of application firewall sessions that the learning engine must observe to learn cookies. Default value:

AS_LEARNINGSETTINGS_DEFAULT_MINTHRESHOLD Minimum value: 1

cookieConsistencyPercentThreshold

Minimum percentage of application firewall sessions that must contain a particular cookie pattern for the learning engine to learn that cookie. Default value:

AS_LEARNINGSETTINGS_DEFAULT_PERCENTTHRESHOLD Maximum value: 100

CSRFtagMinThreshold

Minimum number of application firewall sessions that the learning engine must observe to learn cross-site request forgery (CSRF) tags. Default value:

AS_LEARNINGSETTINGS_DEFAULT_MINTHRESHOLD Minimum value: 1

CSRFtagPercentThreshold

Minimum percentage of application firewall sessions that must contain a particular CSRF tag for the learning engine to learn that CSRF tag. Default value: AS_LEARNINGSETTINGS_DEFAULT_PERCENTTHRESHOLD Maximum value: 100

fieldConsistencyMinThreshold

Minimum number of application firewall sessions that the learning engine must observe to learn field consistency information. Default value: AS_LEARNINGSETTINGS_DEFAULT_MINTHRESHOLD Minimum value: 1

fieldConsistencyPercentThreshold

Minimum percentage of application firewall sessions that must contain a particular field consistency pattern for the learning engine to learn that field consistency pattern. Default value: AS_LEARNINGSETTINGS_DEFAULT_PERCENTTHRESHOLD Maximum value: 100

crossSiteScriptingMinThreshold

Minimum number of application firewall sessions that the learning engine must observe to learn HTML cross-site scripting patterns. Default value: AS_LEARNINGSETTINGS_DEFAULT_MINTHRESHOLD Minimum value: 1

crossSiteScriptingPercentThreshold

Minimum percentage of application firewall sessions that must contain a particular cross-site scripting pattern for the learning engine to learn that cross-site scripting pattern. Default value: AS_LEARNINGSETTINGS_DEFAULT_PERCENTTHRESHOLD Maximum value: 100

SQLInjectionMinThreshold

Minimum number of application firewall sessions that the learning engine must observe to learn HTML SQL injection patterns. Default value: AS_LEARNINGSETTINGS_DEFAULT_MINTHRESHOLD Minimum value: 1

SQLInjectionPercentThreshold

Minimum percentage of application firewall sessions that must contain a particular HTML SQL injection pattern for the learning engine to learn that HTML SQL injection pattern. Default value: AS_LEARNINGSETTINGS_DEFAULT_PERCENTTHRESHOLD Maximum value: 100

fieldFormatMinThreshold

Minimum number of application firewall sessions that the learning engine must observe to learn field formats. Default value: AS_LEARNINGSETTINGS_DEFAULT_MINTHRESHOLD Minimum value: 1

fieldFormatPercentThreshold

Minimum percentage of application firewall sessions that must contain a particular web form field pattern for the learning engine to recommend a field format for that form field. Default value: AS_LEARNINGSETTINGS_DEFAULT_PERCENTTHRESHOLD Maximum value: 100

XMLWSIMinThreshold

Minimum number of application firewall sessions that the learning engine must observe to learn web services interoperability (WSI) information. Default value: AS_LEARNINGSETTINGS_DEFAULT_MINTHRESHOLD Minimum value: 1

XMLWSIPercentThreshold

Minimum percentage of application firewall sessions that must contain a particular pattern for the learning engine to learn a web services interoperability (WSI) pattern. Default value: AS_LEARNINGSETTINGS_DEFAULT_PERCENTTHRESHOLD
Maximum value: 100

XMLAttachmentMinThreshold

Minimum number of application firewall sessions that the learning engine must observe to learn XML attachment patterns. Default value:
AS_LEARNINGSETTINGS_DEFAULT_MINTHRESHOLD Minimum value: 1

XMLAttachmentPercentThreshold

Minimum percentage of application firewall sessions that must contain a particular XML attachment pattern for the learning engine to learn that XML attachment pattern. Default value: AS_LEARNINGSETTINGS_DEFAULT_PERCENTTHRESHOLD
Maximum value: 100

[Top](#)

unset appfw learningsettings

Synopsis

```
unset appfw learningsettings <profileName> [-startURLMinThreshold] [-startURLPercentThreshold] [-cookieConsistencyMinThreshold] [-cookieConsistencyPercentThreshold] [-CSRFtagMinThreshold] [-CSRFtagPercentThreshold] [-fieldConsistencyMinThreshold] [-fieldConsistencyPercentThreshold] [-crossSiteScriptingMinThreshold] [-crossSiteScriptingPercentThreshold] [-SQLInjectionMinThreshold] [-SQLInjectionPercentThreshold] [-fieldFormatMinThreshold] [-fieldFormatPercentThreshold] [-XMLWSIMinThreshold] [-XMLWSIPercentThreshold] [-XMLAttachmentMinThreshold] [-XMLAttachmentPercentThreshold]
```

Description

Use this command to remove appfw learningsettings settings. Refer to the set appfw learningsettings command for meanings of the arguments.

[Top](#)

show appfw learningsettings

Synopsis

```
show appfw learningsettings [<profileName>]
```

Description

Displays the current application firewall learning settings for the specified profile. If no profile is specified, displays the current application firewall settings for all profiles on the NetScaler appliance.

Parameters

profileName
Name of the profile.

[Top](#)

appfw learningdata

[\[rm | show | reset | export \]](#)

rm appfw learningdata

Synopsis

```
rm appfw learningdata <profileName> (-startURL <expression> | -cookieConsistency
<string> | (-fieldConsistency <string> <formActionURL>) | (-crossSiteScripting <string>
<formActionURL>) | (-SQLInjection <string> <formActionURL>) | (-fieldFormat <string>
<formActionURL>) | (-CSRFTag <expression> <CSRFFormOriginURL>) | -XMLDoSCheck
<expression> | -XMLWSICheck <expression> | -XMLAttachmentCheck <expression>) [-
TotalXMLRequests]
```

Description

Removes unreviewed application firewall learning data for the specified application firewall profile.

Parameters

profileName

Name of the profile.

startURL

Start URL configuration.

cookieConsistency

Cookie Name.

fieldConsistency

Form field name.

crossSiteScripting

Cross-site scripting.

SQLInjection

Form field name.

fieldFormat

Field format name.

CSRFTag

CSRF Form Action URL

XMLDoSCheck

XML Denial of Service check, one of MaxAttributes MaxAttributeNameLength
MaxAttributeValueLength MaxElementNameLength MaxFileSize MinFileSize
MaxCDATALength MaxElements MaxElementDepth MaxElementChildren NumDTDs
NumProcessingInstructions NumExternalEntities MaxEntityExpansions
MaxEntityExpansionDepth MaxNamespaces MaxNamespaceUriLength
MaxSOAPArraySize MaxSOAPArrayRank

XMLWSICheck

Web Services Interoperability Rule ID.

XMLAttachmentCheck

XML Attachment Content-Type.

TotalXMLRequests

Total XML requests.

[Top](#)

show appfw learningdata

Synopsis

show appfw learningdata <profileName> <securityCheck>

Description

Displays the unreviewed application firewall learning data for the specified profile and security check.

Parameters

profileName

Name of the profile.

securityCheck

Name of the security check. Possible values: startURL, cookieConsistency, fieldConsistency, crossSiteScripting, SQLInjection, fieldFormat, CSRFtag, XMLDoSCheck, XMLWSICheck, XMLAttachmentCheck, TotalXMLRequests

[Top](#)

reset appfw learningdata

Synopsis

reset appfw learningdata

Description

Remove all databases. Make transaction count zero

[Top](#)

export appfw learningdata

Synopsis

export appfw learningdata <profileName> <securityCheck> [-target <string>]

Description

Export appfw learnt data in csv format to the location /var/learnt_data/

Parameters

profileName

Name of the profile.

securityCheck

Name of the security check. Possible values: startURL, cookieConsistency, fieldConsistency, crossSiteScripting, SQLInjection, fieldFormat, CSRFtag, XMLDoSCheck, XMLWSICheck, XMLAttachmentCheck, TotalXMLRequests

target

Target filename for data to be exported.

[Top](#)

appfw JSONContentType

[[add](#) | [rm](#) | [show](#)]

add appfw JSONContentType

Synopsis

```
add appfw JSONContentType <JSONContenttypevalue> [-isRegex ( REGEX | NOTREGEX )]
```

Description

Add JSON content type. This will classify a request/response with the specified content type as JSON

Parameters**JSONContenttypevalue**

Content type to be classified as JSON

isRegex

Is json content type a regular expression? Possible values: REGEX, NOTREGEX Default value: NS_NOTREGEX

[Top](#)

rm appfw JSONContentType

Synopsis

```
rm appfw JSONContentType <JSONContenttypevalue>
```

Description

Remove JSON content type.

Parameters**JSONContenttypevalue**

Content type to be classified as JSON

[Top](#)

show appfw JSONContentType

Synopsis

show appfw JSONContentType [<JSONContenttypevalue>]

Description

Display all JSON content types.

Parameters

JSONContenttypevalue

Content type to be classified as JSON

[Top](#)

appfw wsd

[[rm](#) | [show](#) | [import](#)]

rm appfw wsd

Synopsis

rm appfw wsd <name>

Description

Removes the specified imported WSDL file from the application firewall.

Parameters

name

Name of the WSDL file to remove.

Example

```
rm wsd <name>
```

[Top](#)

show appfw wsd

Synopsis

show appfw wsd [<name>]

Description

Removes the specified imported WSDL file.

Parameters

name

Name of the WSDL file to display.

Example

```
show appfw wsdl
```

[Top](#)

import appfw wsdl

Synopsis

```
import appfw wsdl <src> <name> [-comment <string>] [-overwrite]
```

Description

Imports the specified WSDL file to the application firewall.

Parameters

src

URL (protocol, host, path, and name) of the WSDL file to be imported is stored.
NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

name

Name to assign to the WSDL on the NetScaler appliance.

comment

Any comments to preserve information about the WSDL.

overwrite

Overwrite any existing WSDL of the same name.

Example

```
import appfw wsdl http://www.webs servicex.net/  
stockquote.asmx?wsdl stockquote
```

[Top](#)

appfw signatures

[[rm](#) | [show](#) | [import](#) | [update](#)]

rm appfw signatures

Synopsis

```
rm appfw signatures <name>
```

Description

Removes the specified signature object from the application firewall.

Parameters

name
Name of the signature object.

Example

```
rm signatures <name>
```

[Top](#)

show appfw signatures

Synopsis

show appfw signatures [<name>]

Description

Displays the specified signatures object. If no signatures object is specified, displays all signatures objects defined on the NetScaler appliance.

Parameters

name
Name of the signature object.

Example

```
show appfw signatures
```

[Top](#)

import appfw signatures

Synopsis

import appfw signatures <src> <name> [-xslt <string>] [-comment <string>] [-overwrite] [-merge] [-sha1 <string>]

Description

Imports the specified signatures object to the NetScaler appliance and assigns it the specified name.

Parameters

src
URL (protocol, host, path, and file name) for the location at which to store the imported signatures object. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

name

Name to assign to the signatures object on the NetScaler appliance.

xslt

XSLT file source.

comment

Any comments to preserve information about the signatures object.

overwrite

Overwrite any existing signatures object of the same name.

merge

Merges the existing Signature with new signature rules

sha1

File path for sha1 file to validate signature file

Example

```
import signatures http://www.example.com/ns/
signatures.xml my-signature
```

[Top](#)

update appfw signatures

Synopsis

update appfw signatures <name> [-mergeDefault]

Description

Updates the specified signatures object from the source.

Parameters**name**

Name of the signatures object to update.

mergeDefault

Merges signature file with default signature file.

Example

```
update signatures my-signatures
```

[Top](#)

appfw xmlschema

[[rm](#) | [show](#) | [import](#)]

rm appfw xmlschema

Synopsis

rm appfw xmlschema <name>

Description

Removes the specified XML Schema object from the application firewall.

Parameters

name

Name of the XML Schema object to remove.

Example

```
rm xmlschema <name>
```

[Top](#)

show appfw xmlschema

Synopsis

show appfw xmlschema [<name>]

Description

Displays the specified XML Schema object. If no object is specified, displays all XML Schema objects on the NetScaler appliance.

Parameters

name

Name of the XML Schema object to display.

Example

```
show appfw xmlschema
```

[Top](#)

import appfw xmlschema

Synopsis

import appfw xmlschema <src> <name> [-comment <string>] [-overwrite]

Description

Imports the specified XML Schema to the NetScaler appliance and assigns it the specified name.

Parameters

src

URL (protocol, host, path, and file name) for the location at which to store the imported XML Schema. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

name

Name to assign to the XML Schema object on the NetScaler appliance.

comment

Any comments to preserve information about the XML Schema object.

overwrite

Overwrite any existing XML Schema object of the same name.

Example

```
import xmlschema http://schemas.xmlsoap.org/soap/
envelope/ soap
```

[Top](#)

appfw XMLContentType

[[add](#) | [rm](#) | [show](#)]

add appfw XMLContentType

Synopsis

```
add appfw XMLContentType <XMLContenttypevalue> [-isRegex ( REGEX | NOTREGEX )]
```

Description

Add XML content type. This will classify a request/response with the specified content type as XML

Parameters

XMLContenttypevalue

Content type to be classified as XML

isRegex

Is field name a regular expression? Possible values: REGEX, NOTREGEX Default value: NS_NOTREGEX

[Top](#)

rm appfw XMLContentType

Synopsis

```
rm appfw XMLContentType <XMLContenttypevalue>
```

Description

Remove XML content type.

Parameters

XMLContenttypevalue

Content type to be classified as XML

[Top](#)

show appfw XMLContentType

Synopsis

show appfw XMLContentType [<XMLContenttypevalue>]

Description

Display all xml content types.

Parameters

XMLContenttypevalue

Content type to be classified as XML

[Top](#)

appfw archive

[[show](#) | [export](#) | [import](#) | [rm](#)]

show appfw archive

Synopsis

show appfw archive

Example

```
show appfw archive
```

[Top](#)

export appfw archive

Synopsis

export appfw archive <name> <target>

Description

Exports the archive file to the specified location

Parameters

name

Name of tar archive

target

Path to the file to be exported

[Top](#)

import appfw archive

Synopsis

```
import appfw archive <src> <name> [-comment <string>]
```

Description

Imports the archive file from specified location

Parameters

src

Indicates the source of the tar archive file as a URL of the form <protocol>://<host>[:<port>][/<path>] <protocol> is http or https. <host> is the DNS name or IP address of the http or https server. <port> is the port number of the server. If omitted, the default port for http or https will be used. <path> is the path of the file on the server. Import will fail if an https server requires client certificate authentication.

name

Indicates name of archive

comment

Comments associated with this archive.

[Top](#)

rm appfw archive

Synopsis

```
rm appfw archive <name>
```

Description

Removes the archive created by archive command.

Parameters

name

Indicates name of the archive to be removed.

Example

```
rm appfw archive <name>
```

[Top](#)

APPQOE Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [appqoe](#)
- ♦ [appqoe action](#)
- ♦ [appqoe policy](#)
- ♦ [appqoe parameter](#)
- ♦ [appqoe stats](#)

appqoe

stat appqoe

Synopsis

```
stat appqoe [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile  
<input_filename>] [-clearstats ( basic | full )]
```

Description

Displays statistics of feature AppQoE.

Parameters

clearstats

Clear the statistics / counters Possible values: basic, full

appqoe action

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add appqoe action

Synopsis

```
add appqoe action <name> [-priority <priority>] [-responseWith <responseWith> [-  
altContentSvcName <string>] [-altContentPath <string>] [-maxConn <positive_integer>]  
[-delay <usecs>] [-clientDetectRate <positive_integer>] [-dosAtckThresh  
<positive_integer>] [-HIChallenge ( ENABLED | DISABLED )]] [-polqDepth  
<positive_integer>] [-priqDepth <positive_integer>]
```

Description

Add a new AppQoE action for triggering

Parameters

name

Name for the AppQoE action. Must begin with a letter, number, or the underscore symbol (_). Other characters allowed, after the first character, are the hyphen (-),

period (.) hash (#), space (), at (@), equals (=), and colon (:) characters. This is a mandatory argument

priority

Priority for queuing the request. If server resources are not available for a request that matches the configured rule, this option specifies a priority for queuing the request until the server resources are available again. If priority is not configured then Lowest priority will be used to queue the request. Possible values: HIGH, MEDIUM, LOW, LOWEST

responseWith

Responder action to be taken when the threshold is reached. Available settings function as follows: ACS - Serve content from an alternative content service Threshold : maxConn or delay NS - Serve from the NetScaler appliance (built-in response) Threshold : maxConn or delay DOS - Send challenge response to verify client, if DOS thresholds are not matched then drop connections to lowest priority if maxConn or delay is reached Threshold : dosAtkThrsh and clientDetectRate CUSTOM - Serve content from custom response file. Threshold : custom response file can be used as any of the above action type, so thresholds depends on the response type. Custom File : set appqoe parameter -fileName /netscaler/custom.html NO ACTION - Serve no alternative content, drop connections to lowest priority if maxConn or delay is reached Possible values: ACS, NS, DOS, NOACTION, CUSTOM

altContentSvcName

Name of the alternative content service to be used in the ACS

altContentPath

Path to the alternative content service to be used in the ACS

polqDepth

Policy queue depth threshold value. When the policy queue size (number of requests queued for the policy binding this action is attached to) increases to the specified polqDepth value, subsequent requests are dropped to the lowest priority level. Minimum value: 1 Maximum value: 4294967294

priqDepth

Queue depth threshold value per priority level. If the queue size (number of requests in the queue of that particular priority) on the virtual server to which this policy is bound, increases to the specified qDepth value, subsequent requests are dropped to the lowest priority level. Minimum value: 1 Maximum value: 4294967294

maxConn

Maximum number of concurrent connections that can be open for requests that matches with rule. Minimum value: 1 Maximum value: 4294967294

delay

Delay threshold, in microseconds, for requests that match the policy's rule. If the delay statistics gathered for the matching request exceed the specified delay, configured action triggered for that request, if there is no action then requests are dropped to the lowest priority level Minimum value: 1 Maximum value: 599999999

clientDetectRate

Client detect rate, Integer representing the percentage of traffic to which the HTTP DoS policy is to be applied after the DOS attack threshold condition is satisfied
Minimum value: 1 Maximum value: 100

dosAtckThrsh

DOS atck threshold, The queue size (the number of outstanding client requests on the vserver) before DoS protection is activated on the vserver to which the DoS protection policy is bound. This is a mandatory argument for DOS action. Minimum value: 21 Maximum value: 4294967294

HIChallenge

enable or disable Human Interactive Challenge (HIC) response Possible values: ENABLED, DISABLED

[Top](#)

rm appqoe action**Synopsis**

rm appqoe action <name>

Description

Removes the specified AppQoE action.

Parameters**name**

Name of the action to be removed.

[Top](#)

set appqoe action**Synopsis**

set appqoe action <name> [-priority <priority>] [-altContentSvcName <string>] [-altContentPath <string>] [-polqDepth <positive_integer>] [-priqDepth <positive_integer>] [-maxConn <positive_integer>] [-delay <usecs>] [-clientDetectRate <positive_integer>] [-dosAtckThrsh <positive_integer>] [-HIChallenge (ENABLED | DISABLED)]

Description

Set the argument of specified AppQoE action.

Parameters**name**

Name for the AppQoE action. Must begin with a letter, number, or the underscore symbol (_). Other characters allowed, after the first character, are the hyphen (-), period (.) hash (#), space (), at (@), equals (=), and colon (:) characters. This is a mandatory argument

priority

Priority for queuing the request. If server resources are not available for a request that matches the configured rule, this option specifies a priority for queuing the request until the server resources are available again. If priority is not configured then Lowest priority will be used to queue the request. Possible values: HIGH, MEDIUM, LOW, LOWEST

altContentSvcName

Name of the alternative content service to be used in the ACS

altContentPath

Path to the alternative content service to be used in the ACS

polqDepth

Policy queue depth threshold value. When the policy queue size (number of requests queued for the policy binding this action is attached to) increases to the specified polqDepth value, subsequent requests are dropped to the lowest priority level. Minimum value: 1 Maximum value: 4294967294

priqDepth

Queue depth threshold value per priority level. If the queue size (number of requests in the queue of that particular priority) on the virtual server to which this policy is bound, increases to the specified qDepth value, subsequent requests are dropped to the lowest priority level. Minimum value: 1 Maximum value: 4294967294

maxConn

Maximum number of concurrent connections that can be open for requests that matches with rule. Minimum value: 1 Maximum value: 4294967294

delay

Delay threshold, in microseconds, for requests that match the policy's rule. If the delay statistics gathered for the matching request exceed the specified delay, configured action triggered for that request, if there is no action then requests are dropped to the lowest priority level Minimum value: 1 Maximum value: 599999999

clientDetectRate

Client detect rate, Integer representing the percentage of traffic to which the HTTP DoS policy is to be applied after the DOS attack threshold condition is satisfied Minimum value: 1 Maximum value: 100

dosAtckThrsh

DOS attack threshold, The queue size (the number of outstanding client requests on the vserver) before DoS protection is activated on the vserver to which the DoS protection policy is bound. This is a mandatory argument for DOS action. Minimum value: 21 Maximum value: 4294967294

HICChallenge

enable or disable Human Interactive Challenge (HIC) response Possible values: ENABLED, DISABLED

[Top](#)

unset appqoe action

Synopsis

```
unset appqoe action <name> [-priority] [-altContentSvcName] [-altContentPath] [-polqDepth] [-priqDepth] [-maxConn] [-delay] [-clientDetectRate] [-dosAtckThrsh] [-HIChallenge]
```

Description

Use this command to remove appqoe action settings. Refer to the set appqoe action command for meanings of the arguments.

[Top](#)

show appqoe action

Synopsis

```
show appqoe action [<name>]
```

Description

Display configured AppQoE action(s).

Parameters

name

Name for the AppQoE action. Must begin with a letter, number, or the underscore symbol (_). Other characters allowed, after the first character, are the hyphen (-), period (.) hash (#), space (), at (@), equals (=), and colon (:) characters. This is a mandatory argument

[Top](#)

appqoe policy

[[add](#) | [rm](#) | [set](#) | [show](#) | [stat](#)]

add appqoe policy

Synopsis

```
add appqoe policy <name> -rule <expression> -action <string>
```

Description

Add a new AppQoE policy for binding rule with action

Parameters

rule

Expression or name of a named expression, against which the request is evaluated. The policy is applied if the rule evaluates to true.

action

Configured AppQoE action to trigger

[Top](#)

rm appqoe policy

Synopsis

rm appqoe policy <name>

Description

Remove an AppQoE policy.

Parameters

name

Name of the AppQoE policy to be removed.

[Top](#)

set appqoe policy

Synopsis

set appqoe policy <name> [-rule <expression>] [-action <string>]

Parameters

rule

Expression or name of a named expression, against which the request is evaluated.
The policy is applied if the rule evaluates to true.

action

Configured AppQoE action to trigger

[Top](#)

show appqoe policy

Synopsis

show appqoe policy [<name>]

Description

Display all the configured AppQoE policies.

[Top](#)

stat appqoe policy

Synopsis

stat appqoe policy [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-clearstats (basic | full)]

Description

Displays collected brief statistics for all AppQoE policies, or detailed statistics for only the specified policy.

Parameters

name

policyName

clearstats

Clear the statistics / counters Possible values: basic, full

Example

```
stat appqos policy
```

[Top](#)

appqoe parameter

[[set](#) | [unset](#) | [show](#)]

set appqoe parameter

Synopsis

set appqoe parameter [-sessionLife <secs>] [-fileName <input_filename>] [-avgwaitingclient <positive_integer>]

Description

Sets the parameters for displaying appqoe information.

Parameters

sessionLife

Time, in seconds, between the first time and the next time the AppQoE alternative content window is displayed. The alternative content window is displayed only once during a session for the same browser accessing a configured URL, so this parameter determines the length of a session. Default value: 300 Minimum value: 1 Maximum value: 4294967294

fileName

File containing the customized response to be displayed when the ACTION in the AppQoE policy is set to NS. Default value: "DEFAULT"

avgwaitingclient

average number of client connections, that can sit in service waiting queue Default value: 1000000 Maximum value: 4294967294

Example

```
set appqoe parameter -sessionlife 200 -fileName /  
netscaler/custom.html -avgwaitingclient 10
```

[Top](#)

unset appqoe parameter

Synopsis

unset appqoe parameter [-sessionLife] [-fileName] [-avgwaitingclient]

Description

Use this command to remove appqoe parameter settings. Refer to the set appqoe parameter command for meanings of the arguments.

[Top](#)

show appqoe parameter

Synopsis

show appqoe parameter

Description

Displays the values of the session life and filename parameters

Example

```
show appqos parameter
```

[Top](#)

appqoe stats

show appqoe stats

Synopsis

show appqoe stats - alias for 'stat appqoe'

Description

show appqoe stats is an alias for stat appqoe Displays global AppQoE statistics.

Audit Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [audit](#)
- ♦ [audit syslogAction](#)
- ♦ [audit syslogPolicy](#)
- ♦ [audit nslogAction](#)

- ♦ [audit nslogPolicy](#)
- ♦ [audit messageaction](#)
- ♦ [audit stats](#)
- ♦ [audit messages](#)
- ♦ [audit syslogParams](#)
- ♦ [audit nslogParams](#)

audit

stat audit

Synopsis

```
stat audit [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile  
<input_filename>] [-clearstats ( basic | full )]
```

Description

Display the audit statistics

Parameters

clearstats

Clear the statistics / counters Possible values: basic, full

audit syslogAction

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add audit syslogAction

Synopsis

```
add audit syslogAction <name> <serverIP> [-serverPort <port>] -logLevel <logLevel> ...  
[-dateFormat <dateFormat>] [-logFacility <logFacility>] [-tcp ( NONE | ALL )] [-acl  
( ENABLED | DISABLED )] [-timeZone ( GMT_TIME | LOCAL_TIME )] [-userDefinedAuditlog  
( YES | NO )] [-appflowExport ( ENABLED | DISABLED )]
```

Description

Adds a syslog action. The action contains a reference to a syslog server, and specifies which information to log and how to log that information.

Parameters

name

Name of the syslog action. Must begin with a letter, number, or the underscore character (`_`), and must contain only letters, numbers, and the hyphen (`-`), period (`.`) pound (`#`), space (), at (`@`), equals (`=`), colon (`:`), and underscore characters. Cannot be changed after the syslog action is added. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my syslog action" or 'my syslog action').

serverIP

IP address of the syslog server.

serverPort

Port on which the syslog server accepts connections. Minimum value: 1

logLevel

Audit log level, which specifies the types of events to log. Available values function as follows: * ALL - All events. * EMERGENCY - Events that indicate an immediate crisis on the server. * ALERT - Events that might require action. * CRITICAL - Events that indicate an imminent server crisis. * ERROR - Events that indicate some type of error. * WARNING - Events that require action in the near future. * NOTICE - Events that the administrator should know about. * INFORMATIONAL - All but low-level events. * DEBUG - All events, in extreme detail. * NONE - No events.

dateFormat

Format of dates in the logs. Supported formats are: * MMDDYYYY. -U.S. style month/date/year format. * DDMMYYYY - European style date/month/year format. * YYYYMMDD - ISO style year/month/date format. Possible values: MMDDYYYY, DDMMYYYY, YYYYMMDD

logFacility

Facility value, as defined in RFC 3164, assigned to the log message. Log facility values are numbers 0 to 7 (LOCAL0 through LOCAL7). Each number indicates where a specific message originated from, such as the NetScaler appliance itself, the VPN, or external. Possible values: LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7

tcp

Log TCP messages. Possible values: NONE, ALL

acl

Log access control list (ACL) messages. Possible values: ENABLED, DISABLED

timeZone

Time zone used for date and timestamps in the logs. Supported settings are: * GMT_TIME. Coordinated Universal time. * LOCAL_TIME. Use the server's timezone setting. Possible values: GMT_TIME, LOCAL_TIME

userDefinedAuditlog

Log user-configurable log messages to syslog. Setting this parameter to NO causes auditing to ignore all user-configured message actions. Setting this parameter to YES causes auditing to log user-configured message actions that meet the other logging criteria. Possible values: YES, NO

appflowExport

Export log messages to AppFlow collectors. Appflow collectors are entities to which log messages can be sent so that some action can be performed on them. Possible values: ENABLED, DISABLED

[Top](#)

rm audit syslogAction

Synopsis

rm audit syslogAction <name>

Description

Removes the specified syslog action and associated configuration. Note: A syslog action cannot be removed if it is bound to a syslog policy.

Parameters

name

Name of the syslog action to remove.

[Top](#)

set audit syslogAction

Synopsis

set audit syslogAction <name> [-serverIP <ip_addr|ipv6_addr|*>] [-serverPort <port>] [-logLevel <logLevel> ...] [-dateFormat <dateFormat>] [-logFacility <logFacility>] [-tcp (NONE | ALL)] [-acl (ENABLED | DISABLED)] [-timeZone (GMT_TIME | LOCAL_TIME)] [-userDefinedAuditlog (YES | NO)] [-appflowExport (ENABLED | DISABLED)]

Description

Modifies the specified parameters of an existing syslog action.

Parameters

name

Name of the syslog action to be modified.

serverIP

IP address of the syslog server.

serverPort

Port on which the syslog server accepts connections. Minimum value: 1

logLevel

Audit log level, which specifies the types of events to log. Available values function as follows: * ALL - All events. * EMERGENCY - Events that indicate an immediate crisis on the server. * ALERT - Events that might require action. * CRITICAL - Events that indicate an imminent server crisis. * ERROR - Events that indicate some type of error. * WARNING - Events that require action in the near future. * NOTICE - Events that the administrator should know about. * INFORMATIONAL - All but low-level events. * DEBUG - All events, in extreme detail. * NONE - No events.

dateFormat

Format of dates in the logs. Supported formats are: * MMDDYYYY. -U.S. style month/date/year format. * DDMMYYYY - European style date/month/year format. * YYYYMMDD - ISO style year/month/date format. Possible values: MMDDYYYY, DDMMYYYY, YYYYMMDD

logFacility

Facility value, as defined in RFC 3164, assigned to the log message. Log facility values are numbers 0 to 7 (LOCAL0 through LOCAL7). Each number indicates where a specific message originated from, such as the NetScaler appliance itself, the VPN, or external. Possible values: LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7

tcp

Log TCP messages. Possible values: NONE, ALL

acl

Log access control list (ACL) messages. Possible values: ENABLED, DISABLED

timeZone

Time zone used for date and timestamps in the logs. Supported settings are: * GMT_TIME. Coordinated Universal time. * LOCAL_TIME. Use the server's timezone setting. Possible values: GMT_TIME, LOCAL_TIME

userDefinedAuditlog

Log user-configurable log messages to syslog. Setting this parameter to NO causes auditing to ignore all user-configured message actions. Setting this parameter to YES causes auditing to log user-configured message actions that meet the other logging criteria. Possible values: YES, NO

appflowExport

Export log messages to AppFlow collectors. Appflow collectors are entities to which log messages can be sent so that some action can be performed on them. Possible values: ENABLED, DISABLED

[Top](#)

unset audit syslogAction**Synopsis**

```
unset audit syslogAction <name> [-serverPort] [-logLevel] [-dateFormat] [-logFacility] [-tcp] [-acl] [-timeZone] [-userDefinedAuditlog] [-appflowExport] [-serverIP]
```

Description

Removes the settings of an existing syslog action. Attributes for which a default value is available revert to their default values. See the set audit syslogAction command for a description of the parameters. Refer to the set audit syslogAction command for meanings of the arguments.

[Top](#)

show audit syslogAction**Synopsis**

```
show audit syslogAction [<name>]
```

Description

Displays the current configuration of the specified syslog action. If no syslog action is specified, displays a list of all syslog actions currently configured on the NetScaler appliance.

Parameters

name
Name of the syslog action.

[Top](#)

audit syslogPolicy

[[add](#) | [rm](#) | [set](#) | [show](#)]

add audit syslogPolicy

Synopsis

add audit syslogPolicy <name> <rule> <action>

Description

Adds a policy that defines which messages to log to the specified syslog server.

Parameters

name
Name for the policy. Must begin with a letter, number, or the underscore character (_), and must consist only of letters, numbers, and the hyphen (-), period (.) pound (#), space (), at sign (@), equals (=), colon (:), and underscore characters. Cannot be changed after the syslog policy is added. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my syslog policy" or 'my syslog policy').

rule
Name of the NetScaler named rule, or a default syntax expression, that defines the messages to be logged to the syslog server.

action
Syslog server action to perform when this policy matches traffic. NOTE: A syslog server action must be associated with a syslog audit policy.

[Top](#)

rm audit syslogPolicy

Synopsis

rm audit syslogPolicy <name>

Description

Removes the specified syslog policy and associated configuration.

Parameters**name**

Name of the syslog policy to remove.

[Top](#)

set audit syslogPolicy**Synopsis**

set audit syslogPolicy <name> [-rule <expression>] [-action <string>]

Description

Configures an existing syslog policy.

Parameters**name**

Name of the syslog policy to be configured.

rule

Name of the NetScaler named rule, or a default syntax expression, that defines the messages to be logged to the syslog server.

action

Syslog server action to perform when this policy matches traffic. NOTE: A syslog server action must be associated with a syslog audit policy.

[Top](#)

show audit syslogPolicy**Synopsis**

show audit syslogPolicy [<name>]

Description

Displays the current configuration of the specified syslog policy. If no syslog policy is specified, displays a list of all syslog policies currently configured on the NetScaler appliance.

Parameters**name**

Name of the policy.

[Top](#)

audit nslogAction

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add audit nslogAction

Synopsis

```
add audit nslogAction <name> <serverIP> [-serverPort <port>] -logLevel <logLevel> ... [-dateFormat <dateFormat>] [-logFacility <logFacility>] [-tcp ( NONE | ALL )] [-acl ( ENABLED | DISABLED )] [-timeZone ( GMT_TIME | LOCAL_TIME )] [-userDefinedAuditlog ( YES | NO )] [-appflowExport ( ENABLED | DISABLED )]
```

Description

Adds an nslog action. The action contains a reference to an nslog server and specifies which information to log and how to log that information.

Parameters

name

Name of the nslog action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.), pound (#), space (), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the nslog action is added. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my nslog action" or 'my nslog action').

serverIP

IP address of the nslog server.

serverPort

Port on which the nslog server accepts connections. Minimum value: 1

logLevel

Audit log level, which specifies the types of events to log. Available settings function as follows: * ALL - All events. * EMERGENCY - Events that indicate an immediate crisis on the server. * ALERT - Events that might require action. * CRITICAL - Events that indicate an imminent server crisis. * ERROR - Events that indicate some type of error. * WARNING - Events that require action in the near future. * NOTICE - Events that the administrator should know about. * INFORMATIONAL - All but low-level events. * DEBUG - All events, in extreme detail. * NONE - No events.

dateFormat

Format of dates in the logs. Supported formats are: * MMDDYYYY - U.S. style month/date/year format. * DDMMYYYY - European style date/month/year format. * YYYYMMDD - ISO style year/month/date format. Possible values: MMDDYYYY, DDMMYYYY, YYYYMMDD

logFacility

Facility value, as defined in RFC 3164, assigned to the log message. Log facility values are numbers 0 to 7 (LOCAL0 through LOCAL7). Each number indicates where a specific message originated from, such as the NetScaler appliance itself, the VPN, or external. Possible values: LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7

tcp

Log TCP messages. Possible values: NONE, ALL

acl

Log access control list (ACL) messages. Possible values: ENABLED, DISABLED

timeZone

Time zone used for date and timestamps in the logs. Available settings function as follows: * GMT_TIME. Coordinated Universal Time. * LOCAL_TIME. The server's timezone setting. Possible values: GMT_TIME, LOCAL_TIME

userDefinedAuditlog

Log user-configurable log messages to nslog. Setting this parameter to NO causes auditing to ignore all user-configured message actions. Setting this parameter to YES causes auditing to log user-configured message actions that meet the other logging criteria. Possible values: YES, NO

appflowExport

Export log messages to AppFlow collectors. Appflow collectors are entities to which log messages can be sent so that some action can be performed on them. Possible values: ENABLED, DISABLED

[Top](#)

rm audit nslogAction**Synopsis**

```
rm audit nslogAction <name>
```

Description

Removes the specified nslog action and associated configuration. Note: An nslog action cannot be removed if it is bound to an nslog policy.

Parameters**name**

Name of the nslog action to remove.

[Top](#)

set audit nslogAction**Synopsis**

```
set audit nslogAction <name> [-serverIP <ip_addr|ipv6_addr|*>] [-serverPort <port>] [-logLevel <logLevel> ...] [-dateFormat <dateFormat>] [-logFacility <logFacility>] [-tcp ( NONE | ALL )] [-acl ( ENABLED | DISABLED )] [-timeZone ( GMT_TIME | LOCAL_TIME )] [-userDefinedAuditlog ( YES | NO )] [-appflowExport ( ENABLED | DISABLED )]
```

Description

Modifies the specified settings of an existing nslog action.

Parameters**name**

Name of the nslog action to be modified.

serverIP

IP address of the nslog server.

serverPort

Port on which the nslog server accepts connections. Minimum value: 1

logLevel

Audit log level, which specifies the types of events to log. Available settings function as follows: * ALL - All events. * EMERGENCY - Events that indicate an immediate crisis on the server. * ALERT - Events that might require action. * CRITICAL - Events that indicate an imminent server crisis. * ERROR - Events that indicate some type of error. * WARNING - Events that require action in the near future. * NOTICE - Events that the administrator should know about. * INFORMATIONAL - All but low-level events. * DEBUG - All events, in extreme detail. * NONE - No events.

dateFormat

Format of dates in the logs. Supported formats are: * MMDDYYYY - U.S. style month/date/year format. * DDMMYYYY - European style date/month/year format. * YYYYMMDD - ISO style year/month/date format. Possible values: MMDDYYYY, DDMMYYYY, YYYYMMDD

logFacility

Facility value, as defined in RFC 3164, assigned to the log message. Log facility values are numbers 0 to 7 (LOCAL0 through LOCAL7). Each number indicates where a specific message originated from, such as the NetScaler appliance itself, the VPN, or external. Possible values: LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7

tcp

Log TCP messages. Possible values: NONE, ALL

acl

Log access control list (ACL) messages. Possible values: ENABLED, DISABLED

timeZone

Time zone used for date and timestamps in the logs. Available settings function as follows: * GMT_TIME. Coordinated Universal Time. * LOCAL_TIME. The server's timezone setting. Possible values: GMT_TIME, LOCAL_TIME

userDefinedAuditlog

Log user-configurable log messages to nslog. Setting this parameter to NO causes auditing to ignore all user-configured message actions. Setting this parameter to YES causes auditing to log user-configured message actions that meet the other logging criteria. Possible values: YES, NO

appflowExport

Export log messages to AppFlow collectors. Appflow collectors are entities to which log messages can be sent so that some action can be performed on them. Possible values: ENABLED, DISABLED

[Top](#)

unset audit nslogAction

Synopsis

```
unset audit nslogAction <name> [-serverPort] [-logLevel] [-dateFormat] [-logFacility] [-tcp] [-acl] [-timeZone] [-userDefinedAuditlog] [-appflowExport]
```

Description

Removes the settings of an existing nslog action. Attributes for which a default value is available revert to their default values. See the set audit nslogAction command for descriptions of the parameters..Refer to the set audit nslogAction command for meanings of the arguments.

[Top](#)

show audit nslogAction

Synopsis

```
show audit nslogAction [<name>]
```

Description

Displays the current configuration of the specified nslog action. If no nslog action is specified, displays a list of all nslog actions currently configured on the NetScaler appliance.

Parameters

name
Name of the nslog action.

[Top](#)

audit nslogPolicy

[[add](#) | [rm](#) | [set](#) | [show](#)]

add audit nslogPolicy

Synopsis

```
add audit nslogPolicy <name> <rule> <action>
```

Description

Adds a policy that defines which messages to log to the specified nslog server.

Parameters

name
Name for the policy. Must begin with a letter, number, or the underscore character (_), and must consist only of letters, numbers, and the hyphen (-), period (.) pound (#), space (), at sign (@), equals (=), colon (:), and underscore characters. Cannot be changed after the nslog policy is added. The following requirement applies only to

the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my nslog policy" or 'my nslog policy').

rule

Name of the NetScaler named rule, or a default syntax expression, that defines the messages to be logged to the nslog server.

action

Nslog server action that is performed when this policy matches. NOTE: An nslog server action must be associated with an nslog audit policy.

[Top](#)

rm audit nslogPolicy

Synopsis

```
rm audit nslogPolicy <name>
```

Description

Removes the specified nslog policy and associated configuration.

Parameters

name

Name of the nslog policy to remove.

[Top](#)

set audit nslogPolicy

Synopsis

```
set audit nslogPolicy <name> [-rule <expression>] [-action <string>]
```

Description

Modifies the specified parameters of an existing nslog policy.

Parameters

name

Name of the nslog policy to modify.

rule

Name of the NetScaler named rule, or a default syntax expression, that defines the messages to be logged to the nslog server.

action

Nslog server action that is performed when this policy matches. NOTE: An nslog server action must be associated with an nslog audit policy.

[Top](#)

show audit nslogPolicy

Synopsis

show audit nslogPolicy [<name>]

Description

Displays the current configuration of the specified nslog policy. If no nslog policy is specified, displays a list of all nslog policies currently configured on the NetScaler appliance.

Parameters

name

Name of the policy.

[Top](#)

audit messageaction

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add audit messageaction

Synopsis

add audit messageaction <name> <logLevel> <stringBuilderExpr> [-logtoNewslog (YES | NO)] [-bypassSafetyCheck (YES | NO)]

Description

Adds an audit message action. The action specifies whether to log the message, and to which log.

Parameters

name

Name of the audit message action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space (), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the message action is added. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my message action" or 'my message action').

logLevel

Audit log level, which specifies the severity level of the log message being generated.. The following loglevels are valid: * EMERGENCY - Events that indicate an immediate crisis on the server. * ALERT - Events that might require action. * CRITICAL - Events that indicate an imminent server crisis. * ERROR - Events that indicate some type of error. * WARNING - Events that require action in the near future. * NOTICE - Events that the administrator should know about. * INFORMATIONAL - All but low-level events. * DEBUG - All events, in extreme detail. Possible values: EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, DEBUG

stringBuilderExpr

Default-syntax expression that defines the format and content of the log message.

logtoNewnslog

Send the message to the new nslog. Possible values: YES, NO

bypassSafetyCheck

Bypass the safety check and allow unsafe expressions. Possible values: YES, NO

Default value: NO

[Top](#)

rm audit messageaction

Synopsis

rm audit messageaction <name>

Description

Removes the specified audit message action and associated configuration.

Parameters

name

Name of the audit message action to remove.

[Top](#)

set audit messageaction

Synopsis

set audit messageaction <name> [-logLevel <logLevel>] [-stringBuilderExpr <string>] [-logtoNewnslog (YES | NO)] [-bypassSafetyCheck (YES | NO)]

Description

Modifies the specified parameters of an existing audit message action.

Parameters

name

Name of the audit message action to modify.

logLevel

Audit log level, which specifies the severity level of the log message being generated. The following loglevels are valid: * EMERGENCY - Events that indicate an immediate crisis on the server. * ALERT - Events that might require action. * CRITICAL - Events that indicate an imminent server crisis. * ERROR - Events that indicate some type of error. * WARNING - Events that require action in the near future. * NOTICE - Events that the administrator should know about. * INFORMATIONAL - All but low-level events. * DEBUG - All events, in extreme detail. Possible values: EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, DEBUG

stringBuilderExpr

Default-syntax expression that defines the format and content of the log message.

logtoNewnslog

Send the message to the new nslog. Possible values: YES, NO

bypassSafetyCheck

Bypass the safety check and allow unsafe expressions. Possible values: YES, NO

Default value: NO

[Top](#)

unset audit messageaction

Synopsis

```
unset audit messageaction <name> [-logtoNewnslog] [-bypassSafetyCheck]
```

Description

Use this command to remove audit messageaction settings. Refer to the set audit messageaction command for meanings of the arguments.

[Top](#)

show audit messageaction

Synopsis

```
show audit messageaction [<name>]
```

Description

Displays the current configuration of the specified audit message action. If no audit message action is specified, displays a list of all audit message actions currently configured on the NetScaler appliance.

Parameters**name**

Name of the audit message action.

[Top](#)

audit stats

show audit stats

Synopsis

```
show audit stats - alias for 'stat audit'
```

Description

show audit stats is an alias for stat audit

audit messages

show audit messages

Synopsis

show audit messages [-logLevel <logLevel> ...] [-numOfMesgs <positive_integer>]

Description

Displays the most recent audit log messages.

Parameters

logLevel

Audit log level filter, which specifies the types of events to display. The following loglevels are valid: * ALL - All events. * EMERGENCY - Events that indicate an immediate crisis on the server. * ALERT - Events that might require action. * CRITICAL - Events that indicate an imminent server crisis. * ERROR - Events that indicate some type of error. * WARNING - Events that require action in the near future. * NOTICE - Events that the administrator should know about. * INFORMATIONAL - All but low-level events. * DEBUG - All events, in extreme detail.

numOfMesgs

Number of log messages to be displayed. Default value: 20 Minimum value: 1 Maximum value: 256

audit syslogParams

[[set](#) | [unset](#) | [show](#)]

set audit syslogParams

Synopsis

set audit syslogParams [-serverIP <ip_addr|ipv6_addr|*>] [-serverPort <port>] [-dateFormat <dateFormat>] [-logLevel <logLevel> ...] [-logFacility <logFacility>] [-tcp (NONE | ALL)] [-acl (ENABLED | DISABLED)] [-timeZone (GMT_TIME | LOCAL_TIME)] [-userDefinedAuditlog (YES | NO)] [-appflowExport (ENABLED | DISABLED)]

Description

Modifies the syslog parameters. Changes the IP, the port, or the logging parameters for logs sent to syslog.

Parameters

serverIP

IP address of the syslog server.

serverPort

Port on which the syslog server accepts connections. Minimum value: 1

dateFormat

Format of dates in the logs. Supported formats are: * MMDDYYYY - U.S. style month/date/year format. * DDMMYYYY. European style -date/month/year format. * YYYYMMDD - ISO style year/month/date format. Possible values: MMDDYYYY, DDMMYYYY, YYYYMMDD

logLevel

Types of information to be logged. Available settings function as follows: * ALL - All events. * EMERGENCY - Events that indicate an immediate crisis on the server. * ALERT - Events that might require action. * CRITICAL - Events that indicate an imminent server crisis. * ERROR - Events that indicate some type of error. * WARNING - Events that require action in the near future. * NOTICE - Events that the administrator should know about. * INFORMATIONAL - All but low-level events. * DEBUG - All events, in extreme detail. * NONE - No events.

logFacility

Facility value, as defined in RFC 3164, assigned to the log message. Log facility values are numbers 0 to 7 (LOCAL0 through LOCAL7). Each number indicates where a specific message originated from, such as the NetScaler appliance itself, the VPN, or external. Possible values: LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7

tcp

Log TCP messages. Possible values: NONE, ALL

acl

Log access control list (ACL) messages. Possible values: ENABLED, DISABLED

timeZone

Time zone used for date and timestamps in the logs. Available settings function as follows: * GMT_TIME - Coordinated Universal Time. * LOCAL_TIME Use the server's timezone setting. Possible values: GMT_TIME, LOCAL_TIME

userDefinedAuditlog

Log user-configurable log messages to syslog. Setting this parameter to NO causes audit to ignore all user-configured message actions. Setting this parameter to YES causes audit to log user-configured message actions that meet the other logging criteria. Possible values: YES, NO

appflowExport

Export log messages to AppFlow collectors. Appflow collectors are entities to which log messages can be sent so that some action can be performed on them. Possible values: ENABLED, DISABLED

[Top](#)

unset audit syslogParams**Synopsis**

```
unset audit syslogParams [-serverIP] [-serverPort] [-logLevel] [-dateFormat] [-logFacility] [-tcp] [-acl] [-timeZone] [-userDefinedAuditlog] [-appflowExport]
```

Description

Removes the existing syslog parameter settings. Attributes for which a default value is available revert to their default values. See the set audit syslogParams command for descriptions of the parameters..Refer to the set audit syslogParams command for meanings of the arguments.

[Top](#)

show audit syslogParams

Synopsis

show audit syslogParams

Description

Displays the current syslog parameter settings.

[Top](#)

audit nslogParams

[[set](#) | [unset](#) | [show](#)]

set audit nslogParams

Synopsis

```
set audit nslogParams [-serverIP <ip_addr|ipv6_addr|*>] [-serverPort <port>] [-dateFormat <dateFormat>] [-logLevel <logLevel> ...] [-logFacility <logFacility>] [-tcp ( NONE | ALL )] [-acl ( ENABLED | DISABLED )] [-timeZone ( GMT_TIME | LOCAL_TIME )] [-userDefinedAuditlog ( YES | NO )] [-appflowExport ( ENABLED | DISABLED )]
```

Description

Modifies the specified nslog parameters. Changes the IP address, the port, or the logging parameters for logs sent to nslog.

Parameters

serverIP

IP address of the nslog server.

serverPort

Port on which the nslog server accepts connections. Minimum value: 1

dateFormat

Format of dates in the logs. Supported formats are: * MMDDYYYY - U.S. style month/date/year format. * DDMMYYYY - European style date/month/year format. * YYYYMMDD - ISO style year/month/date format. Possible values: MMDDYYYY, DDMMYYYY, YYYYMMDD

logLevel

Types of information to be logged. Available settings function as follows: * ALL - All events. * EMERGENCY - Events that indicate an immediate crisis on the server. * ALERT - Events that might require action. * CRITICAL - Events that indicate an imminent server crisis. * ERROR - Events that indicate some type of error. * WARNING - Events that require action in the near future. * NOTICE - Events that the administrator should know about. * INFORMATIONAL - All but low-level events. * DEBUG - All events, in extreme detail. * NONE - No events.

logFacility

Facility value, as defined in RFC 3164, assigned to the log message. Log facility values are numbers 0 to 7 (LOCAL0 through LOCAL7). Each number indicates where a specific message originated from, such as the NetScaler appliance itself, the VPN, or

external. Possible values: LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7

tcp

Configure auditing to log TCP messages. Possible values: NONE, ALL

acl

Configure auditing to log access control list (ACL) messages. Possible values: ENABLED, DISABLED

timeZone

Time zone used for date and timestamps in the logs. Supported settings are: * GMT_TIME - Coordinated Universal Time. * LOCAL_TIME - Use the server's timezone setting. Possible values: GMT_TIME, LOCAL_TIME

userDefinedAuditlog

Log user-configurable log messages to nslog. Setting this parameter to NO causes auditing to ignore all user-configured message actions. Setting this parameter to YES causes auditing to log user-configured message actions that meet the other logging criteria. Possible values: YES, NO

appflowExport

Export log messages to AppFlow collectors. Appflow collectors are entities to which log messages can be sent so that some action can be performed on them. Possible values: ENABLED, DISABLED

[Top](#)

unset audit nslogParams

Synopsis

```
unset audit nslogParams [-serverIP] [-serverPort] [-logLevel] [-dateFormat] [-logFacility] [-tcp] [-acl] [-timeZone] [-userDefinedAuditlog] [-appflowExport]
```

Description

Removes the existing nslog parameter settings. Attributes for which a default value is available revert to their default values. See the set audit nslogParams command for a description of the parameters..Refer to the set audit nslogParams command for meanings of the arguments.

[Top](#)

show audit nslogParams

Synopsis

```
show audit nslogParams
```

Description

Displays the current nslog parameter settings.

[Top](#)

Authentication Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [authentication radiusAction](#)
- ♦ [authentication ldapAction](#)
- ♦ [authentication tacacsAction](#)
- ♦ [authentication negotiateAction](#)
- ♦ [authentication samlAction](#)
- ♦ [authentication certAction](#)
- ♦ [authentication localPolicy](#)
- ♦ [authentication radiusPolicy](#)
- ♦ [authentication certPolicy](#)
- ♦ [authentication ldapPolicy](#)
- ♦ [authentication tacacsPolicy](#)
- ♦ [authentication negotiatePolicy](#)
- ♦ [authentication samlPolicy](#)
- ♦ [authentication vserver](#)
- ♦ [authentication authnProfile](#)

authentication radiusAction

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add authentication radiusAction

Synopsis

```
add authentication radiusAction <name> {-serverIP <ip_addr|ipv6_addr|*>} [-serverPort <port>] [-authTimeout <positive_integer>] {-radKey } [-radNASip ( ENABLED | DISABLED )] [-radNASid <string>] [-radVendorID <positive_integer>] [-radAttributeType <positive_integer>] [-radGroupsPrefix <string>] [-radGroupSeparator <string>] [-passEncoding <passEncoding>] [-ipVendorID <positive_integer>] [-ipAttributeType <positive_integer>] [-accounting ( ON | OFF )] [-pwdVendorID <positive_integer>] [-pwdAttributeType <positive_integer>]] [-defaultAuthenticationGroup <string>] [-callingstationid ( ENABLED | DISABLED )]
```

Description

Creates an action (profile) for a RADIUS server. The profile contains all configuration data necessary to communicate with that RADIUS server.

Parameters

name

Name for the RADIUS action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.), pound (#), space (), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the RADIUS action is added.

serverIP

IP address assigned to the RADIUS server.

serverPort

Port number on which the RADIUS server listens for connections. Default value: 1812
Minimum value: 1

authTimeout

Number of seconds the NetScaler appliance waits for a response from the RADIUS server. Default value: 3 Minimum value: 1

radKey

Key shared between the RADIUS server and the NetScaler appliance. Required to allow the NetScaler appliance to communicate with the RADIUS server.

radNASip

If enabled, the NetScaler appliance IP address (NSIP) is sent to the RADIUS server as the Network Access Server IP (NASIP) address. The RADIUS protocol defines the meaning and use of the NASIP address. Possible values: ENABLED, DISABLED

radNASid

If configured, this string is sent to the RADIUS server as the Network Access Server ID (NASID).

radVendorID

RADIUS vendor ID attribute, used for RADIUS group extraction. Minimum value: 1

radAttributeType

RADIUS attribute type, used for RADIUS group extraction. Minimum value: 1

radGroupsPrefix

RADIUS groups prefix string. This groups prefix precedes the group names within a RADIUS attribute for RADIUS group extraction.

radGroupSeparator

RADIUS group separator string The group separator delimits group names within a RADIUS attribute for RADIUS group extraction.

passEncoding

Encoding type for passwords in RADIUS packets that the NetScaler appliance sends to the RADIUS server. Possible values: pap, chap, mschapv1, mschapv2 Default value: AAA_PAP

ipVendorID

Vendor ID of the intranet IP attribute in the RADIUS response. NOTE: A value of 0 indicates that the attribute is not vendor encoded.

ipAttributeType

Remote IP address attribute type in a RADIUS response. Minimum value: 1

accounting

Whether the RADIUS server is currently accepting accounting messages. Possible values: ON, OFF

pwdVendorID

Vendor ID of the attribute, in the RADIUS response, used to extract the user password. Minimum value: 1

pwdAttributeType

Vendor-specific password attribute type in a RADIUS response. Minimum value: 1

defaultAuthenticationGroup

This is the default group that is chosen when the authentication succeeds in addition to extracted groups. Maximum value: 64

callingstationid

Send Calling-Station-ID of the client to the RADIUS server. IP Address of the client is sent as its Calling-Station-ID. Possible values: ENABLED, DISABLED Default value: DISABLED

[Top](#)

rm authentication radiusAction

Synopsis

rm authentication radiusAction <name>

Description

Removes a RADIUS profile (action). An action cannot be removed as long as it is bound to a policy.

Parameters

name

Name of the action to be removed.

[Top](#)

set authentication radiusAction

Synopsis

set authentication radiusAction <name> [-serverIP <ip_addr|ipv6_addr|*>] [-serverPort <port>] [-authTimeout <positive_integer>] {-radKey } [-radNASip (ENABLED | DISABLED)] [-radNASid <string>] [-radVendorID <positive_integer>] [-radAttributeType <positive_integer>] [-radGroupsPrefix <string>] [-radGroupSeparator <string>] [-passEncoding <passEncoding>] [-ipVendorID <positive_integer>] [-ipAttributeType <positive_integer>] [-accounting (ON | OFF)] [-pwdVendorID <positive_integer>] [-pwdAttributeType <positive_integer>] [-defaultAuthenticationGroup <string>] [-callingstationid (ENABLED | DISABLED)]

Description

Configures a RADIUS server profile (action). The profile contains all configuration data needed to communicate with that RADIUS server.

Parameters

name

Name of the RADIUS profile.

serverIP

IP address assigned to the RADIUS server.

serverPort

Port number on which the RADIUS server listens for connections. Default value: 1812
Minimum value: 1

authTimeout

Number of seconds the NetScaler appliance waits for a response from the RADIUS server. Default value: 3 Minimum value: 1

radKey

Key shared between the RADIUS server and the NetScaler appliance. Required to allow the NetScaler appliance to communicate with the RADIUS server.

radNASip

If enabled, the NetScaler appliance IP address (NSIP) is sent to the RADIUS server as the Network Access Server IP (NASIP) address. The RADIUS protocol defines the meaning and use of the NASIP address. Possible values: ENABLED, DISABLED

radNASid

If configured, this string is sent to the RADIUS server as the Network Access Server ID (NASID).

radVendorID

RADIUS vendor ID attribute, used for RADIUS group extraction. Minimum value: 1

radAttributeType

RADIUS attribute type, used for RADIUS group extraction. Minimum value: 1

radGroupsPrefix

RADIUS groups prefix string. This groups prefix precedes the group names within a RADIUS attribute for RADIUS group extraction.

radGroupSeparator

RADIUS group separator string The group separator delimits group names within a RADIUS attribute for RADIUS group extraction.

passEncoding

Encoding type for passwords in RADIUS packets that the NetScaler appliance sends to the RADIUS server. Possible values: pap, chap, mschapv1, mschapv2 Default value: AAA_PAP

ipVendorID

Vendor ID of the intranet IP attribute in the RADIUS response. NOTE: A value of 0 indicates that the attribute is not vendor encoded.

ipAttributeType

Remote IP address attribute type in a RADIUS response. Minimum value: 1

accounting

Whether the RADIUS server is currently accepting accounting messages. Possible values: ON, OFF

pwdVendorID

Vendor ID of the attribute, in the RADIUS response, used to extract the user password. Minimum value: 1

defaultAuthenticationGroup

This is the default group that is chosen when the authentication succeeds in addition to extracted groups. Maximum value: 64

callingstationid

Send Calling-Station-ID of the client to the RADIUS server. IP Address of the client is sent as its Calling-Station-ID. Possible values: ENABLED, DISABLED Default value: DISABLED

[Top](#)

unset authentication radiusAction

Synopsis

```
unset authentication radiusAction <name> [-serverIP] [-serverPort] [-authTimeout] [-radNASip] [-radNASid] [-radVendorID] [-radAttributeType] [-radGroupsPrefix] [-radGroupSeparator] [-passEncoding] [-ipVendorID] [-ipAttributeType] [-accounting] [-pwdVendorID] [-pwdAttributeType] [-defaultAuthenticationGroup] [-callingstationid]
```

Description

Use this command to remove authentication radiusAction settings. Refer to the set authentication radiusAction command for meanings of the arguments.

[Top](#)

show authentication radiusAction

Synopsis

```
show authentication radiusAction [<name>]
```

Description

Displays the current configuration settings for the specified RADIUS profile (action).

Parameters

name

Name of the RADIUS profile.

[Top](#)

authentication ldapAction

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add authentication ldapAction

Synopsis

```
add authentication ldapAction <name> [-serverIP <ip_addr|ipv6_addr|*>] [-serverPort
<port>] [-authTimeout <positive_integer>] [-ldapBase <string>] [-ldapBindDn <string>] {-
ldapBindDnPassword } [-ldapLoginName <string>] [-searchFilter <string>] [-
groupAttrName <string>] [-subAttributeName <string>] [-secType <secType>] [-svrType
( AD | NDS )] [-ssoNameAttribute <string>] [-authentication ( ENABLED | DISABLED )] [-
requireUser ( YES | NO )] [-passwdChange ( ENABLED | DISABLED )] [-
nestedGroupExtraction ( ON | OFF )] [-maxNestingLevel <positive_integer>] [-
groupSearchSubAttribute <string>] [-groupSearchFilter <string>]] [-followReferrals ( ON
| OFF )] [-maxLDAPReferrals <positive_integer>]] [-validateServerCert ( YES | NO )] [-
ldapHostname <string>] [-groupNameIdentifier <string>] [-groupSearchAttribute
<string>] [-defaultAuthenticationGroup <string>]
```

Description

Creates an action (profile) for an LDAP server. This profile contains all configuration data needed to communicate with that LDAP server.

Parameters

name

Name for the new LDAP action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.), pound (#), space (), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the LDAP action is added. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication action" or 'my authentication action').

serverIP

IP address assigned to the LDAP server.

serverPort

Port on which the LDAP server accepts connections. Default value: 389 Minimum value: 1

authTimeout

Number of seconds the NetScaler appliance waits for a response from the RADIUS server. Default value: 3 Minimum value: 1

ldapBase

Base (node) from which to start LDAP searches. If the LDAP server is running locally, the default value of base is dc=netScaler, dc=com.

ldapBindDn

Full distinguished name (DN) that is used to bind to the LDAP server. Default: cn=Manager,dc=netScaler,dc=com

ldapBindDnPassword

Password used to bind to the LDAP server.

ldapLoginName

LDAP login name attribute. The NetScaler appliance uses the LDAP login name to query external LDAP servers or Active Directories.

searchFilter

String to be combined with the default LDAP user search string to form the search value. For example, if the search filter `""vpnallowed=true""` is combined with the LDAP login name `""samaccount""` and the user-supplied username is `""bob""`, the result is the LDAP search string `""(&(vpnallowed=true)(samaccount=bob)""` (Be sure to enclose the search string in two sets of double quotation marks; both sets are needed.).

groupAttrName

LDAP group attribute name. Used for group extraction on the LDAP server.

subAttributeName

LDAP group sub-attribute name. Used for group extraction from the LDAP server.

secType

Type of security used for communications between the NetScaler appliance and the LDAP server. For the PLAINTEXT setting, no encryption is required. Possible values: PLAINTEXT, TLS, SSL Default value: AAA_LDAP_PLAINTEXT

svrType

The type of LDAP server. Possible values: AD, NDS Default value: AAA_LDAP_SERVER_TYPE_DEFAULT

ssoNameAttribute

LDAP single signon (SSO) attribute. The NetScaler appliance uses the SSO name attribute to query external LDAP servers or Active Directories for an alternate username.

authentication

Perform LDAP authentication. If authentication is disabled, any LDAP authentication attempt returns authentication success if the user is found. CAUTION! Authentication should be disabled only for authorization group extraction or where other (non-LDAP) authentication methods are in use and either bound to a primary list or flagged as secondary. Possible values: ENABLED, DISABLED Default value: ENABLED

requireUser

Require a successful user search for authentication. Possible values: YES, NO Default value: YES

passwdChange

Allow password change requests. Possible values: ENABLED, DISABLED Default value: DISABLED

nestedGroupExtraction

Allow nested group extraction, in which the NetScaler appliance queries external LDAP servers to determine whether a group is part of another group. Possible values: ON, OFF Default value: OFF

maxNestingLevel

If nested group extraction is ON, specifies the number of levels up to which group extraction is performed. Default value: 2 Minimum value: 2

followReferrals

Setting this option to ON enables following LDAP referrals received from the LDAP server. Possible values: ON, OFF Default value: OFF

maxLDAPReferrals

Specifies the maximum number of nested referrals to follow. Default value: 1 Minimum value: 1

validateServerCert

When to validate LDAP server certs Possible values: YES, NO Default value: NO

ldapHostname

Hostname for the LDAP server. If -validateServerCert is ON then this must be the host name on the certificate from the LDAP server. A hostname mismatch will cause a connection failure.

groupNameIdentifier

Name that uniquely identifies a group in LDAP or Active Directory.

groupSearchAttribute

LDAP group search attribute. Used to determine to which groups a group belongs.

groupSearchSubAttribute

LDAP group search subattribute. Used to determine to which groups a group belongs.

groupSearchFilter

String to be combined with the default LDAP group search string to form the search value. For example, the group search filter ""vpnallowed=true"" when combined with the group identifier ""samaccount"" and the group name ""g1"" yields the LDAP search string ""(&(vpnallowed=true)(samaccount=g1)"". (Be sure to enclose the search string in two sets of double quotation marks; both sets are needed.)

defaultAuthenticationGroup

This is the default group that is chosen when the authentication succeeds in addition to extracted groups. Maximum value: 64

[Top](#)

rm authentication ldapAction

Synopsis

rm authentication ldapAction <name>

Description

Removes an LDAP profile (action). NOTE: An action cannot be removed if it is bound to a policy.

Parameters

name

Name of the LDAP profile (action) to be removed.

[Top](#)

set authentication ldapAction

Synopsis

```
set authentication ldapAction <name> [-serverIP <ip_addr|ipv6_addr|*>] [-serverPort
<port>] [-authTimeout <positive_integer>] [-ldapBase <string>] [-ldapBindDn <string>] {-
ldapBindDnPassword } [-ldapLoginName <string>] [-searchFilter <string>] [-
groupAttrName <string>] [-subAttributeName <string>] [-secType <secType>] [-svrType
( AD | NDS )] [-ssoNameAttribute <string>] [-authentication ( ENABLED | DISABLED )] [-
requireUser ( YES | NO )] [-passwdChange ( ENABLED | DISABLED )] [-validateServerCert
( YES | NO )] [-ldapHostname <string>] [-nestedGroupExtraction ( ON | OFF )] [-
maxNestingLevel <positive_integer>] [-groupNameIdentifier <string>] [-
groupSearchAttribute <string> [-groupSearchSubAttribute <string>]] [-groupSearchFilter
<string>] [-followReferrals ( ON | OFF )] [-maxLDAPReferrals <positive_integer>] [-
defaultAuthenticationGroup <string>]
```

Description

Modifies an LDAP server profile (action.) The profile contains all configuration data needed to communicate with that LDAP server.

Parameters

name

Name of the LDAP profile to modify.

serverIP

IP address assigned to the LDAP server.

serverPort

Port on which the LDAP server accepts connections. Default value: 389 Minimum value: 1

authTimeout

Number of seconds the NetScaler appliance waits for a response from the RADIUS server. Default value: 3 Minimum value: 1

ldapBase

Base (node) from which to start LDAP searches. If the LDAP server is running locally, the default value of base is dc=netScaler, dc=com.

ldapBindDn

Full distinguished name (DN) that is used to bind to the LDAP server. Default: cn=Manager,dc=netScaler,dc=com

ldapBindDnPassword

Password used to bind to the LDAP server.

ldapLoginName

LDAP login name attribute. The NetScaler appliance uses the LDAP login name to query external LDAP servers or Active Directories.

searchFilter

String to be combined with the default LDAP user search string to form the search value. For example, if the search filter ""vpnaallowed=true"" is combined with the

LDAP login name ""samaccount"" and the user-supplied username is ""bob"", the result is the LDAP search string ""(&(vpnallowed=true)(samaccount=bob)"" (Be sure to enclose the search string in two sets of double quotation marks; both sets are needed.).

groupAttrName

LDAP group attribute name. Used for group extraction on the LDAP server.

subAttributeName

LDAP group sub-attribute name. Used for group extraction from the LDAP server.

secType

Type of security used for communications between the NetScaler appliance and the LDAP server. For the PLAINTEXT setting, no encryption is required. Possible values: PLAINTEXT, TLS, SSL Default value: AAA_LDAP_PLAINTEXT

svrType

The type of LDAP server. Possible values: AD, NDS Default value: AAA_LDAP_SERVER_TYPE_DEFAULT

ssoNameAttribute

LDAP single signon (SSO) attribute. The NetScaler appliance uses the SSO name attribute to query external LDAP servers or Active Directories for an alternate username.

authentication

Perform LDAP authentication. If authentication is disabled, any LDAP authentication attempt returns authentication success if the user is found. CAUTION! Authentication should be disabled only for authorization group extraction or where other (non-LDAP) authentication methods are in use and either bound to a primary list or flagged as secondary. Possible values: ENABLED, DISABLED Default value: ENABLED

requireUser

Require a successful user search for authentication. Possible values: YES, NO Default value: YES

passwdChange

Allow password change requests. Possible values: ENABLED, DISABLED Default value: DISABLED

validateServerCert

When to validate LDAP server certs Possible values: YES, NO Default value: NO

ldapHostname

Hostname for the LDAP server. If -validateServerCert is ON then this must be the host name on the certificate from the LDAP server. A hostname mismatch will cause a connection failure.

nestedGroupExtraction

Allow nested group extraction, in which the NetScaler appliance queries external LDAP servers to determine whether a group is part of another group. Possible values: ON, OFF Default value: OFF

followReferrals

Setting this option to ON enables following LDAP referrals received from the LDAP server. Possible values: ON, OFF Default value: OFF

defaultAuthenticationGroup

This is the default group that is chosen when the authentication succeeds in addition to extracted groups. Maximum value: 64

[Top](#)

unset authentication ldapAction**Synopsis**

```
unset authentication ldapAction <name> [-serverIP] [-serverPort] [-authTimeout] [-ldapBase] [-ldapBindDn] [-ldapBindDnPassword] [-ldapLoginName] [-searchFilter] [-groupAttrName] [-subAttributeName] [-secType] [-svrType] [-ssoNameAttribute] [-authentication] [-requireUser] [-passwdChange] [-validateServerCert] [-ldapHostname] [-nestedGroupExtraction] [-maxNestingLevel] [-groupNameIdentifier] [-groupSearchAttribute] [-groupSearchSubAttribute] [-groupSearchFilter] [-followReferrals] [-maxLDAPReferrals] [-defaultAuthenticationGroup]
```

Description

Use this command to remove authentication ldapAction settings. Refer to the set authentication ldapAction command for meanings of the arguments.

[Top](#)

show authentication ldapAction**Synopsis**

```
show authentication ldapAction [<name>]
```

Description

Displays the current configuration settings for the specified LDAP profile (action).

Parameters

name

Name of the LDAP profile.

[Top](#)

authentication tacacsAction

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add authentication tacacsAction**Synopsis**

```
add authentication tacacsAction <name> [-serverIP <ip_addr|ipv6_addr|*>] [-serverPort <port>] [-authTimeout <positive_integer>] {-tacacsSecret } [-authorization ( ON | OFF )]
```

```
[-accounting ( ON | OFF )] [-auditFailedCmds ( ON | OFF )] [-  
defaultAuthenticationGroup <string>]
```

Description

Creates an action (profile) for a TACACS+ server. The profile contains all configuration data necessary to communicate with that TACACS+ server.

Parameters

name

Name for the TACACS+ profile (action). Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space (), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after TACACS profile is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication action" or 'my authentication action').

serverIP

IP address assigned to the TACACS+ server.

serverPort

Port number on which the TACACS+ server listens for connections. Default value: 49
Minimum value: 1

authTimeout

Number of seconds the NetScaler appliance waits for a response from the TACACS+ server. Default value: 3 Minimum value: 1

tacacsSecret

Key shared between the TACACS+ server and the NetScaler appliance. Required for allowing the NetScaler appliance to communicate with the TACACS+ server.

authorization

Use streaming authorization on the TACACS+ server. Possible values: ON, OFF

accounting

Whether the TACACS+ server is currently accepting accounting messages. Possible values: ON, OFF

auditFailedCmds

The state of the TACACS+ server that will receive accounting messages. Possible values: ON, OFF

defaultAuthenticationGroup

This is the default group that is chosen when the authentication succeeds in addition to extracted groups. Maximum value: 64

[Top](#)

rm authentication tacacsAction

Synopsis

```
rm authentication tacacsAction <name>
```

Description

Removes a TACACS+ profile (action). A profile cannot be removed as long as it is bound to a policy.

Parameters

name

Name of the profile to be removed.

[Top](#)

set authentication tacacsAction

Synopsis

```
set authentication tacacsAction <name> [-serverIP <ip_addr|ipv6_addr|*>] [-serverPort <port>] [-authTimeout <positive_integer>] {-tacacsSecret } [-authorization ( ON | OFF )] [-accounting ( ON | OFF )] [-auditFailedCmds ( ON | OFF )] [-defaultAuthenticationGroup <string>]
```

Description

Modifies a TACACS+ server profile (action).

Parameters

name

Name of the TACACS+ profile to modify.

serverIP

IP address assigned to the TACACS+ server.

serverPort

Port number on which the TACACS+ server listens for connections. Default value: 49
Minimum value: 1

authTimeout

Number of seconds the NetScaler appliance waits for a response from the TACACS+ server. Default value: 3 Minimum value: 1

tacacsSecret

Key shared between the TACACS+ server and the NetScaler appliance. Required for allowing the NetScaler appliance to communicate with the TACACS+ server.

authorization

Use streaming authorization on the TACACS+ server. Possible values: ON, OFF

accounting

Whether the TACACS+ server is currently accepting accounting messages. Possible values: ON, OFF

auditFailedCmds

The state of the TACACS+ server that will receive accounting messages. Possible values: ON, OFF

defaultAuthenticationGroup

This is the default group that is chosen when the authentication succeeds in addition to extracted groups. Maximum value: 64

[Top](#)

unset authentication tacacsAction**Synopsis**

```
unset authentication tacacsAction <name> [-serverIP] [-serverPort] [-authTimeout] [-tacacsSecret] [-authorization] [-accounting] [-auditFailedCmds] [-defaultAuthenticationGroup]
```

Description

Use this command to remove authentication tacacsAction settings. Refer to the set authentication tacacsAction command for meanings of the arguments.

[Top](#)

show authentication tacacsAction**Synopsis**

```
show authentication tacacsAction [<name>]
```

Description

Displays the current configuration settings for the specified TACACS+ profile (action).

Parameters

name

Name of the TACACS+ profile.

[Top](#)

authentication negotiateAction

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add authentication negotiateAction**Synopsis**

```
add authentication negotiateAction <name> {-domain <string>} {-domainUser <string>} {-domainUserPasswd } {-OU <string>} [-defaultAuthenticationGroup <string>] [-keytab <string>]
```

Description

Creates an action (profile) for an Active Directory (AD) server that is used as a Kerberos Key Distribution Center (KDC). The profile contains all configuration data necessary to communicate with that AD KDC server.

Parameters

name

Name for the AD KDC server profile (negotiate action). Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space (), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after AD KDC server profile is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication action" or 'my authentication action').

domain

Domain name of the AD KDC server.

domainUser

User name that the NetScaler appliance uses to join the AD KDC server domain. The NetScaler appliance uses the domain user name to check the health of the AD KDC server.

domainUserPasswd

Password that the NetScaler appliance uses to join the AD KDC server domain.

OU

Active Directory organizational units (OU) attribute.

defaultAuthenticationGroup

This is the default group that is chosen when the authentication succeeds in addition to extracted groups. Maximum value: 64

keytab

The path to the keytab file

[Top](#)

rm authentication negotiateAction

Synopsis

```
rm authentication negotiateAction <name>
```

Description

Removes an AD KDC server profile (negotiate action). An action cannot be removed if it is bound to a policy.

Parameters

name

Name of the AD KDC server profile to be removed.

[Top](#)

set authentication negotiateAction

Synopsis

```
set authentication negotiateAction <name> [-domain <string>] [-domainUser <string>] [-domainUserPasswd <string>] [-OU <string>] [-defaultAuthenticationGroup <string>] [-keytab <string>]
```

Description

Configures an AD KDC server profile (negotiate action).

Parameters

name

Name of the AD KDC server profile.

domain

Domain name of the AD KDC server.

domainUser

User name that the NetScaler appliance uses to join the AD KDC server domain. The NetScaler appliance uses the domain user name to check the health of the AD KDC server.

domainUserPasswd

Password that the NetScaler appliance uses to join the AD KDC server domain.

OU

Active Directory organizational units (OU) attribute.

defaultAuthenticationGroup

This is the default group that is chosen when the authentication succeeds in addition to extracted groups. Maximum value: 64

keytab

The path to the keytab file

[Top](#)

unset authentication negotiateAction

Synopsis

```
unset authentication negotiateAction <name> [-domain] [-domainUser] [-domainUserPasswd] [-OU] [-defaultAuthenticationGroup]
```

Description

Use this command to remove authentication negotiateAction settings. Refer to the set authentication negotiateAction command for meanings of the arguments.

[Top](#)

show authentication negotiateAction

Synopsis

```
show authentication negotiateAction [<name>]
```

Description

Displays the current configuration settings for the specified AD KDC server profile (negotiate action).

Parameters

name

Name of the AD KDC server profile.

[Top](#)

authentication samlAction

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add authentication samlAction

Synopsis

```
add authentication samlAction <name> {-samlIdPCertName <string>} {-samlSigningCertName <string>} {-samlRedirectUrl <string>} {-samlUserField <string>} {-samlRejectUnsignedAssertion ( ON | OFF )} {-samlIssuerName <string>} {-samlTwoFactor ( ON | OFF )} [-defaultAuthenticationGroup <string>]
```

Description

Creates an action (profile) for a Security Assertion Markup Language (SAML) server. The profile contains all configuration data necessary to communicate with that SAML server.

Parameters

name

Name for the SAML server profile (action). Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space (), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after SAML profile is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication action" or 'my authentication action').

samlIdPCertName

Name of the SAML server as given in that server's SSL certificate.

samlSigningCertName

Name of the signing authority as given in the SAML server's SSL certificate.

samlRedirectUrl

URL to which users are redirected after successful authentication.

samlUserField

SAML user ID, as given in the SAML assertion.

samlRejectUnsignedAssertion

Reject unsigned SAML assertions. Possible values: ON, OFF Default value: ON

samlIssuerName

The name to be used in requests sent from Netscaler to IdP to uniquely identify Netscaler.

samlTwoFactor

Option to enable second factor after SAML Possible values: ON, OFF Default value: NS_OFF

defaultAuthenticationGroup

This is the default group that is chosen when the authentication succeeds in addition to extracted groups. Maximum value: 64

[Top](#)

rm authentication samlAction

Synopsis

```
rm authentication samlAction <name>
```

Description

Removes a SAML profile (action). An action cannot be removed if it is bound to a policy.

Parameters

name

Name of the SAML profile to be removed.

[Top](#)

set authentication samlAction

Synopsis

```
set authentication samlAction <name> [-samlIdPCertName <string>] [-samlSigningCertName <string>] [-samlRedirectUrl <string>] [-samlUserField <string>] [-samlRejectUnsignedAssertion ( ON | OFF )] [-samlIssuerName <string>] [-samlTwoFactor ( ON | OFF )] [-defaultAuthenticationGroup <string>]
```

Description

Modifies the specified parameters of a SAML server profile (action).

Parameters

name

Name of the SAML profile (action) to modify.

samlIdPCertName

Name of the SAML server as given in that server's SSL certificate.

samlSigningCertName

Name of the signing authority as given in the SAML server's SSL certificate.

samlRedirectUrl

URL to which users are redirected after successful authentication.

samlUserField

SAML user ID, as given in the SAML assertion.

samlRejectUnsignedAssertion

Reject unsigned SAML assertions. Possible values: ON, OFF Default value: ON

samlIssuerName

The name to be used in requests sent from Netscaler to IdP to uniquely identify Netscaler.

samlTwoFactor

Option to enable second factor after SAML Possible values: ON, OFF Default value: NS_OFF

defaultAuthenticationGroup

This is the default group that is chosen when the authentication succeeds in addition to extracted groups. Maximum value: 64

[Top](#)

unset authentication samlAction

Synopsis

```
unset authentication samlAction <name> [-samlIdPCertName] [-samlSigningCertName]
[-samlRedirectUrl] [-samlUserField] [-samlRejectUnsignedAssertion] [-samlIssuerName]
[-samlTwoFactor] [-defaultAuthenticationGroup]
```

Description

Use this command to remove authentication samlAction settings. Refer to the set authentication samlAction command for meanings of the arguments.

[Top](#)

show authentication samlAction

Synopsis

```
show authentication samlAction [<name>]
```

Description

Displays the current configuration settings for the specified SAML server profile (action).

Parameters

name

Name of the SAML server profile.

[Top](#)

authentication certAction

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add authentication certAction

Synopsis

```
add authentication certAction <name> [-twoFactor ( ON | OFF )] [-userNameField
<string>] [-groupNameField <string>] [-defaultAuthenticationGroup <string>]
```

Description

Adds an action (profile) for a client certificate (cert) authentication server. The profile contains all configuration data necessary to communicate with that client cert authentication server.

Parameters

name

Name for the client cert authentication server profile (action). Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.), pound (#), space (), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after certificate action is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication action" or 'my authentication action').

twoFactor

Enables or disables two-factor authentication. Two factor authentication is client cert authentication followed by password authentication. Possible values: ON, OFF
Default value: OFF

userNameField

Client-cert field from which the username is extracted. Must be set to either ""Subject"" and ""Issuer"" (include both sets of double quotation marks). Format: <field>:<subfield>.

groupNameField

Client-cert field from which the group is extracted. Must be set to either ""Subject"" and ""Issuer"" (include both sets of double quotation marks). Format: <field>:<subfield>

defaultAuthenticationGroup

This is the default group that is chosen when the authentication succeeds in addition to extracted groups. Maximum value: 64

Example

```
add authentication certaction -twoFactor ON -
userNameField "Subject:CN" -groupNameField
"Subject:OU"
```

[Top](#)

rm authentication certAction

Synopsis

rm authentication certAction <name>

Description

Removes an existing client cert authentication server profile (action).

Parameters

name

Name of the profile to be removed.

[Top](#)

set authentication certAction

Synopsis

set authentication certAction <name> [-twoFactor (ON | OFF)] [-userNameField <string>] [-groupNameField <string>] [-defaultAuthenticationGroup <string>]

Description

Configures a client cert authentication server profile (action).

Parameters

name

Name of the client cert server profile.

twoFactor

Enables or disables two-factor authentication. Two factor authentication is client cert authentication followed by password authentication. Possible values: ON, OFF
Default value: OFF

userNameField

Client-cert field from which the username is extracted. Must be set to either ""Subject"" and ""Issuer"" (include both sets of double quotation marks). Format: <field>:<subfield>.

groupNameField

Client-cert field from which the group is extracted. Must be set to either ""Subject"" and ""Issuer"" (include both sets of double quotation marks). Format: <field>:<subfield>

defaultAuthenticationGroup

This is the default group that is chosen when the authentication succeeds in addition to extracted groups. Maximum value: 64

Example

```
set authentication certaction -twoFactor ON -
userNameField "Subject:CN" -groupNameField
"Subject:OU"
```

[Top](#)**unset authentication certAction****Synopsis**

```
unset authentication certAction <name> [-twoFactor] [-userNameField] [-
groupNameField] [-defaultAuthenticationGroup]
```

Description

Use this command to remove authentication certAction settings. Refer to the set authentication certAction command for meanings of the arguments.

[Top](#)**show authentication certAction****Synopsis**

```
show authentication certAction [<name>]
```

Description

Displays the current configuration settings for the specified client cert authentication server profile (action).

Parameters

name

Name of the client cert server profile (action).

[Top](#)**authentication localPolicy**

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add authentication localPolicy**Synopsis**

```
add authentication localPolicy <name> <rule>
```

Description

Adds a policy for the NetScaler appliance to locally authenticate a user. The policy contains criteria that specify when and how to authenticate a user.

Parameters

name

Name for the local authentication policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space (), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after local policy is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy" or 'my authentication policy').

rule

Name of the NetScaler named rule, or a default syntax expression, that the policy uses to perform the authentication.

[Top](#)

rm authentication localPolicy

Synopsis

rm authentication localPolicy <name>

Description

Removes the specified local authentication policy.

Parameters

name

Name of the local policy to remove.

[Top](#)

set authentication localPolicy

Synopsis

set authentication localPolicy <name> -rule <expression>

Description

Configures the specified local authentication policy.

Parameters

name

Name of the local authentication policy.

rule

Name of the NetScaler named rule, or a default syntax expression, that the policy uses to perform the authentication.

[Top](#)

unset authentication localPolicy

Synopsis

unset authentication localPolicy <name> -rule

Description

Use this command to remove authentication localPolicy settings. Refer to the set authentication localPolicy command for meanings of the arguments.

[Top](#)

show authentication localPolicy

Synopsis

show authentication localPolicy [<name>]

Description

Displays the current settings for the specified local authentication policy. If no policy name is provided, displays a list of all local authentication policies currently configured on the NetScaler appliance.

Parameters

name

Name of the local authentication policy.

[Top](#)

authentication radiusPolicy

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add authentication radiusPolicy

Synopsis

add authentication radiusPolicy <name> <rule> [<reqAction>]

Description

Adds a RADIUS authentication policy. The policy defines the criteria under which the NetScaler appliance attempts to authenticate the user with the RADIUS server.

Parameters

name

Name for the RADIUS authentication policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space (), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after RADIUS policy is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy" or 'my authentication policy').

rule

Name of the NetScaler named rule, or a default syntax expression, that the policy uses to determine whether to attempt to authenticate the user with the RADIUS server.

reqAction

Name of the RADIUS action to perform if the policy matches.

[Top](#)

rm authentication radiusPolicy

Synopsis

rm authentication radiusPolicy <name>

Description

Removes a RADIUS authentication policy.

Parameters

name

Name of the RADIUS authentication policy to remove.

[Top](#)

set authentication radiusPolicy

Synopsis

set authentication radiusPolicy <name> [-rule <expression>] [-reqAction <string>]

Description

Configures the specified RADIUS authentication policy.

Parameters

name

Name of the RADIUS authentication policy.

rule

Name of the NetScaler named rule, or a default syntax expression, that the policy uses to determine whether to attempt to authenticate the user with the RADIUS server.

reqAction

Name of the RADIUS action to perform if the policy matches.

[Top](#)

unset authentication radiusPolicy

Synopsis

unset authentication radiusPolicy <name> [-rule] [-reqAction]

Description

Use this command to remove authentication radiusPolicy settings. Refer to the set authentication radiusPolicy command for meanings of the arguments.

[Top](#)

show authentication radiusPolicy

Synopsis

show authentication radiusPolicy [<name>]

Description

Displays the current settings for the specified RADIUS authentication policy. If no policy name is provided, displays a list of all RADIUS authentication policies currently configured on the NetScaler appliance.

Parameters

name

Name of the RADIUS authentication policy.

[Top](#)

authentication certPolicy

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add authentication certPolicy

Synopsis

add authentication certPolicy <name> <rule> [<reqAction>]

Description

Adds a client certificate (cert) authentication policy. The policy defines the criteria under which the NetScaler appliance attempts to authenticate the user with the specified client cert authentication server.

Parameters

name

Name for the client certificate authentication policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space (), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after cert authentication policy is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy" or 'my authentication policy').

rule

Name of the NetScaler named rule, or a default syntax expression, that the policy uses to determine whether to attempt to authenticate the user with the authentication server.

reqAction

Name of the client cert authentication action to be performed if the policy matches.

[Top](#)

rm authentication certPolicy

Synopsis

rm authentication certPolicy <name>

Description

Removes a client cert authentication policy.

Parameters

name

Name of the client cert policy to remove.

[Top](#)

set authentication certPolicy

Synopsis

set authentication certPolicy <name> [-rule <expression>] [-reqAction <string>]

Description

Configures the specified client cert authentication policy.

Parameters

name

Name of the client cert policy.

rule

Name of the NetScaler named rule, or a default syntax expression, that the policy uses to determine whether to attempt to authenticate the user with the authentication server.

reqAction

Name of the client cert authentication action to be performed if the policy matches.

[Top](#)

unset authentication certPolicy

Synopsis

unset authentication certPolicy <name> [-rule] [-reqAction]

Description

Use this command to remove authentication certPolicy settings. Refer to the set authentication certPolicy command for meanings of the arguments.

[Top](#)

show authentication certPolicy

Synopsis

show authentication certPolicy [<name>]

Description

Displays the current settings for the specified client cert authentication policy. If no policy name is provided, displays a list of all client cert authentication policies currently configured on the NetScaler appliance.

Parameters

name

Name of the client cert authentication policy.

[Top](#)

authentication ldapPolicy

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add authentication ldapPolicy

Synopsis

add authentication ldapPolicy <name> <rule> [<reqAction>]

Description

Adds an LDAP authentication policy. The policy defines the criteria under which the NetScaler appliance attempts to authenticate the user with the specified LDAP server.

Parameters

name

Name for the LDAP policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space (), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after LDAP policy is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy" or 'my authentication policy').

rule

Name of the NetScaler named rule, or a default syntax expression, that the policy uses to determine whether to attempt to authenticate the user with the LDAP server.

reqAction

Name of the LDAP action to perform if the policy matches.

[Top](#)

rm authentication ldapPolicy

Synopsis

rm authentication ldapPolicy <name>

Description

Removes an LDAP policy.

Parameters

name

Name of the LDAP policy to remove.

[Top](#)

set authentication ldapPolicy

Synopsis

set authentication ldapPolicy <name> [-rule <string>] [-reqAction <string>]

Description

Configures the specified LDAP policy.

Parameters

name

Name of the LDAP policy.

rule

The new rule to associate with the policy.

reqAction

The new LDAP action to associate with the policy.

[Top](#)

unset authentication ldapPolicy

Synopsis

unset authentication ldapPolicy <name> [-rule] [-reqAction]

Description

Use this command to remove authentication ldapPolicy settings. Refer to the set authentication ldapPolicy command for meanings of the arguments.

[Top](#)

show authentication ldapPolicy

Synopsis

show authentication ldapPolicy [<name>]

Description

Displays the current settings for the specified LDAP policy. If no policy name is provided, displays a list of all LDAP policies currently configured on the NetScaler appliance.

Parameters

name

Name of the LDAP policy.

[Top](#)

authentication tacacsPolicy

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add authentication tacacsPolicy

Synopsis

add authentication tacacsPolicy <name> <rule> [<reqAction>]

Description

Adds a TACACS+ authentication policy. The policy defines the criteria under which the NetScaler appliance attempts to authenticate the user with the specified TACACS+ server.

Parameters

name

Name for the TACACS+ policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space (), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after TACACS+ policy is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy" or 'my authentication policy').

rule

Name of the NetScaler named rule, or a default syntax expression, that the policy uses to determine whether to attempt to authenticate the user with the TACACS+ server.

reqAction

Name of the TACACS+ action to perform if the policy matches.

[Top](#)

rm authentication tacacsPolicy

Synopsis

rm authentication tacacsPolicy <name>

Description

Removes the specified TACACS+ policy.

Parameters

name

Name of the TACACS+ policy to remove.

[Top](#)

set authentication tacacsPolicy

Synopsis

set authentication tacacsPolicy <name> [-rule <expression>] [-reqAction <string>]

Description

Configures the specified TACACS+ policy.

Parameters

name

Name of the TACACS+ policy.

rule

Name of the NetScaler named rule, or a default syntax expression, that the policy uses to determine whether to attempt to authenticate the user with the TACACS+ server.

reqAction

Name of the TACACS+ action to perform if the policy matches.

[Top](#)

unset authentication tacacsPolicy

Synopsis

unset authentication tacacsPolicy <name> [-rule] [-reqAction]

Description

Use this command to remove authentication tacacsPolicy settings. Refer to the set authentication tacacsPolicy command for meanings of the arguments.

[Top](#)

show authentication tacacsPolicy

Synopsis

show authentication tacacsPolicy [<name>]

Description

Displays the current settings for the specified TACACS+ policy. If no policy name is provided, displays a list of all TACACS+ policies currently configured on the NetScaler appliance.

Parameters

name
Name of the TACACS+ policy.

[Top](#)

authentication negotiatePolicy

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add authentication negotiatePolicy

Synopsis

add authentication negotiatePolicy <name> <rule> <reqAction>

Description

Adds an Active Directory (AD) Kerberos Key Distribution Center (KCD) authentication policy (negotiate policy). The policy defines the criteria under which the NetScaler appliance attempts to authenticate the user with the specified AD KCD server.

Parameters

name
Name for the negotiate authentication policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space (), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after AD KCD (negotiate) policy is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy" or 'my authentication policy').

rule
Name of the NetScaler named rule, or a default syntax expression, that the policy uses to determine whether to attempt to authenticate the user with the AD KCD server.

reqAction
Name of the negotiate action to perform if the policy matches.

[Top](#)

rm authentication negotiatePolicy

Synopsis

rm authentication negotiatePolicy <name>

Description

Removes the specified AD KCD (negotiate) policy.

Parameters

name

Name of the negotiate policy to remove.

[Top](#)

set authentication negotiatePolicy

Synopsis

set authentication negotiatePolicy <name> [-rule <expression>] [-reqAction <string>]

Description

Modifies the specified AD KCD (negotiate) policy.

Parameters

name

Name of the negotiate policy to modify.

rule

Name of the NetScaler named rule, or a default syntax expression, that the policy uses to determine whether to attempt to authenticate the user with the AD KCD server.

reqAction

Name of the negotiate action to perform if the policy matches.

[Top](#)

unset authentication negotiatePolicy

Synopsis

unset authentication negotiatePolicy <name> [-rule] [-reqAction]

Description

Use this command to remove authentication negotiatePolicy settings. Refer to the set authentication negotiatePolicy command for meanings of the arguments.

[Top](#)

show authentication negotiatePolicy

Synopsis

show authentication negotiatePolicy [<name>]

Description

Displays the current settings for the specified AD KCD (negotiate) policy. If no policy name is provided, displays a list of all negotiate policies currently configured on the NetScaler appliance.

Parameters**name**

Name of the negotiate policy.

[Top](#)

authentication samlPolicy

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add authentication samlPolicy

Synopsis

add authentication samlPolicy <name> <rule> <reqAction>

Description

Adds a SAML authentication policy. The policy defines the criteria under which the NetScaler appliance attempts to authenticate the user with the specified SAML server.

Parameters**name**

Name for the SAML policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space (), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after SAML policy is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy" or 'my authentication policy').

rule

Name of the NetScaler named rule, or a default syntax expression, that the policy uses to determine whether to attempt to authenticate the user with the SAML server.

reqAction

Name of the SAML authentication action to be performed if the policy matches.

[Top](#)

rm authentication samlPolicy

Synopsis

rm authentication samlPolicy <name>

Description

Removes the specified SAML policy.

Parameters**name**

Name of the policy to remove.

[Top](#)

set authentication samlPolicy

Synopsis

set authentication samlPolicy <name> [-rule <expression>] [-reqAction <string>]

Description

Modifies the specified parameters of a SAML policy.

Parameters

name

Name of the SAML policy to modify.

rule

Name of the NetScaler named rule, or a default syntax expression, that the policy uses to determine whether to attempt to authenticate the user with the SAML server.

reqAction

Name of the SAML authentication action to be performed if the policy matches.

[Top](#)

unset authentication samlPolicy

Synopsis

unset authentication samlPolicy <name> [-rule] [-reqAction]

Description

Use this command to remove authentication samlPolicy settings. Refer to the set authentication samlPolicy command for meanings of the arguments.

[Top](#)

show authentication samlPolicy

Synopsis

show authentication samlPolicy [<name>]

Description

Displays the current settings for the specified SAML policy. If no policy name is provided, displays a list of all SAML policies currently configured on the NetScaler appliance.

Parameters

name

Name of the SAML policy.

[Top](#)

authentication vserver

[[add](#) | [rm](#) | [set](#) | [unset](#) | [bind](#) | [unbind](#) | [enable](#) | [disable](#) | [show](#) | [stat](#) | [rename](#)]

add authentication vserver

Synopsis

```
add authentication vserver <name> <serviceType> (<IPAddress> [-range
<positive_integer>]) <port> [-state ( ENABLED | DISABLED )] [-authentication ( ON |
OFF )] [-AuthenticationDomain <string>] [-comment <string>] [-td <positive_integer>] [-
appflowLog ( ENABLED | DISABLED )] [-maxLoginAttempts <positive_integer> [-
failedLoginTimeout <positive_integer>]]
```

Description

Creates an authentication virtual server.

Parameters

name

Name for the new authentication virtual server. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space (), at (@), equals (=), colon (:), and underscore characters. Can be changed after the authentication virtual server is added by using the rename authentication vserver command. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy" or 'my authentication policy').

serviceType

Protocol type of the authentication virtual server. Always SSL. Possible values: SSL
Default value: NSSVC_SSL

IPAddress

IP address of the authentication virtual server, if a single IP address is assigned to the virtual server.

port

TCP port on which the virtual server accepts connections. Minimum value: 1

state

Initial state of the new virtual server. Possible values: ENABLED, DISABLED
Default value: ENABLED

authentication

Require users to be authenticated before sending traffic through this virtual server.
Possible values: ON, OFF
Default value: ON

AuthenticationDomain

Fully-qualified domain name (FQDN) of the authentication virtual server.

comment

Any comments associated with this virtual server.

td

Traffic Domain ID Maximum value: 4094

appflowLog

Log AppFlow flow information. Possible values: ENABLED, DISABLED Default value: ENABLED

maxLoginAttempts

Maximum Number of login Attempts Minimum value: 1 Maximum value: 255

Example

```
The following example creates an authentication
vserver named myauthenticationvip which supports
SSL portocol and with AAA functionality enabled:
vserver myauthenticationvip SSL 65.219.17.34 443 -
aaa ON
```

[Top](#)

rm authentication vserver

Synopsis

rm authentication vserver <name>@ ...

Description

Removes an authentication virtual server.

Parameters

name

Name of the authentication virtual server to remove.

Example

```
rm vserver authn_vip
```

[Top](#)

set authentication vserver

Synopsis

```
set authentication vserver <name> [-IPAddress <ip_addr|ipv6_addr|*>] [-authentication
( ON | OFF )] [-AuthenticationDomain <string>] [-comment <string>] [-appflowLog
( ENABLED | DISABLED )] [-maxLoginAttempts <positive_integer>] [-failedLoginTimeout
<positive_integer>]
```

Description

Modifies the specified parameters of an existing authentication virtual server.

Parameters

name

Name of the virtual server to modify.

IPAddress

IP address of the authentication virtual server, if a single IP address is assigned to the virtual server.

authentication

Require users to be authenticated before sending traffic through this virtual server.
Possible values: ON, OFF Default value: ON

AuthenticationDomain

Fully-qualified domain name (FQDN) of the authentication virtual server.

comment

Any comments associated with this virtual server.

appflowLog

Log AppFlow flow information. Possible values: ENABLED, DISABLED Default value: ENABLED

maxLoginAttempts

Maximum Number of login Attempts Minimum value: 1 Maximum value: 255

failedLoginTimeout

Failed Login timeout Minimum value: 1

[Top](#)

unset authentication vserver

Synopsis

```
unset authentication vserver <name> [-AuthenticationDomain] [-maxLoginAttempts] [-authentication] [-comment] [-appflowLog]
```

Description

Removes the settings of an existing authentication virtual server. Attributes for which a default value is available revert to their default values. Refer to the set authentication vserver command for descriptions of the parameters..Refer to the set authentication vserver command for meanings of the arguments.

[Top](#)

bind authentication vserver

Synopsis

```
bind authentication vserver <name> [-policy <string> [-priority <positive_integer>] [-secondary] [-groupExtraction]]
```

Description

Binds authentication policies to an authentication virtual server.

Parameters

name

Name of the authentication virtual server to which to bind the policy.

policy

Name of the policy to bind to the virtual server.

[Top](#)

unbind authentication vserver

Synopsis

```
unbind authentication vserver <name> [-policy <string> [-secondary] [-groupExtraction]]
```

Description

Unbinds the specified policy from the specified authentication virtual server.

Parameters

name

Name of the virtual server.

policy

Name of the policy to be unbound.

[Top](#)

enable authentication vserver

Synopsis

```
enable authentication vserver <name>@
```

Description

Enables an authentication virtual server that is disabled. Note: Virtual servers, when added, are normally enabled by default.

Parameters

name

Name of the virtual server to enable.

Example

```
enable vserver authentication1
```

[Top](#)

disable authentication vserver

Synopsis

disable authentication vserver <name>@

Description

Disables an authentication virtual server, taking it out of service.

Parameters

name

Name of the virtual server to disable. Notes: 1. The NetScaler appliance still responds to ARP and/or ping requests for the IP address of disabled virtual servers. 2. Because the virtual server configuration still exists on the NetScaler appliance, you can reenable the virtual server.

Example

```
disable vserver authn_vip
```

[Top](#)

show authentication vserver

Synopsis

show authentication vserver [<name>] show authentication vserver stats - alias for 'stat authentication vserver'

Description

Displays the configuration of the specified authentication virtual server. If no authentication virtual server is specified, displays a list of all authentication virtual servers that are currently configured on the NetScaler appliance.

Parameters

name

Name of the authentication virtual server.

Example

```
show authentication vserver
```

[Top](#)

stat authentication vserver

Synopsis

```
stat authentication vserver [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>]
[-logFile <input_filename>] [-clearstats ( basic | full )]
```

Description

Displays statistics about the specified authentication virtual server. If no authentication virtual server is specified, displays statistics for all authentication virtual servers that are currently configured on the NetScaler appliance.

Parameters

name

Name of the authentication virtual server.

clearstats

Clear the statistics / counters Possible values: basic, full

[Top](#)

rename authentication vserver

Synopsis

```
rename authentication vserver <name>@ <newName>@
```

Description

Rename an authentication virtual server.

Parameters

name

Current name of the authentication virtual server.

newName

New name of the authentication virtual server. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space (), at (@), equals (=), colon (:), and underscore characters. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy" or 'my authentication policy').

Example

```
rename authentication vserver av1 av_new
```

[Top](#)

authentication authnProfile

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add authentication authnProfile

Synopsis

```
add authentication authnProfile <name> {-authnVsName <string>} {-AuthenticationHost <string>} {-AuthenticationDomain <string>} [-AuthenticationLevel <positive_integer>]
```

Description

Creates an authentication profile to hold all authentication related configuration for TM vserver.

Parameters

name

Name for the authentication profile. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space (), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the RADIUS action is added.

authnVsName

Name of the authentication vserver at which authentication should be done.
Maximum value: 128

AuthenticationHost

Hostname of the authentication vserver. Maximum value: 256

AuthenticationDomain

Domain for which TM cookie must to be set. If unspecified, cookie will be set for FQDN. Maximum value: 256

[Top](#)

rm authentication authnProfile

Synopsis

```
rm authentication authnProfile <name>
```

Description

Removes an authentication profile. A profile cannot be removed as long as it is set to a vserver.

Parameters

name

Name of the authentication profile to be removed.

[Top](#)

set authentication authnProfile

Synopsis

set authentication authnProfile <name> [-authnVsName <string>] [-AuthenticationHost <string>] [-AuthenticationDomain <string>] [-AuthenticationLevel <positive_integer>]

Description

Configures an authentication profile.

Parameters

name

Name of the authentication profile.

authnVsName

Name of the authentication vserver at which authentication should be done.
Maximum value: 128

AuthenticationHost

Hostname of the authentication vserver. Maximum value: 256

AuthenticationDomain

Domain for which TM cookie must to be set. If unspecified, cookie will be set for FQDN. Maximum value: 256

[Top](#)

unset authentication authnProfile

Synopsis

unset authentication authnProfile <name> [-AuthenticationDomain] [-AuthenticationLevel]

Description

Use this command to remove authentication authnProfile settings. Refer to the set authentication authnProfile command for meanings of the arguments.

[Top](#)

show authentication authnProfile

Synopsis

show authentication authnProfile [<name>]

Description

Displays the current configuration for the authentication profile specified

Parameters

name

Name of the authentication profile.

[Top](#)

Authorization Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [authorization policy](#)
- ♦ [authorization policylabel](#)
- ♦ [authorization action](#)

authorization policy

[[add](#) | [rm](#) | [set](#) | [rename](#) | [show](#)]

add authorization policy

Synopsis

add authorization policy <name> <rule> <action>

Description

Creates an authorization policy. Authorization policies allow AAA users and AAA groups to access resources through SSL VPN/AAA-TM enabled virtual servers.

Parameters

name

Name for the new authorization policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.), pound (#), space (), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the authorization policy is added. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authorization policy" or 'my authorization policy').

rule

Name of the NetScaler named rule, or a default syntax expression, that the policy uses to perform the authentication.

action

Action to perform if the policy matches: either allow or deny the request.

Example

Example: Consider the following authorization policy, "author-policy",

```
add authorization policy author-policy "URL
== /*.gif" DENY
bind aaa user foo -policy author-policy
```

If the user "foo" now logs in through the SSL VPN and makes any other request except "gif", the rule

```
will be evaluated to FALSE, and the negetion of
DENY, i.e. ALLOW, will be applied. So all those
resource will implicitly be allowed to access. If
"foo" tries to accesss "abc.gif" this access will
be denied.
```

[Top](#)

rm authorization policy

Synopsis

rm authorization policy <name>

Description

Removes an authorization policy.

Parameters

name

Name of the authorization policy to be removed.

[Top](#)

set authorization policy

Synopsis

set authorization policy <name> [-rule <expression>] [-action <string>]

Description

Configures the specified parameters of an authorization policy.

Parameters

name

Name of the authorization policy to modify.

rule

Name of the NetScaler named rule, or a default syntax expression, that the policy uses to perform the authentication.

action

Action to perform if the policy matches: either allow or deny the request.

[Top](#)

rename authorization policy

Synopsis

rename authorization policy <name>@ <newName>@

Description

Rename a author policy.

Parameters

name

The name of the author policy.

newName

The new name of the author policy.

Example

```
rename auth policy oldname newname
```

[Top](#)

show authorization policy

Synopsis

show authorization policy [<name>]

Description

Displays the current settings for the specified authorization policy. If no policy name is provided, displays a list of all authorization policies currently configured on the NetScaler appliance.

Parameters

name

Name of the authorization policy.

[Top](#)

authorization policylabel

[[add](#) | [rm](#) | [bind](#) | [unbind](#) | [rename](#) | [show](#) | [stat](#)]

add authorization policylabel

Synopsis

add authorization policylabel <labelName>

Description

Creates a user-defined authorization policy label.

Parameters

labelName

Name for the new authorization policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space (), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the authorization policy is created. The following requirement applies only to the NetScaler CLI: If the name includes one or

more spaces, enclose the name in double or single quotation marks (for example, "my authorization policy label" or 'authorization policy label').

Example

```
add authorization policylabel trans_http_url
```

[Top](#)

rm authorization policylabel

Synopsis

```
rm authorization policylabel <labelName>
```

Description

Removes an authorization policy label.

Parameters

labelName

Name of the authorization policy label to remove.

Example

```
rm authorization policylabel trans_http_url
```

[Top](#)

bind authorization policylabel

Synopsis

```
bind authorization policylabel <labelName> <policyName> <priority>  
[<gotoPriorityExpression>] [-invoke (<labelType> <labelName>)]
```

Description

Binds an authorization policy to a label.

Parameters

labelName

Name of the authorization policy label to which to bind the policy.

policyName

Name of the authorization policy to bind to the policy label.

Example

```
i)    bind authorization policylabel  
trans_http_url pol_1 1 2 -invoke reqvserver CURRENT
```

```
ii)      bind authorization policylabel
trans_http_url pol_2 2
```

[Top](#)

unbind authorization policylabel

Synopsis

```
unbind authorization policylabel <labelName> <policyName> [-priority
<positive_integer>]
```

Description

Unbinds the specified policy from the specified authorization policy label.

Parameters

labelName

Name for the new authorization policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space (), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the authorization policy is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authorization policy label" or 'authorization policy label').

policyName

Name of the authorization policy to bind to the policy label.

priority

Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

```
unbind authorization policylabel trans_http_url
pol_1
```

[Top](#)

rename authorization policylabel

Synopsis

```
rename authorization policylabel <labelName>@ <newName>@
```

Description

Rename a auth policy label.

Parameters

labelName

The name of the auth policy label

newName

The new name of the auth policy label

Example

```
rename auth policy label oldname newname
```

[Top](#)

show authorization policylabel

Synopsis

show authorization policylabel [<labelName>]

Description

Displays the current settings for the specified authorization policy label. If no policy name is provided, displays a list of all authorization policy labels currently configured on the NetScaler appliance.

Parameters**labelName**

Name of the authorization policy label.

Example

```
i)    show authorization policylabel trans_http_url
ii)   show authorization policylabel
```

[Top](#)

stat authorization policylabel

Synopsis

stat authorization policylabel [<labelName>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-clearstats (basic | full)]

Description

Displays statistics for the specified authorization policy label. If no authorization policy label is specified, displays a list of all authorization policy labels.

Parameters**labelName**

Name of the authorization policy label.

clearstats

Clear the statistics / counters Possible values: basic, full

[Top](#)

authorization action

show authorization action

Synopsis

show authorization action [<name>]

Description

Show details of authorization actions.

Parameters

name
Name of authorization action

AUTOSCALE Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [autoscale profile](#)
- ♦ [autoscale action](#)
- ♦ [autoscale policy](#)

autoscale profile

[[add](#) | [rm](#) | [set](#) | [show](#)]

add autoscale profile

Synopsis

add autoscale profile <name> -type CLOUDSTACK -url <URL> -apiKey -sharedSecret

Description

Create a AutoScale policy.

Parameters

name
AutoScale profile name.

type
The type of profile. Possible values: CLOUDSTACK

url
URL providing the service

apiKey
api key for authentication with service

sharedSecret

shared secret for authentication with service

[Top](#)

rm autoscale profile

Synopsis

rm autoscale profile <name>

Description

Remove a AutoScale policy.

Parameters

name

AutoScale profile name.

[Top](#)

set autoscale profile

Synopsis

set autoscale profile <name> [-url <URL>] [-apiKey] [-sharedSecret]

Description

Set a AutoScale policy.

Parameters

name

AutoScale profile name.

url

URL providing the service

apiKey

api key for authentication with service

sharedSecret

shared secret for authentication with service

[Top](#)

show autoscale profile

Synopsis

show autoscale profile [<name>]

Description

Display the autoscale profile.

Parameters**name**

AutoScale profile name.

[Top](#)

autoscale action

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add autoscale action

Synopsis

```
add autoscale action <name> -type ( SCALE_UP | SCALE_DOWN ) -profileName <string>
-parameters <string> [-vmDestroyGracePeriod <positive_integer>] [-quietTime
<positive_integer>] -vServer <string>
```

Description

Create a AutoScale action.

Parameters**name**

ActionScale action name.

type

The type of action. Possible values: SCALE_UP, SCALE_DOWN

profileName

AutoScale profile name.

parameters

Parameters to use in the action

vmDestroyGracePeriod

Time in minutes a VM is kept in inactive state before destroying Default value: 10

quietTime

Time in seconds no other policy is evaluated or action is taken Default value: 300

vServer

Name of the vserver on which autoscale action has to be taken.

[Top](#)

rm autoscale action

Synopsis

```
rm autoscale action <name>
```

Description

Remove a AutoScale action.

Parameters

name
ActionScale action name.

[Top](#)

set autoscale action

Synopsis

```
set autoscale action <name> [-profileName <string>] [-parameters <string>] [-vmDestroyGracePeriod <positive_integer>] [-quietTime <positive_integer>] [-vServer <string>]
```

Description

Set a AutoScale action.

Parameters

name
ActionScale action name.

profileName
AutoScale profile name.

parameters
Parameters to use in the action

vmDestroyGracePeriod
Time in minutes a VM is kept in inactive state before destroying Default value: 10

quietTime
Time in seconds no other policy is evaluated or action is taken Default value: 300

vServer
Name of the vserver on which autoscale action has to be taken.

[Top](#)

unset autoscale action

Synopsis

```
unset autoscale action <name> [-vmDestroyGracePeriod] [-quietTime]
```

Description

Use this command to remove autoscale action settings.Refer to the set autoscale action command for meanings of the arguments.

[Top](#)

show autoscale action

Synopsis

```
show autoscale action [<name>]
```

Description

Display the autoscale actions.

Parameters**name**

ActionScale action name.

[Top](#)

autoscale policy

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#) | [stat](#) | [rename](#)]

add autoscale policy

Synopsis

add autoscale policy <name> -rule <expression> -action <string> [-comment <string>] [-logAction <string>]

Description

Create a autoscale policy.

Parameters**name**

The name of the autoscale policy.

rule

The rule associated with the policy.

action

The autoscale profile associated with the policy.

comment

Comments associated with this autoscale policy.

logAction

The log action associated with the autoscale policy

[Top](#)

rm autoscale policy

Synopsis

rm autoscale policy <name>

Description

Remove a autoscale policy.

Parameters**name**

The name of the autoscale policy.

Example

```
rm autoscale policy pol
```

[Top](#)

set autoscale policy

Synopsis

```
set autoscale policy <name> [-rule <expression>] [-action <string>] [-comment <string>]
[-logAction <string>]
```

Description

Set a new rule/action/comment for an existing autoscale policy.

Parameters

name

The name of the autoscale policy.

rule

The rule associated with the policy.

action

The autoscale profile associated with the policy.

comment

Comments associated with this autoscale policy.

logAction

The log action associated with the autoscale policy

Example

```
set autoscaler policy pol -rule true
```

[Top](#)

unset autoscale policy

Synopsis

```
unset autoscale policy <name> [-rule <expression>] [-action <string>] [-comment
<string>] [-logAction <string>]
```

Description

Unset comment/logaction for existing autoscale policy..Refer to the set autoscale policy command for meanings of the arguments.

Example

```
unset autoscale policy pol9 -undefAction
```

[Top](#)**show autoscale policy****Synopsis**

```
show autoscale policy [<name>]
```

Description

Display the autoscale policies.

Parameters**name**

The name of the autoscale policy.

[Top](#)**stat autoscale policy****Synopsis**

```
stat autoscale policy [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-clearstats ( basic | full )]
```

Description

Display autoscale policy statistics.

Parameters**name**

The name of the autoscale policy for which statistics will be displayed. If not given statistics are shown for all autoscale policies.

clearstats

Clear the statistics / counters Possible values: basic, full

Example

```
stat autoscale policy
```

[Top](#)**rename autoscale policy****Synopsis**

```
rename autoscale policy <name>@ <newName>@
```

Description

Rename a autoscale policy.

Parameters

name

The name of the autoscale policy.

newName

The new name of the autoscale policy.

Example

```
rename autoscale policy oldname newname
```

[Top](#)

Basic Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [location](#)
- ♦ [locationFile](#)
- ♦ [server](#)
- ♦ [service](#)
- ♦ [serviceGroup](#)
- ♦ [dbsMonitors](#)
- ♦ [locationData](#)
- ♦ [svcbindings](#)
- ♦ [servicegroupbindings](#)
- ♦ [serviceGroupMember](#)
- ♦ [configstatus](#)
- ♦ [locationParameter](#)
- ♦ [vserver](#)
- ♦ [uiinternal](#)
- ♦ [reporting](#)
- ♦ [nstrace](#)

location

[[add](#) | [rm](#) | [show](#)]

add location

Synopsis

```
add location <IPfrom> <IPto> <preferredLocation> [-longitude <integer>] [-latitude <integer>]]
```

Description

Creates a custom location entry on the NetScaler appliance. Custom locations can be used instead of a static location database if the number of locations you need does not exceed 500. Custom locations can also be used to override incorrect entries in the static database, because the appliance searches the static database before it searches the static location database.

Parameters

IPfrom

First IP address in the range, in dotted decimal notation.

IPto

Last IP address in the range, in dotted decimal notation.

preferredLocation

String of qualifiers, in dotted notation, describing the geographical location of the IP address range. Each qualifier is more specific than the one that precedes it, as in continent.country.region.city.isp.organization. For example, "NA.US.CA.San Jose.ATT.citrix". Note: A qualifier that includes a dot (.) or space () must be enclosed in double quotation marks.

longitude

Numerical value, in degrees, specifying the longitude of the geographical location of the IP address-range. Note: Longitude and latitude parameters are used for selecting a service with the static proximity GSLB method. If they are not specified, selection is based on the qualifiers specified for the location. Minimum value: -180 Maximum value: 180

latitude

Numerical value, in degrees, specifying the latitude of the geographical location of the IP address-range. Note: Longitude and latitude parameters are used for selecting a service with the static proximity GSLB method. If they are not specified, selection is based on the qualifiers specified for the location. Minimum value: -90 Maximum value: 90

Example

```
Add location 192.168.100.1 192.168.100.100  
*.us.ca.san jose
```

[Top](#)

rm location

Synopsis

rm location <IPfrom> <IPto>

Description

Removes a custom location entry from the NetScaler appliance.

Parameters

IPfrom

First IP address in the range, in dotted decimal notation.

IPto

Last IP address in the range, in dotted decimal notation.

Example

```
rm location 192.168.100.1 192.168.100.100
```

[Top](#)

show location

Synopsis

show location [<IPfrom>]

Description

Displays all the custom location entries configured on the NetScaler appliance, or just the entry for the specified IP address range.

Parameters

IPfrom

The qualifiers in dotted notation for the ipaddress. If this value is not specified, all custom entries are displayed.

Example

```
show location
```

[Top](#)

locationFile

[[add](#) | [rm](#) | [show](#)]

add locationFile

Synopsis

add locationFile <locationFile> [-format <format>]

Description

Loads the static location database from the specified file.

Parameters

locationFile

Name of the location file, with or without absolute path. If the path is not included, the default path (/var/netScaler/locdb) is assumed. In a high availability setup, the static database must be stored in the same location on both NetScaler appliances.

format

Format of the location file. Required for the NetScaler appliance to identify how to read the location file. Possible values: netscaler, ip-country, ip-country-isp, ip-country-region-city, ip-country-region-city-isp, geoip-country, geoip-region, geoip-city, geoip-country-org, geoip-country-isp, geoip-city-isp-org Default value: NSMAP_FORMAT_NETSCALER

Example

```
add locationfile /var/nsmap/locationdb -format
netscaler
```

[Top](#)

rm locationFile

Synopsis

rm locationFile

Description

Removes the currently loaded static location database from the NetScaler appliance.

Example

```
rm locationfile
```

[Top](#)

show locationFile

Synopsis

show locationFile

Description

Displays the name, including the absolute path, and format of the location file currently loaded on the NetScaler appliance.

Example

```
show locationfile
```

[Top](#)

server

[[add](#) | [rm](#) | [set](#) | [unset](#) | [enable](#) | [disable](#) | [show](#) | [rename](#)]

add server

Synopsis

```
add server <name>@ (<IPAddress>@ | (<domain>@ [-domainResolveRetry <integer>] [-IPv6Address ( YES | NO )]) | (-translationIp <ip_addr> -translationMask <netmask>)) [-state ( ENABLED | DISABLED )] [-comment <string>] [-td <positive_integer>]
```

Description

Creates a server entry on the NetScaler appliance. The NetScaler appliance supports two types of servers: IP address based servers and domain based servers.

Parameters

name

Name for the server. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the name is created.

IPAddress

IPv4 or IPv6 address of the server. If you create an IP address based server, you can specify the name of the server, instead of its IP address, when creating a service. Note: If you do not create a server entry, the server IP address that you enter when you create a service becomes the name of the server.

domain

Domain name of the server. For a domain based configuration, you must create the server first.

translationIp

IP address used to transform the server's DNS-resolved IP address.

domainResolveRetry

Time, in seconds, for which the NetScaler appliance must wait, after DNS resolution fails, before sending the next DNS query to resolve the domain name. Default value: 5 Minimum value: 5 Maximum value: 20939

state

Initial state of the server. Possible values: ENABLED, DISABLED Default value: ENABLED

IPv6Address

Support IPv6 addressing mode. If you configure a server with the IPv6 addressing mode, you cannot use the server in the IPv4 addressing mode. Possible values: YES, NO Default value: NO

comment

Any information about the server.

td

Traffic Domain Id. Maximum value: 4094

Example

```
add server web_serv 10.102.27.150
    To add multiple servers you can use the
    following command:
    add server serv[1-3] 10.102.27.[151-153]
    The above command adds three servers: serv1
    with IP 10.102.27.151, serv2 with IP 10.102.27.152
    and serv3 with IP 10.102.27.153.
```

[Top](#)

rm server**Synopsis**

```
rm server <name>@ ...
```

Description

Removes a server entry from the NetScaler appliance.

Parameters**name**

Name of the server entry to remove.

Example

```
rm server web_svr
    To remove the servers named serv1, serv2 and
    serv3 at once you can use the following command:
    rm server serv[1-3]
```

[Top](#)

set server

Synopsis

```
set server <name>@ [-IPAddress <ip_addr|ipv6_addr|*>@ | -domainResolveRetry
<integer> | -translationIp <ip_addr> | -translationMask <netmask> | -
domainResolveNow] [-comment <string>]
```

Description

Modifies the specified parameters of a server entry.

Parameters

name

Name of the server whose parameters you are configuring.

IPAddress

Name of the server whose parameters you are configuring.

domainResolveRetry

Time, in seconds, for which the NetScaler appliance must wait, after DNS resolution fails, before sending the next DNS query to resolve the domain name. Default value: 5 Minimum value: 5 Maximum value: 20939

translationIp

IP address used to transform the server's DNS-resolved IP address.

translationMask

The netmask of the translation ip

domainResolveNow

Immediately send a DNS query to resolve the server's domain name.

comment

Any information about the server.

Example

```
set server http_svr -IPAddress 10.102.1.112
To set multiple servers IP addresses at once
you can use the following command:
setserver serv[1-3] -IPAddress 10.102.27.[1-3]
The above command sets the IP address of serv1
to 10.102.27.1, serv2 to 10.102.27.2 and serv3 to
10.102.27.3.
```

[Top](#)

unset server

Synopsis

```
unset server <name>@ -comment
```

Description

Use this command to remove server settings. Refer to the set server command for meanings of the arguments.

[Top](#)

enable server

Synopsis

```
enable server <name>@
```

Description

Enables all services on the specified server.

Parameters

name

Name of the server to enable.

Example

```
enable server web_serv
    To enable all the services configured on
    servers named serv1, serv2 and serv3 at once, use
    the following command:
    enable server serv[1-3]
```

[Top](#)

disable server

Synopsis

```
disable server <name>@ [<delay>] [-graceFul ( YES | NO )]
```

Description

Disables all services on the server. When a server is disabled, all services on the server are disabled.

Parameters

name

Name of the server to disable.

delay

Time, in seconds, after which all the services configured on the server are disabled.

graceFul

Shut down gracefully, without accepting any new connections, and disabling each service when all of its connections are closed. Possible values: YES, NO Default value: NO

Example

```
disable server web_svr 30
    To disable all the services configured on
    servers named serv1, serv2 and serv3 at once, use
    the following command:
    disable server serv[1-3]
```

[Top](#)

show server

Synopsis

show server [<name> | -internal]

Description

Displays the parameters of all the server entries on the appliance, or the parameters of the specified server entry.

Parameters

name

Name of the server for which to display parameters.

internal

Display names of the servers that have been created for internal use.

Example

```
> show server web_svr1
    Name:          web_svr1          State:ENABLED
    IPAddress:     10.102.27.154

> show server web_svr1
    Name:          web_svr2          State:ENABLED
    Domain: www.abc.com      Resolve Retry: 30 Secs
    Translation IP: 10.102.27.153 Translation
    Mask:         255.255.255.0
```

[Top](#)

rename server

Synopsis

rename server <name>@ <newName>@

Description

Renames a server.

Parameters

name

Existing name of the server.

newName

New name for the server. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

Example

```
rename server s1 s1-new
```

[Top](#)

service

[[add](#) | [rm](#) | [set](#) | [unset](#) | [bind](#) | [unbind](#) | [enable](#) | [disable](#) | [show](#) | [rename](#) | [stat](#)]

add service

Synopsis

add service <name>@ (<IP>@ | <serverName>@) <serviceType> <port> [-clearTextPort <port>] [-cacheType <cacheType>] [-maxClient <positive_integer>] [-healthMonitor (YES | NO)] [-maxReq <positive_integer>] [-cacheable (YES | NO)] [-cip (ENABLED | DISABLED)] [<cipHeader>] [-usip (YES | NO)] [-pathMonitor (YES | NO)] [-pathMonitorIndv (YES | NO)] [-useproxyport (YES | NO)] [-sc (ON | OFF)] [-sp (ON | OFF)] [-rtspSessionidRemap (ON | OFF)] [-cltTimeout <secs>] [-svrTimeout <secs>] [-CustomServerID <string>] [-CKA (YES | NO)] [-TCPB (YES | NO)] [-CMP (YES | NO)] [-maxBandwidth <positive_integer>] [-accessDown (YES | NO)] [-monThreshold <positive_integer>] [-state (ENABLED | DISABLED)] [-downStateFlush (ENABLED | DISABLED)] [-tcpProfileName <string>] [-httpProfileName <string>] [-hashId <positive_integer>] [-comment <string>] [-appflowLog (ENABLED | DISABLED)] [-netProfile <string>] [-td <positive_integer>]

Description

Creates a service on the NetScaler appliance. If the service is domain based, before you create the service, create the server entry by using the add server command. Then, in this command, specify the Server parameter.

Parameters

name

Name for the service. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the service has been created.

IP

IP to assign to the service.

serverName

Name of the server that hosts the service.

serviceType

Protocol in which data is exchanged with the service. Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, DTLS, NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, DNS_TCP, ADNS_TCP, MYSQL, MSSQL, RADIUS, RDP, DIAMETER, SSL_DIAMETER, TFTP

port

Port number of the service.

clearTextPort

Port to which clear text data must be sent after the appliance decrypts incoming SSL traffic. Applicable to transparent SSL services. Minimum value: 1

cacheType

Cache type supported by the cache server. Possible values: TRANSPARENT, REVERSE, FORWARD

maxClient

Maximum number of simultaneous open connections to the service. Maximum value: 4294967294

healthMonitor

Monitor the health of this service. Available settings function as follows: YES - Send probes to check the health of the service. NO - Do not send probes to check the health of the service. With the NO option, the appliance shows the service as UP at all times. Possible values: YES, NO Default value: YES

maxReq

Maximum number of requests that can be sent on a persistent connection to the service. Note: Connection requests beyond this value are rejected. Maximum value: 65535

cacheable

Use the transparent cache redirection virtual server to forward requests to the cache server. Note: Do not specify this parameter if you set the Cache Type parameter. Possible values: YES, NO Default value: NO

cip

Before forwarding a request to the service, insert an HTTP header with the client's IPv4 or IPv6 address as its value. Used if the server needs the client's IP address for security, accounting, or other purposes, and setting the Use Source IP parameter is not a viable option. Possible values: ENABLED, DISABLED

cipHeader

Name for the HTTP header whose value must be set to the IP address of the client. Used with the Client IP parameter. If you set the Client IP parameter, and you do not specify a name for the header, the appliance uses the header name specified for the global Client IP Header parameter (the cipHeader parameter in the set ns param CLI command or the Client IP Header parameter in the Configure HTTP Parameters dialog

box at System > Settings > Change HTTP parameters). If the global Client IP Header parameter is not specified, the appliance inserts a header with the name "client-ip."

usip

Use the client's IP address as the source IP address when initiating a connection to the server. When creating a service, if you do not set this parameter, the service inherits the global Use Source IP setting (available in the enable ns mode and disable ns mode CLI commands, or in the System > Settings > Configure modes > Configure Modes dialog box). However, you can override this setting after you create the service. Possible values: YES, NO

pathMonitor

Path monitoring for clustering Possible values: YES, NO

pathMonitorIndv

Individual Path monitoring decisions Possible values: YES, NO

useproxyport

Use the proxy port as the source port when initiating connections with the server. With the NO setting, the client-side connection port is used as the source port for the server-side connection. Note: This parameter is available only when the Use Source IP (USIP) parameter is set to YES. Possible values: YES, NO

sc

State of SureConnect for the service. Possible values: ON, OFF Default value: OFF

sp

Enable surge protection for the service. Possible values: ON, OFF

rtspSessionidRemap

Enable RTSP session ID mapping for the service. Possible values: ON, OFF Default value: OFF

cltTimeout

Time, in seconds, after which to terminate an idle client connection. Maximum value: 31536000

svrTimeout

Time, in seconds, after which to terminate an idle server connection. Maximum value: 31536000

CustomServerID

Unique identifier for the service. Used when the persistency type for the virtual server is set to Custom Server ID. Default value: "None"

serverID

The identifier for the service. This is used when the persistency type is set to Custom Server ID.

CKA

Enable client keep-alive for the service. Possible values: YES, NO

TCPB

Enable TCP buffering for the service. Possible values: YES, NO

CMP

Enable compression for the service. Possible values: YES, NO

maxBandwidth

Maximum bandwidth, in Kbps, allocated to the service. Maximum value: 4294967287

accessDown

Use Layer 2 mode to bridge the packets sent to this service if it is marked as DOWN. If the service is DOWN, and this parameter is disabled, the packets are dropped. Possible values: YES, NO Default value: NO

monThreshold

Minimum sum of weights of the monitors that are bound to this service. Used to determine whether to mark a service as UP or DOWN. Maximum value: 65535

state

Initial state of the service. Possible values: ENABLED, DISABLED Default value: ENABLED

downStateFlush

Perform delayed clean-up of connections to the service. Possible values: ENABLED, DISABLED Default value: ENABLED

tcpProfileName

Name of the TCP profile that contains TCP configuration settings for the service.

httpProfileName

Name of the HTTP profile that contains HTTP configuration settings for the service.

hashId

A numerical identifier that can be used by hash based load balancing methods. Must be unique for each service. Minimum value: 1

comment

Any information about the service.

appflowLog

Enable logging of AppFlow information. Possible values: ENABLED, DISABLED Default value: ENABLED

netProfile

Network profile to use for the service.

td

Traffic Domain Id. Maximum value: 4094

Example

```
add service http_svc 10.102.1.112 http 80
    The below command adds the service web_svc1
    for the server web_serv1, web_svc2 for web_serv2
    and web_svc3 for web_serv3.
    add service web_svc[1-3] web_serv[1-3] http 80
```

[Top](#)

rm service

Synopsis

rm service <name>@

Description

Removes a service.

Parameters

name

Name of the service.

Example

```
rm service http_svc
    To remove services svc1, svc2 and svc3 in one
    go use the following command:
    rm service svc[1-3]
```

[Top](#)

set service

Synopsis

```
set service <name>@ [-IPAddress <ip_addr|ipv6_addr|*>@] [-maxClient
<positive_integer>] [-maxReq <positive_integer>] [-cacheable ( YES | NO )] [-cip
( ENABLED | DISABLED ) [<cipHeader>]] [-usip ( YES | NO )] [-pathMonitor ( YES | NO )]
[-pathMonitorIndv ( YES | NO )] [-useproxyport ( YES | NO )] [-sc ( ON | OFF )] [-sp ( ON
| OFF )] [-rtspSessionidRemap ( ON | OFF )] [-healthMonitor ( YES | NO )] [-cltTimeout
<secs>] [-svrTimeout <secs>] [-CustomServerID <string>] [-CKA ( YES | NO )] [-TCPB
( YES | NO )] [-CMP ( YES | NO )] [-maxBandwidth <positive_integer>] [-accessDown
( YES | NO )] [-monThreshold <positive_integer>] [-weight <positive_integer>
<monitorName>] [-downStateFlush ( ENABLED | DISABLED )] [-tcpProfileName <string>]
[-httpProfileName <string>] [-hashId <positive_integer>] [-comment <string>] [-
appflowLog ( ENABLED | DISABLED )] [-netProfile <string>]
```

Description

Modifies the parameters of an existing service.

Parameters

name

Name of the service for which to modify parameters.

IPAddress

The new IP address of the service.

maxClient

Maximum number of simultaneous open connections to the service. Maximum value: 4294967294

maxReq

Maximum number of requests that can be sent on a persistent connection to the service. Note: Connection requests beyond this value are rejected. Maximum value: 65535

cacheable

Use the transparent cache redirection virtual server to forward requests to the cache server. Note: Do not specify this parameter if you set the Cache Type parameter. Possible values: YES, NO Default value: NO

cip

Before forwarding a request to the service, insert an HTTP header with the client's IPv4 or IPv6 address as its value. Used if the server needs the client's IP address for security, accounting, or other purposes, and setting the Use Source IP parameter is not a viable option. Possible values: ENABLED, DISABLED

usip

Use the client's IP address as the source IP address when initiating a connection to the server. When creating a service, if you do not set this parameter, the service inherits the global Use Source IP setting (available in the enable ns mode and disable ns mode CLI commands, or in the System > Settings > Configure modes > Configure Modes dialog box). However, you can override this setting after you create the service. Possible values: YES, NO

pathMonitor

Path monitoring for clustering Possible values: YES, NO

pathMonitorIndv

Individual Path monitoring decisions Possible values: YES, NO

useproxyport

Use the proxy port as the source port when initiating connections with the server. With the NO setting, the client-side connection port is used as the source port for the server-side connection. Note: This parameter is available only when the Use Source IP (USIP) parameter is set to YES. Possible values: YES, NO

sc

State of SureConnect for the service. Possible values: ON, OFF Default value: OFF

sp

Enable surge protection for the service. Possible values: ON, OFF

rtspSessionidRemap

Enable RTSP session ID mapping for the service. Possible values: ON, OFF Default value: OFF

healthMonitor

Monitor the health of this service. Available settings function as follows: YES - Send probes to check the health of the service. NO - Do not send probes to check the health of the service. With the NO option, the appliance shows the service as UP at all times. Possible values: YES, NO Default value: YES

cltTimeout

Time, in seconds, after which to terminate an idle client connection. Maximum value: 31536000

svrTimeout

Time, in seconds, after which to terminate an idle server connection. Maximum value: 31536000

CustomServerID

Unique identifier for the service. Used when the persistency type for the virtual server is set to Custom Server ID. Default value: "None"

serverID

The identifier for the service. This is used when the persistency type is set to Custom Server ID.

CKA

Enable client keep-alive for the service. Possible values: YES, NO

TCPB

Enable TCP buffering for the service. Possible values: YES, NO

CMP

Enable compression for the service. Possible values: YES, NO

maxBandwidth

Maximum bandwidth, in Kbps, allocated to the service. Maximum value: 4294967287

accessDown

Use Layer 2 mode to bridge the packets sent to this service if it is marked as DOWN. If the service is DOWN, and this parameter is disabled, the packets are dropped. Possible values: YES, NO Default value: NO

monThreshold

Minimum sum of weights of the monitors that are bound to this service. Used to determine whether to mark a service as UP or DOWN. Maximum value: 65535

weight

Weight to assign to the monitor-service binding. When a monitor is UP, the weight assigned to its binding with the service determines how much the monitor contributes toward keeping the health of the service above the value configured for the Monitor Threshold parameter. Minimum value: 1 Maximum value: 100

downStateFlush

Perform delayed clean-up of connections to the service. Possible values: ENABLED, DISABLED Default value: ENABLED

tcpProfileName

Name of the TCP profile that contains TCP configuration settings for the service.

httpProfileName

Name of the HTTP profile that contains HTTP configuration settings for the service.

hashId

A numerical identifier that can be used by hash based load balancing methods. Must be unique for each service. Minimum value: 1

comment

Any information about the service.

appflowLog

Enable logging of AppFlow information. Possible values: ENABLED, DISABLED Default value: ENABLED

netProfile

Network profile to use for the service.

Example

```
set service http_svc -maxClient 100
    The following command sets IP address
    10.102.27.53 for service svc1, 10.102.27.54 for
    svc2 and 10.102.27.55 for svc3.
    set service svc[1-3] -IPAddress 10.102.27.
    [53-55]
```

[Top](#)

unset service

Synopsis

```
unset service <name>@ [-maxClient] [-maxReq] [-cacheable] [-cip] [-usip] [-
pathMonitor] [-pathMonitorIndv] [-useproxyport] [-sc] [-sp] [-rtspSessionidRemap] [-
CustomServerID] [-CKA] [-TCPB] [-CMP] [-maxBandwidth] [-accessDown] [-
monThreshold] [-cltTimeout] [-svrTimeout] [-tcpProfileName] [-httpProfileName] [-
hashId] [-appflowLog] [-netProfile] [-cipHeader] [-healthMonitor] [-monitorName] [-
downStateFlush] [-comment]
```

Description

Removes the parameter settings of the specified service. Attributes for which a default value is available revert to their default values..Refer to the set service command for meanings of the arguments.

Example

```
unset service http_svc -maxClient
    To unset maxclients for services svc1, svc2
    and svc3, the following command can be used:
    unset service svc[1-3] -maxClient
```

[Top](#)

bind service

Synopsis

```
bind service <name>@ (-policyName <string> | (-monitorName <string>@ [-monState  
( ENABLED | DISABLED )] [-weight <positive_integer>] [-passive]]))
```

Description

Binds a policy or a monitor to a service.

Parameters

name

Name of the service to which to bind a policy or monitor.

policyName

Name of the policy to bind to the service.

monitorName

Name of the monitor to bind to the service.

Example

```
bind service svc1 -policyName poll1
    To bind svc1, svc2 and svc3 to the policy poll1
    you can use the following command:
    bind service svc[1-3] -policyName poll1
```

[Top](#)

unbind service

Synopsis

```
unbind service <name>@ (-policyName <string> | -monitorName <string>@)
```

Description

Unbinds a policy or monitor from the specified service.

Parameters

name

Name of the service from which to unbind a policy or monitor.

policyName

Name of the policy to unbind.

monitorName

Name of the monitor assigned to the service.

Example

```
unbind service http_svc -policyName poll
    To unbind a policy called poll on services
    svc1, svc2 and svc3, use the following command:
    unbind service svc[1-3] -policyName poll
```

[Top](#)

enable service

Synopsis

enable service <name>@

Description

Enables a service.

Parameters

name

Name of the service.

Example

```
enable service http_svc
    To enable svc1, svc2 and svc3 in one go use
    the following command:
    enable service svc[1-3]
```

[Top](#)

disable service

Synopsis

disable service <name>@ [<delay>] [-graceFul (YES | NO)]

Description

Disables a service.

Parameters

name

Name of the service.

delay

Time, in seconds, allocated to the NetScaler appliance for a graceful shutdown of the service. During this period, new requests are sent to the service only for clients who already have persistent sessions on the appliance. Requests from new clients are load balanced among other available services. After the delay time expires, no requests are sent to the service, and the service is marked as unavailable (OUT OF SERVICE).

graceful

Shut down gracefully, not accepting any new connections, and disabling the service when all of its connections are closed. Possible values: YES, NO Default value: NO

Example

```
disable service http_svc 10
  To disable svc1, svc2 and svc3 in one go use
  the following command:
  disable service svc[1-3] 10
```

[Top](#)

show service**Synopsis**

show service [<name> | -all | -internal] show service bindings - alias for 'show svcbindings'

Description

Displays a list of all services configured on the NetScaler appliance, or the configuration details of the specified service.

Parameters**name**

Name of the service for which to display configuration details.

all

Display both user-configured and dynamically learned services.

internal

Display only dynamically learned services.

Example

```
The following is sample output of the show service
-all command:
4 configured services:
1)      svc1 (10.124.99.12:80) - HTTP
State: UP
      Max Conn: 0      Max Req: 0      Use Source
IP: NO
      Client Keepalive(CKA): NO
      TCP Buffering(TCPB): NO
      HTTP Compression(CMP): NO
      Idle timeout: Client: 180 sec      Server: 360 sec
      Client IP: DISABLED
2)      svc_3 (10.100.100.3:53) - DNS      State: UP
      Max Conn: 0      Max Req: 0      Use Source IP:
NO
      Client Keepalive(CKA): NO
```

```

TCP Buffering(TCPB): NO
HTTP Compression(CMP): NO
Idle timeout: Client: 180 sec    Server: 360 sec
Client IP: DISABLED
3) tsvcl (77.45.32.45:80) - HTTP    State: UP
   Max Conn: 0          Max Req: 0    Use Source IP:
NO
   Client Keepalive(CKA): NO
   TCP Buffering(TCPB): NO
   HTTP Compression(CMP): NO
   Idle timeout: Client: 180 sec    Server: 360 sec
   Client IP: DISABLED
4) foosvc (10.124.99.13:7979) - HTTP    State: UP
   Max Conn: 0          Max Req: 0    Use Source IP:
NO
   Client Keepalive(CKA): NO
   TCP Buffering(TCPB): NO
   HTTP Compression(CMP): NO
   Idle timeout: Client: 180 sec    Server: 360 sec
   Client IP: DISABLED

```

[Top](#)

rename service

Synopsis

```
rename service <name>@ <newName>@
```

Description

Renames a service.

Parameters

name

Existing name of the service to be renamed.

newName

New name for the service. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

Example

```
rename service svcl svcnew
```

[Top](#)

stat service

Synopsis

```
stat service [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile
<input_filename>] [-clearstats ( basic | full )]
```

Description

Displays statistics that have been collected for the specified service.

Parameters

name

Name of the service.

clearstats

Clear the statistics / counters Possible values: basic, full

[Top](#)

serviceGroup

[[add](#) | [rm](#) | [set](#) | [unset](#) | [bind](#) | [unbind](#) | [enable](#) | [disable](#) | [show](#) | [stat](#) | [rename](#)]

add serviceGroup

Synopsis

```
add serviceGroup <serviceName>@ <serviceType> [-cacheType <cacheType>] [-td
<positive_integer>] [-maxClient <positive_integer>] [-maxReq <positive_integer>] [-
cacheable ( YES | NO )] [-cip ( ENABLED | DISABLED ) [<cipHeader>]] [-usip ( YES |
NO )] [-pathMonitor ( YES | NO )] [-pathMonitorIndv ( YES | NO )] [-useproxyport ( YES |
NO )] [-healthMonitor ( YES | NO )] [-sc ( ON | OFF )] [-sp ( ON | OFF )] [-
rtspSessionidRemap ( ON | OFF )] [-cltTimeout <secs>] [-svrTimeout <secs>] [-CKA ( YES
| NO )] [-TCPB ( YES | NO )] [-CMP ( YES | NO )] [-maxBandwidth <positive_integer>] [-
monThreshold <positive_integer>] [-state ( ENABLED | DISABLED )] [-downStateFlush
( ENABLED | DISABLED )] [-tcpProfileName <string>] [-httpProfileName <string>] [-
comment <string>] [-appflowLog ( ENABLED | DISABLED )] [-netProfile <string>] [-
autoScale <autoScale> -memberPort <port>]
```

Description

Creates a service group. You can group similar services into a service group and use them as a single entity.

Parameters

serviceName

Name of the service group. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the name is created.

serviceType

Protocol used to exchange data with the service. Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, DTLS, NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, DNS_TCP, ADNS_TCP, MYSQL, MSSQL, RADIUS, RDP, DIAMETER, SSL_DIAMETER, TFTP

cacheType

Cache type supported by the cache server. Possible values: TRANSPARENT, REVERSE, FORWARD

td

Traffic Domain Id. Maximum value: 4094

maxClient

Maximum number of simultaneous open connections for the service group. Maximum value: 4294967294

maxReq

Maximum number of requests that can be sent on a persistent connection to the service group. Note: Connection requests beyond this value are rejected. Maximum value: 65535

cacheable

Use the transparent cache redirection virtual server to forward the request to the cache server. Note: Do not set this parameter if you set the Cache Type. Possible values: YES, NO Default value: NO

cip

Insert the Client IP header in requests forwarded to the service. Possible values: ENABLED, DISABLED

cipHeader

Name of the HTTP header whose value must be set to the IP address of the client. Used with the Client IP parameter. If client IP insertion is enabled, and the client IP header is not specified, the value of Client IP Header parameter or the value set by the set ns config command is used as client's IP header name.

usip

Use client's IP address as the source IP address when initiating connection to the server. With the NO setting, which is the default, a mapped IP (MIP) address or subnet IP (SNIP) address is used as the source IP address to initiate server side connections. Possible values: YES, NO

pathMonitor

Path monitoring for clustering Possible values: YES, NO

pathMonitorIndv

Individual Path monitoring decisions. Possible values: YES, NO

useproxypport

Use the proxy port as the source port when initiating connections with the server. With the NO setting, the client-side connection port is used as the source port for the server-side connection. Note: This parameter is available only when the Use Source IP (USIP) parameter is set to YES. Possible values: YES, NO

healthMonitor

Monitor the health of this service. Available settings function as follows: YES - Send probes to check the health of the service. NO - Do not send probes to check the health of the service. With the NO option, the appliance shows the service as UP at all times. Possible values: YES, NO Default value: YES

sc

State of the SureConnect feature for the service group. Possible values: ON, OFF
Default value: OFF

sp

Enable surge protection for the service group. Possible values: ON, OFF
Default value: OFF

rtspSessionidRemap

Enable RTSP session ID mapping for the service group. Possible values: ON, OFF
Default value: OFF

cltTimeout

Time, in seconds, after which to terminate an idle client connection. Maximum value: 31536000

svrTimeout

Time, in seconds, after which to terminate an idle server connection. Maximum value: 31536000

CKA

Enable client keep-alive for the service group. Possible values: YES, NO

TCPB

Enable TCP buffering for the service group. Possible values: YES, NO

CMP

Enable compression for the specified service. Possible values: YES, NO

maxBandwidth

Maximum bandwidth, in Kbps, allocated for all the services in the service group.
Maximum value: 4294967287

monThreshold

Minimum sum of weights of the monitors that are bound to this service. Used to determine whether to mark a service as UP or DOWN. Maximum value: 65535

state

Initial state of the service group. Possible values: ENABLED, DISABLED
Default value: ENABLED

downStateFlush

Perform delayed clean-up of connections to all services in the service group. Possible values: ENABLED, DISABLED
Default value: ENABLED

tcpProfileName

Name of the TCP profile that contains TCP configuration settings for the service group.

httpProfileName

Name of the HTTP profile that contains HTTP configuration settings for the service group.

comment

Any information about the service group.

appflowLog

Enable logging of AppFlow information for the specified service group. Possible values: ENABLED, DISABLED Default value: ENABLED

netProfile

Network profile for the service group.

autoScale

Auto scale option for a servicegroup Possible values: DISABLED, DNS, POLICY Default value: NSA_AS_DISABLED

Example

```
add servicegroup http_svc_group http
    To add service groups sgrp1, sgrp2 and sgrp3
    at one go use the following command:
    add servicegroup sgrp[1-3] http
```

[Top](#)

rm serviceGroup

Synopsis

rm serviceGroup <serviceGroupName>@

Description

Removes a service group.

Parameters

serviceGroupName

Name of the service group.

Example

```
rm servicegroup http_svc_group
    To remove multiple servicegroups at once, the
    following command can be used:
    rm servicegroup http_svc_group[1-3]
```

[Top](#)

set serviceGroup

Synopsis

set serviceGroup <serviceGroupName>@ [(<serverName>@ <port> [-weight <positive_integer>] [-CustomServerID <string>] [-hashId <positive_integer>]) | -maxClient <positive_integer> | -maxReq <positive_integer> | -cacheable (YES | NO) | -cip (ENABLED | DISABLED) | <cipHeader> | -usip (YES | NO) | -useproxyport (YES | NO) | -sc (ON | OFF) | -sp (ON | OFF) | -rtspSessionidRemap (ON | OFF) | -


```
cltTimeout <secs> | -svrTimeout <secs> | -CKA ( YES | NO ) | -TCPB ( YES | NO ) | -CMP
( YES | NO ) | -maxBandwidth <positive_integer> | -monThreshold <positive_integer> |
-downStateFlush ( ENABLED | DISABLED )] [-monitorName <string> -weight
<positive_integer>] [-healthMonitor ( YES | NO )] [-pathMonitor ( YES | NO )] [-
pathMonitorIndv ( YES | NO )] [-tcpProfileName <string>] [-httpProfileName <string>] [-
comment <string>] [-appflowLog ( ENABLED | DISABLED )] [-netProfile <string>]
```

Description

Modifies the specified parameters of a service group.

Parameters

serviceGroupName

Name of the service group.

serverName

Name of the server to which to bind the service group.

monitorName

Name of the monitor bound to the service group. Used to assign a weight to the monitor.

maxClient

Maximum number of simultaneous open connections for the service group. Maximum value: 4294967294

maxReq

Maximum number of requests that can be sent on a persistent connection to the service group. Note: Connection requests beyond this value are rejected. Maximum value: 65535

healthMonitor

Monitor the health of this service. Available settings function as follows: YES - Send probes to check the health of the service. NO - Do not send probes to check the health of the service. With the NO option, the appliance shows the service as UP at all times. Possible values: YES, NO Default value: YES

cacheable

Use the transparent cache redirection virtual server to forward the request to the cache server. Note: Do not set this parameter if you set the Cache Type. Possible values: YES, NO Default value: NO

cip

Insert the Client IP header in requests forwarded to the service. Possible values: ENABLED, DISABLED

usip

Use client's IP address as the source IP address when initiating connection to the server. With the NO setting, which is the default, a mapped IP (MIP) address or subnet IP (SNIP) address is used as the source IP address to initiate server side connections. Possible values: YES, NO

pathMonitor

Path monitoring for clustering Possible values: YES, NO

pathMonitorIndv

Individual Path monitoring decisions. Possible values: YES, NO

useproxyport

Use the proxy port as the source port when initiating connections with the server. With the NO setting, the client-side connection port is used as the source port for the server-side connection. Note: This parameter is available only when the Use Source IP (USIP) parameter is set to YES. Possible values: YES, NO

sc

State of the SureConnect feature for the service group. Possible values: ON, OFF
Default value: OFF

sp

Enable surge protection for the service group. Possible values: ON, OFF
Default value: OFF

rtspSessionidRemap

Enable RTSP session ID mapping for the service group. Possible values: ON, OFF
Default value: OFF

cltTimeout

Time, in seconds, after which to terminate an idle client connection. Maximum value: 31536000

svrTimeout

Time, in seconds, after which to terminate an idle server connection. Maximum value: 31536000

CKA

Enable client keep-alive for the service group. Possible values: YES, NO

TCPB

Enable TCP buffering for the service group. Possible values: YES, NO

CMP

Enable compression for the specified service. Possible values: YES, NO

maxBandwidth

Maximum bandwidth, in Kbps, allocated for all the services in the service group. Maximum value: 4294967287

monThreshold

Minimum sum of weights of the monitors that are bound to this service. Used to determine whether to mark a service as UP or DOWN. Maximum value: 65535

downStateFlush

Perform delayed clean-up of connections to all services in the service group. Possible values: ENABLED, DISABLED
Default value: ENABLED

tcpProfileName

Name of the TCP profile that contains TCP configuration settings for the service group.

httpProfileName

Name of the HTTP profile that contains HTTP configuration settings for the service group.

comment

Any information about the service group.

appflowLog

Enable logging of AppFlow information for the specified service group. Possible values: ENABLED, DISABLED Default value: ENABLED

netProfile

Network profile for the service group.

Example

```
set servicegroup http_svc_group -maxClient 100
To set the attribute maxclient for multiple
servicegroups at once, use the following command:
set servicegroup http_svc_group[1-3] -
maxClient 100
```

[Top](#)

unset serviceGroup**Synopsis**

```
unset serviceGroup <serviceGroupName>@ [<serverName>@ <port> [-weight] [-
CustomServerID] [-hashId]] [-maxClient] [-maxReq] [-cacheable] [-cip] [-usip] [-
useproxyport] [-sc] [-sp] [-rtspSessionidRemap] [-cltTimeout] [-svrTimeout] [-CKA] [-
TCPB] [-CMP] [-maxBandwidth] [-monThreshold] [-tcpProfileName] [-httpProfileName]
[-appflowLog] [-netProfile] [-monitorName] [-weight] [-healthMonitor] [-cipHeader] [-
pathMonitor] [-pathMonitorIndv] [-downStateFlush] [-comment]
```

Description

Removes the attributes of the specified service group. Attributes for which a default value is available revert to their default values..Refer to the set serviceGroup command for meanings of the arguments.

Example

```
unset servicegroup http_svc_group -maxClient
```

[Top](#)

bind serviceGroup

Synopsis

```
bind serviceGroup <serviceGroupName> ((<IP>@ <port>) | <serverName>@ | ((-  
monitorName <string>@ [-monState ( ENABLED | DISABLED )] [-passive]) | -  
CustomServerID <string> | -state ( ENABLED | DISABLED ) | -hashId <positive_integer> |  
|)) [-weight <positive_integer>]
```

Description

Binds a service to a service group.

Parameters

serviceGroupName

Name of the service group.

IP

IP address of the server that hosts the service. Mutually exclusive with the Server Name parameter.

serverName

Name of the server that hosts the service. Mutually exclusive with the IP address parameter.

port

Port number of the service. Each service must have a unique port number.

monitorName

The name of the service or a service group to which the monitor is to be bound.

CustomServerID

Unique service identifier. Used when the persistency type for the virtual server is set to Custom Server ID. Default value: "None"

serverID

The identifier for the service. This is used when the persistency type is set to Custom Server ID.

state

Initial state of the service after binding. Possible values: ENABLED, DISABLED Default value: ENABLED

hashId

Unique numerical identifier used by hash based load balancing methods to identify a service. Minimum value: 1

Example

```
bind servicegroup http_svc_group 10.102.27.153 80  
    To bind multiple servers to a servicegroup,  
    following command can be used:
```

```
bind servicegroup http_svc_group 10.102.27.
[153-155] 80
```

[Top](#)

unbind serviceGroup

Synopsis

```
unbind serviceGroup <serviceName> ((<IP>@ <port>) | <serverName>@ | -
monitorName <string>@)
```

Description

Unbinds a service or a monitor from a service group.

Parameters

serviceName

Name of the service group.

IP

IP address of the server that hosts the service. Mutually exclusive with the Server Name parameter.

serverName

Name of the server that hosts the service. Mutually exclusive with the IP Address parameter.

port

Port number of the service.

monitorName

Name of the monitor to bind to the service group.

Example

```
unbind servicegroup http_svc_group 10.102.27.153 80
To unbind multiple servers following command
can be used:
unbind servicegroup http_svc_group 10.102.27.
[153-155] 80
```

[Top](#)

enable serviceGroup

Synopsis

```
enable serviceGroup <serviceName>@ [<serverName>@ <port>]
```

Description

Enables a service group or a member of the service group.

Parameters

serviceGroupName

Name of the service group.

serverName

Name of the server that hosts the service.

port

Port number of the service to be enabled.

Example

```
enable servicegroup http_svc_group
    To enable multiple service groups at one go
    use the following command:
    enable servicegroup http_svc_group[1-3]
```

[Top](#)

disable serviceGroup

Synopsis

disable serviceGroup <serviceGroupName>@ [<serverName>@ <port>] [-delay <secs>] [-graceFul (YES | NO)]

Description

Disables a service group or a member of a service group. To disable a service group, provide only the service group name. To disable only a member of a service group, in addition to the service group name, provide the name of the server that hosts the service, and the port number of the service.

Parameters

serviceGroupName

Name of the service group.

serverName

Name of the server that hosts the service.

port

Port number of the service.

delay

Time, in seconds, allocated for a shutdown of the services in the service group. During this period, new requests are sent to the service only for clients who already have persistent sessions on the appliance. Requests from new clients are load balanced among other available services. After the delay time expires, no requests are sent to the service, and the service is marked as unavailable (OUT OF SERVICE).

graceFul

Wait for all existing connections to the service to terminate before shutting down the service. Possible values: YES, NO Default value: NO

Example

```
disable servicegroup http_svc_group 10.102.27.153
80 -delay 10
    To disable multiple servicegroups use the
    following command:
    disable servicegroup http_svc_group[1-3]
10.102.27.[153-155] 80 -delay 30
```

[Top](#)

show serviceGroup**Synopsis**

show serviceGroup [<serviceName> | -includeMembers]

Description

Displays the specified service group's binding information.

Parameters**serviceName**

Name of the service group.

includeMembers

Display the members of the listed service groups in addition to their settings. Can be specified when no service group name is provided in the command. In that case, the details displayed for each service group are identical to the details displayed when a service group name is provided, except that bound monitors are not displayed.

[Top](#)

stat serviceGroup**Synopsis**

stat serviceGroup [<serviceName>] [-detail] [-fullValues] [-ntimes
<positive_integer>] [-logFile <input_filename>] [-clearstats (basic | full)]

Description

Displays configuration statistics of the specified service group or all the service groups configured on the appliance.

Parameters**serviceName**

Name of the service group for which to display settings.

clearstats

Clear the statistics / counters Possible values: basic, full

[Top](#)

rename serviceGroup

Synopsis

rename serviceGroup <serviceName>@ <newName>@

Description

Renames a service group.

Parameters

serviceName

Existing name of the service group.

newName

New name for the service group.

Example

```
rename service svcgrp1 svcgrp-new1
```

[Top](#)

dbMonitors

restart dbMonitors

Synopsis

restart dbMonitors

Description

Immediately send DNS queries to resolve the domain names of all the domain-based servers configured on the NetScaler appliance.

Example

```
restart dbMonitors
```

locationData

clear locationData

Synopsis

clear locationData

Description

Clears all location information, including custom and static database entries.

Example

```
clear locationdata
```

svcbindings

show svcbindings

Synopsis

show svcbindings <serviceName>

Description

Displays a list of all virtual servers to which the service is bound.

Parameters

serviceName

The name of the service.

servicegroupbindings

show servicegroupbindings

Synopsis

show servicegroupbindings <serviceName>

Description

Displays servicegroup information followed by vservers bound to it.

Parameters

serviceName

The name of the service.

serviceGroupMember

stat serviceGroupMember

Synopsis

```
stat serviceGroupMember <serviceGroupName> (<IP> | <serverName>) <port> [-detail]
[-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-clearstats
( basic | full )]
```

Description

Display statistics of a service group member.

Parameters

serviceGroupName

Displays statistics for the specified service group. Name of the service group. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my servicegroup" or 'my servicegroup').

IP

IP address of the service group. Mutually exclusive with the server name parameter.

serverName

Name of the server. Mutually exclusive with the IP address parameter.

port

Port number of the service group member.

clearstats

Clear the statistics / counters Possible values: basic, full

configstatus

show configstatus

Synopsis

```
show configstatus
```

Description

Display status of packet engines.

Example

```
show configstatus
```

locationParameter

[[set](#) | [unset](#) | [show](#)]

set locationParameter

Synopsis

```
set locationParameter [-context ( geographic | custom )] [-q1label <string>] [-q2label <string>] [-q3label <string>] [-q4label <string>] [-q5label <string>] [-q6label <string>]
```

Description

Sets the location parameters used for static-proximity based global server load balancing. Location parameters include up to six qualifiers and a context that specifies how the qualifiers must be interpreted. Each qualifier specifies the location of an IP address range and is more specific than the one that precedes it, as in continent.country.region.city.isp.organization. For example, "NA.US.CA.San Jose.ATT.citrix". Note: A qualifier that includes a dot (.) or space () must be enclosed in double quotation marks.

Parameters

context

Context for describing locations. In geographic context, qualifier labels are assigned by default in the following sequence: Continent.Country.Region.City.ISP.Organization. In custom context, the qualifiers labels can have any meaning that you designate. Possible values: geographic, custom

q1label

Label specifying the meaning of the first qualifier. Can be specified for custom context only.

q2label

Label specifying the meaning of the second qualifier. Can be specified for custom context only.

q3label

Label specifying the meaning of the third qualifier. Can be specified for custom context only.

q4label

Label specifying the meaning of the fourth qualifier. Can be specified for custom context only.

q5label

Label specifying the meaning of the fifth qualifier. Can be specified for custom context only.

q6label

Label specifying the meaning of the sixth qualifier. Can be specified for custom context only.

Example

```
set locationparameter -context    custom
```

[Top](#)

unset locationParameter

Synopsis

```
unset locationParameter [-context] [-q1label] [-q2label] [-q3label] [-q4label] [-q5label]
[-q6label]
```

Description

Use this command to remove locationParameter settings. Refer to the set locationParameter command for meanings of the arguments.

[Top](#)

show locationParameter

Synopsis

```
show locationParameter
```

Description

Displays current values for the location parameters, which are used for static-proximity based load balancing.

Example

```
show locationparameter
```

[Top](#)

vserver

show vserver

Synopsis

```
show vserver
```

Description

Displays information about all virtual servers configured on the appliance.

Example

```
show vserver lb_vip
```

uiinternal

[[set](#) | [unset](#) | [show](#)]

set uiinternal

Synopsis

```
set uiinternal <entityType> <name> [-template <string>] [-comment <string>] [-rule <string>]
```

Description

set uiinternal data for the entities

Parameters

entityType

The entity type of UI internal data Possible values: LBVSERVER, GSLBVSERVER, CRVSERVER, VPNVSERVER, CSVSERVER, AUTHENTICATIONVSERVER, SERVER, SERVICE, SERVICEGROUP, GSLBSERVICE, EXPRESSION, VPNURL

name

The entity name

template

The application template associated with entity

comment

The application template associated with entity

rule

rules associated with entity

Example

```
set uiinternal lbvserver v1 -template app1
```

[Top](#)

unset uiinternal

Synopsis

```
unset uiinternal <entityType> <name> [-template] [-comment] [-rule] [-all]
```

Description

unset uiinternal for the entities. Refer to the set uiinternal command for meanings of the arguments.

Example

```
unset uiinternal lbvserver v1 -template app1
```

[Top](#)

show uiinternal

Synopsis

show uiinternal [<entityType>] [<name>]

Description

display all UI internal data information for the entities

Parameters

entityType

The entity type of UI internal data Possible values: LBVSERVER, GSLBVSERVER, CRVSERVER, VPNVSERVER, CSVSERVER, AUTHENTICATIONVSERVER, SERVER, SERVICE, SERVICEGROUP, GSLBSERVICE, EXPRESSION, VPNURL

name

The entity name

Example

```
show uiinternal LBVSERVER v1
```

[Top](#)

reporting

[[enable](#) | [disable](#) | [show](#)]

enable reporting

Synopsis

enable reporting

Description

Enable the data collection for reporting module.

Example

```
enable reporting
```

[Top](#)

disable reporting

Synopsis

disable reporting

Description

Disable the data collection for reporting module.

Example

```
disable reporting
```

[Top](#)

show reporting

Synopsis

show reporting

Description

show the state of data collection for reporting module.

Example

```
show reporting
```

[Top](#)

nstrace

[[start](#) | [stop](#) | [show](#)]

start nstrace

Synopsis

start nstrace [-nf <positive_integer>] [-time <positive_integer>] [-size <positive_integer>] [-mode <mode> ...] [-tcpdump (ENABLED | DISABLED)] [-perNIC (ENABLED | DISABLED)] [-fileName <string>] [-fileId <string>] [-filter <expression>] [-link (ENABLED | DISABLED)] [-nodes <positive_integer> ...]

Description

Start NetScaler packet capture tool.

Parameters

nf

Number of files to be generated in cycle. Default value: 24 Minimum value: 1
Maximum value: 100

time

Time per file (sec). Default value: 3600 Minimum value: 1

size

Size of the captured data. Set 0 for full packet trace. Default value: 164 Maximum value: 1514

mode

Capturing mode for trace. Mode can be any of the following values or combination of these values: RX Received packets before NIC pipelining NEW_RX Received packets after NIC pipelining TX Transmitted packets TXB Packets buffered for transmission IPV6 Translated IPv6 packets C2C Capture C2C message NS_FR_TX TX/TXB packets are not captured in flow receiver. Default mode: NEW_RX TXB Default value: DEFAULT_MODE

tcpdump

Trace is captured in TCPDUMP(.pcap) format. Default capture format is NSTRACE(.cap). Possible values: ENABLED, DISABLED Default value: DISABLED

perNIC

Use separate trace files for each interface. Works only with tcpdump format. Possible values: ENABLED, DISABLED Default value: DISABLED

fileName

Name of the trace file.

fileId

ID for the trace file name for uniqueness. Should be used only with -name option.

filter

Filter expression for nstrace. Maximum length of filter is 255 and it can be of following format: <expression> [<relop> <expression>] <relop> = (&& | ||) nstrace supports two types of filter expressions: Classic Expressions: <expression> = the expression string in the format: <qualifier> <operator> <qualifier-value> <qualifier> = SOURCEIP. <qualifier-value> = A valid IP address <qualifier> = SOURCEPORT. <qualifier-value> = A valid port number. <qualifier> = DESTIP. <qualifier-value> = A valid IP address. <qualifier> = DESTPORT. <qualifier-value> = A valid port number. <qualifier> = IP. <qualifier-value> = A valid IP address. <qualifier> = PORT. <qualifier-value> = A valid port number. <qualifier> = SVCNAME. <qualifier-value> = The name of a service. <qualifier> = VSVRNAME. <qualifier-value> = The name of a vserver. <qualifier> = CONNID <qualifier-value> = A valid PCB dev number. <qualifier> = VLAN <qualifier-value> = A valid VLAN ID. <qualifier> = INTF <qualifier-value> = A valid interface id in the form of x/y (n/x/y in case of cluster interface). <operator> = (== | eq | != | neq | > | gt | < | lt | >= | ge | <= | le | BETWEEN) eg: start nstrace - filter "SOURCEIP == 10.102.34.201 || (SVCNAME != s1 && SOURCEPORT > 80)" The filter expression should be given in double quotes. Default Expressions: <expression> =: CONNECTION.<qualifier>.<qualifier-method>.<qualifier-value> <qualifier> = SRCIP <qualifier-method> = [EQ | NE] <qualifier-value> = A valid IPv4 address. example = CONNECTION.SRCIP.EQ(127.0.0.1) <qualifier> = DSTIP <qualifier-method> = [EQ | NE] <qualifier-value> = A valid IPv4 address. example = CONNECTION.DSTIP.EQ(127.0.0.1) <qualifier> = IP <qualifier-method> = [EQ | NE] <qualifier-value> = A valid IPv4 address. example = CONNECTION.IP.EQ(127.0.0.1) <qualifier> = SRCIPv6 <qualifier-method> = [EQ | NE] <qualifier-value> = A valid IPv6 address. example = CONNECTION.SRCIPv6.EQ(2001:db8:0:0:1::1) <qualifier> = DSTIPv6 <qualifier-method> = [EQ | NE] <qualifier-value> = A valid IPv6 address. example = CONNECTION.DSTIPv6.EQ(2001:db8:0:0:1::1) <qualifier> = IPv6 <qualifier-

method> = [EQ | NE] <qualifier-value> = A valid IPv6 address. example = CONNECTION.IPv6.EQ(2001:db8:0:0:1::1) <qualifier> = SRCPORT <qualifier-method> = [EQ | NE | GT | GE | LT | LE] <qualifier-value> = A valid port number. example = CONNECTION.SRCPORT.EQ(80) <qualifier> = DSTPORT <qualifier-method> = [EQ | NE | GT | GE | LT | LE] <qualifier-value> = A valid port number. example = CONNECTION.DSTPORT.EQ(80) <qualifier> = PORT <qualifier-method> = [EQ | NE] <qualifier-value> = A valid port number. example = CONNECTION.PORT.EQ(80) <qualifier> = VLANID <qualifier-method> = [EQ | NE | GT | GE | LT | LE] <qualifier-value> = A valid vlan ID. example = CONNECTION.VLANID.EQ(0) <qualifier> = CONNID <qualifier-method> = [EQ | NE | GT | GE | LT | LE] <qualifier-value> = A valid PCB dev number. example = CONNECTION.CONNID.EQ(0) <qualifier> = PPEID <qualifier-method> = [EQ | NE | GT | GE | LT | LE] <qualifier-value> = A valid core ID. example = CONNECTION.PPEID.EQ(0) <qualifier> = SVCNAME <qualifier-method> = [EQ | NE | CONTAINS | STARTSWITH | ENDSWITH] <qualifier-value> = A valid text string. example = CONNECTION.SVCNAME.EQ("name") <qualifier> = INTF <qualifier-method> = [EQ | NE] <qualifier-value> = A valid interface id in the form of x/y. example = CONNECTION.INTF.EQ("x/y") eg: start nstrace -filter "CONNECTION.SRCIP.EQ(127.0.0.1) || (CONNECTION.SVCNAME.NE("s1") && CONNECTION.SRCPORT.EQ(80))" The filter expression should be given in double quotes. common use cases: Trace capturing full sized traffic from/to ip 10.102.44.111, excluding loopback traffic start nstrace -size 0 -filter "CONNECTION.IP.NE(127.0.0.1) && CONNECTION.IP.EQ(10.102.44.111)" Trace capturing all traffic to (terminating at) port 80 or 443 start nstrace -size 0 -filter "CONNECTION.DSTPORT.EQ(443) || CONNECTION.DSTPORT.EQ(80)" Trace capturing all backend traffic specific to service service1 along with corresponding client side traffic start nstrace -size 0 -filter "CONNECTION.SVCNAME.EQ("service1")" -link ENABLED Trace capturing all traffic through NS interface 1/1 start nstrace -filter "CONNECTION.INTF.EQ("1/1")" Trace capturing all traffic specific through vlan 2 start nstrace -filter "CONNECTION.VLANID.EQ(2)" Trace capturing all frontend (client side) traffic specific to lb vserver vserver1 along with corresponding server side traffic start nstrace -size 0 -filter "CONNECTION.LB_VSERVER.NAME.EQ("vserver1")" -link ENABLED

link

Includes filtered connection's peer traffic. Possible values: ENABLED, DISABLED
Default value: DISABLED

nodes

Nodes on which tracing is started. Maximum value: 32

Example

```
start nstrace -time 10
```

[Top](#)

stop nstrace**Synopsis**

```
stop nstrace
```

Description

Stop running NetScaler packet capture tool.

Example

```
stop nstrace
```

[Top](#)

show nstrace

Synopsis

show nstrace

Description

Display nstrace parameters set through 'start nstrace' command.

Example

```
show nstrace
```

[Top](#)

Cache Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [cache](#)
- ♦ [cache policy](#)
- ♦ [cache policylabel](#)
- ♦ [cache contentGroup](#)
- ♦ [cache forwardProxy](#)
- ♦ [cache selector](#)
- ♦ [cache object](#)
- ♦ [cache stats](#)
- ♦ [cache global](#)
- ♦ [cache parameter](#)

cache

stat cache

Synopsis

```
stat cache [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile
<input_filename>] [-clearstats ( basic | full )]
```

Description

Shows Integrated Cache performance statistics.

Parameters

clearstats

Clear the statistics / counters Possible values: basic, full

cache policy

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#) | [stat](#) | [rename](#)]

add cache policy

Synopsis

```
add cache policy <policyName> -rule <expression> -action <action> [-storeInGroup
<string>] [-invalGroups <string> ...] [-invalObjects <string> ...] [-undefAction
( NOCACHE | RESET )]
```

Description

Creates an integrated caching policy. The newly created policy is in inactive state. To activate the policy, use the bind cache global command.

Parameters

policyName

Name for the policy. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the policy is created.

rule

Expression against which the traffic is evaluated. Note: Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>". The following requirements apply only to the NetScaler CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action

Action to apply to content that matches the policy. * CACHE or MAY_CACHE action - positive cachability policy * NOCACHE or MAY_NOCACHE action - negative cachability

policy * INVALID action - Dynamic Invalidation Policy Possible values: CACHE, NOCACHE, MAY_CACHE, MAY_NOCACHE, INVALID

storeInGroup

Name of the content group in which to store the object when the final result of policy evaluation is CACHE. The content group must exist before being mentioned here. Use the "show cache contentgroup" command to view the list of existing content groups.

invalidGroups

Content group(s) to be invalidated when the INVALID action is applied. Maximum number of content groups that can be specified is 16.

invalidObjects

Content groups(s) in which the objects will be invalidated if the action is INVALID.

undefAction

Action to be performed when the result of rule evaluation is undefined. Possible values: NOCACHE, RESET

[Top](#)

rm cache policy

Synopsis

rm cache policy <policyName>

Description

Removes the specified caching policy. Make sure that the policy is not bound globally or to a virtual server. A bound policy cannot be removed.

Parameters

policyName

Name of the cache policy to be removed.

[Top](#)

set cache policy

Synopsis

set cache policy <policyName> [-rule <expression>] [-action <action>] [-storeInGroup <string>] [-invalidGroups <string> ...] [-invalidObjects <string> ...] [-undefAction (NOCACHE | RESET)]

Description

Modifies the specified attributes of an existing cache policy. The rule, flow type, can be changed only if action and undefAction (if present) are of NEUTRAL flow type.

Parameters

policyName

Name for the policy. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space,

colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the policy is created.

rule

Expression against which the traffic is evaluated. Note: Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>". The following requirements apply only to the NetScaler CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action

Action to apply to content that matches the policy. * CACHE or MAY_CACHE action - positive cachability policy * NOCACHE or MAY_NOCACHE action - negative cachability policy * INVALID action - Dynamic Invalidation Policy Possible values: CACHE, NOCACHE, MAY_CACHE, MAY_NOCACHE, INVALID

storeInGroup

Name of the content group in which to store the object when the final result of policy evaluation is CACHE. The content group must exist before being mentioned here. Use the "show cache contentgroup" command to view the list of existing content groups.

invalGroups

Content group(s) to be invalidated when the INVALID action is applied. Maximum number of content groups that can be specified is 16.

invalObjects

Content groups(s) in which the objects will be invalidated if the action is INVALID.

undefAction

Action to be performed when the result of rule evaluation is undefined. Possible values: NOCACHE, RESET

Example

```
set cache policy pol9 -rule "http.req.HEADER(\
\"header\\") .CONTAINS (\\\"qh2\\\") "
```

[Top](#)

unset cache policy

Synopsis

```
unset cache policy <policyName> [-storeInGroup] [-invalGroups] [-invalObjects] [-undefAction]
```

Description

Use this command to remove cache policy settings. Refer to the set cache policy command for meanings of the arguments.

[Top](#)

show cache policy

Synopsis

show cache policy [<policyName>] show cache policy stats - alias for 'stat cache policy'

Description

Displays all configured cache policies. To display details about a particular cache policy, specify the name of the policy. When all caching policies are displayed, the order of the displayed policies within each group is the same as the evaluation order of the policies. There are three groups: request policies, response policies, and dynamic invalidation policies.

Parameters

policyName

Name of the cache policy about which to display details.

[Top](#)

stat cache policy

Synopsis

stat cache policy [<policyName>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-clearstats (basic | full)]

Description

Displays a summary of cache policy statistics.

Parameters

policyName

Name of the cache policy for which to display statistics. If you do not set this parameter, statistics are shown for all cache policies.

clearstats

Clear the statistics / counters Possible values: basic, full

Example

```
stat cache policy
```

[Top](#)

rename cache policy

Synopsis

rename cache policy <policyName>@ <newName>@

Description

Renames an existing cache policy.

Parameters

policyName

Existing name of the cache policy.

newName

New name for the cache policy. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

Example

```
rename cache policy oldname newname
```

[Top](#)

cache policylabel

[[add](#) | [rm](#) | [bind](#) | [unbind](#) | [show](#) | [stat](#) | [rename](#)]

add cache policylabel

Synopsis

add cache policylabel <labelName> -evaluates <evaluates>

Description

Creates a user-defined cache policy label. A policy label is a bind point of a group of policies.

Parameters

labelName

Name for the label. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the label is created.

evaluates

When to evaluate policies bound to this label: request-time or response-time.
Possible values: REQ, RES, MSSQL_REQ, MSSQL_RES, MYSQL_REQ, MYSQL_RES

Example

```
add cache policylabel cache_http_url -evaluates REQ
```

[Top](#)

rm cache policylabel

Synopsis

```
rm cache policylabel <labelName>
```

Description

Removes the specified integrated caching policy label.

Parameters

labelName

Name of the label to be removed.

Example

```
rm cache policylabel cache_http_url
```

[Top](#)

bind cache policylabel

Synopsis

```
bind cache policylabel <labelName> -policyName <string> -priority <positive_integer> [-  
gotoPriorityExpression <expression>] [-invoke (<labelType> <labelName>)]
```

Description

Binds a cache policy to a policy label.

Parameters

labelName

Name of the cache policy label to which to bind the policy.

policyName

Name of the cache policy to bind to the policy label.

Example

```
i)    bind cache policylabel cache_http_url pol_1  
1 2 -invoke reqvserver CURRENT  
      ii)    bind cache policylabel cache_http_url  
pol_2 2
```


[Top](#)

unbind cache policylabel

Synopsis

unbind cache policylabel <labelName> -policyName <string> [-priority <positive_integer>]

Description

Unbinds a policy from a cache-policy label.

Parameters

labelName

Name of the cache policy label from which to unbind the policy.

policyName

Name of the policy to unbind from the label.

priority

Required only if you want to unbind a NOPOLICY that might have been bound to this policy label. Minimum value: 1 Maximum value: 2147483647

Example

```
unbind cache policylabel cache_http_url pol_1
```

[Top](#)

show cache policylabel

Synopsis

show cache policylabel [<labelName>]

Description

Displays information about all cache-policy labels or about the specified cache-policy label.

Parameters

labelName

Name of the cache-policy label about which to display information.

Example

```
i)    show cache policylabel cache_http_url
ii)   show cache policylabel
```

[Top](#)

stat cache policylabel

Synopsis

```
stat cache policylabel [<labelName>] [-detail] [-fullValues] [-ntimes <positive_integer>]
[-logFile <input_filename>] [-clearstats ( basic | full )]
```

Description

Displays statistics of cache policy label(s).

Parameters

labelName

Name of the cache-policy label for which to display statistics. If you do not set this parameter statistics are shown for all cache-policy labels.

clearstats

Clear the statistics / counters Possible values: basic, full

[Top](#)

rename cache policylabel

Synopsis

```
rename cache policylabel <labelName>@ <newName>@
```

Description

Renames a cache-policy label.

Parameters

labelName

Existing name of the cache-policy label.

newName

New name for the cache-policy label. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

Example

```
rename cache policylabel oldname newname
```

[Top](#)

cache contentGroup

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#) | [expire](#) | [flush](#) | [save](#)]

add cache contentGroup

Synopsis

```
add cache contentGroup <name> [-weakPosRelExpiry <secs> | -relExpiry <secs> | -
relExpiryMilliSec <msecs> | -absExpiry <HH:MM> ... | -absExpiryGMT <HH:MM> ...] [-
heurExpiryParam <positive_integer>] [-weakNegRelExpiry <secs>] [(-hitParams
<string> ... [-ignoreParamValueCase ( YES | NO ) | -hitSelector <string> | -invalSelector
<string>] [-matchCookies ( YES | NO )]) [-invalParams <string> ... [-
invalRestrictedToHost ( YES | NO )]] [-pollEveryTime ( YES | NO )] [-ignoreReloadReq
( YES | NO )] [-removeCookies ( YES | NO )] [-prefetch ( YES | NO ) [-prefetchPeriod
<secs> | -prefetchPeriodMilliSec <msecs>]] [-prefetchMaxPending <positive_integer>] [-
flashCache ( YES | NO )] [-expireAtLastByte ( YES | NO )] [-insertVia ( YES | NO )] [-
insertAge ( YES | NO )] [-insertETag ( YES | NO )] [-cacheControl <string>] [-
quickAbortSize <KBytes>] [-minResSize <KBytes>] [-maxResSize <KBytes>] [-memLimit
<MBytes>] [-ignoreReqCachingHdrs ( YES | NO )] [-minHits <integer>] [-
alwaysEvalPolicies ( YES | NO )] [-persist ( YES | NO )] [-pinned ( YES | NO )] [-
lazyDnsResolve ( YES | NO )] [-type <type>]
```

Description

Creates a new content group for grouping cached objects on the basis of some unique property.

Parameters

name

Name for the content group. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the content group is created.

weakPosRelExpiry

Relative expiry time, in seconds, for expiring positive responses with response codes between 200 and 399. Cannot be used in combination with other Expiry attributes. Similar to -relExpiry but has lower precedence. Default value: VAL_NOT_SET Maximum value: 31536000

heurExpiryParam

Heuristic expiry time, in percent of the duration, since the object was last modified. Default value: VAL_NOT_SET Maximum value: 100

relExpiry

Relative expiry time, in seconds, after which to expire an object cached in this content group. Default value: VAL_NOT_SET Maximum value: 31536000

relExpiryMilliSec

Relative expiry time, in milliseconds, after which to expire an object cached in this content group. Default value: VAL_NOT_SET Maximum value: 86400000

absExpiry

Local time, up to 4 times a day, at which all objects in the content group must expire. CLI Users: For example, to specify that the objects in the content group should expire by 11:00 PM, type the following command: add cache contentgroup <contentgroup name> -absexpiry 23:00 To specify that the objects in the content

group should expire at 10:00 AM, 3 PM, 6 PM, and 11:00 PM, type: add cache
contentgroup <contentgroup name> -absexpiry 10:00 15:00 18:00 23:00

absExpiryGMT

Coordinated Universal Time (GMT), up to 4 times a day, when all objects in the content group must expire.

weakNegRelExpiry

Relative expiry time, in seconds, for expiring negative responses. This value is used only if the expiry time cannot be determined from any other source. It is applicable only to the following status codes: 307, 403, 404, and 410. Default value: VAL_NOT_SET Maximum value: 31536000

hitParams

Parameters to use for parameterized hit evaluation of an object. Up to 128 parameters can be specified. Mutually exclusive with the Hit Selector parameter.

invalParams

Parameters for parameterized invalidation of an object. You can specify up to 8 parameters. Mutually exclusive with invalSelector.

ignoreParamValueCase

Ignore case when comparing parameter values during parameterized hit evaluation. (Parameter value case is ignored by default during parameterized invalidation.) Possible values: YES, NO Default value: VAL_NOT_SET

matchCookies

Evaluate for parameters in the cookie header also. Possible values: YES, NO Default value: VAL_NOT_SET

invalRestrictedToHost

Take the host header into account during parameterized invalidation. Possible values: YES, NO Default value: VAL_NOT_SET

pollEveryTime

Always poll for the objects in this content group. That is, retrieve the objects from the origin server whenever they are requested. Possible values: YES, NO Default value: NO

ignoreReloadReq

Ignore any request to reload a cached object from the origin server. To guard against Denial of Service attacks, set this parameter to YES. For RFC-compliant behavior, set it to NO. Possible values: YES, NO Default value: YES

removeCookies

Remove cookies from responses. Possible values: YES, NO Default value: YES

prefetch

Attempt to refresh objects that are about to go stale. Possible values: YES, NO Default value: YES

prefetchPeriod

Time period, in seconds before an object's calculated expiry time, during which to attempt prefetch. Default value: VAL_NOT_SET Maximum value: 4294967294

prefetchPeriodMilliSec

Time period, in milliseconds before an object's calculated expiry time, during which to attempt prefetch. Default value: VAL_NOT_SET Maximum value: 4294967290

prefetchMaxPending

Maximum number of outstanding prefetches that can be queued for the content group. Default value: VAL_NOT_SET Maximum value: 4294967294

flashCache

Perform flash cache. Mutually exclusive with Poll Every Time (PET) on the same content group. Possible values: YES, NO Default value: NO

expireAtLastByte

Force expiration of the content immediately after the response is downloaded (upon receipt of the last byte of the response body). Applicable only to positive responses. Possible values: YES, NO Default value: NO

insertVia

Insert a Via header into the response. Possible values: YES, NO Default value: YES

insertAge

Insert an Age header into the response. An Age header contains information about the age of the object, in seconds, as calculated by the integrated cache. Possible values: YES, NO Default value: YES

insertETag

Insert an ETag header in the response. With ETag header insertion, the integrated cache does not serve full responses on repeat requests. Possible values: YES, NO Default value: YES

cacheControl

Insert a Cache-Control header into the response.

quickAbortSize

If the size of an object that is being downloaded is less than or equal to the quick abort value, and a client aborts during the download, the cache stops downloading the response. If the object is larger than the quick abort size, the cache continues to download the response. Default value: 4194303 Maximum value: 4194303

minResSize

Minimum size of a response that can be cached in this content group. Default minimum response size is 0. Maximum value: 2097151

maxResSize

Maximum size of a response that can be cached in this content group. Default value: 80 Maximum value: 2097151

memLimit

Maximum amount of memory that the cache can use. The effective limit is based on the available memory of the NetScaler appliance. Default value: 65536

ignoreReqCachingHdrs

Ignore Cache-Control and Pragma headers in the incoming request. Possible values: YES, NO Default value: YES

minHits

Number of hits that qualifies a response for storage in this content group.

alwaysEvalPolicies

Force policy evaluation for each response arriving from the origin server. Cannot be set to YES if the Prefetch parameter is also set to YES. Possible values: YES, NO
Default value: NO

persist

Setting persist to YES causes IC to save objects in contentgroup to disk. Possible values: YES, NO Default value: NO

pinned

Do not flush objects from this content group under memory pressure. Possible values: YES, NO Default value: NO

lazyDnsResolve

Perform DNS resolution for responses only if the destination IP address in the request does not match the destination IP address of the cached response. Possible values: YES, NO Default value: YES

hitSelector

Selector for evaluating whether an object gets stored in a particular content group. A selector is an abstraction for a collection of PIXL expressions.

invalidSelector

Selector for invalidating objects in the content group. A selector is an abstraction for a collection of PIXL expressions.

type

The type of the content group. Possible values: HTTP, MYSQL, MSSQL Default value: NSSVC_HTTP

[Top](#)

rm cache contentGroup

Synopsis

```
rm cache contentGroup <name>
```

Description

Removes the specified content group. Before removing, make sure that no cache policy has its storeInGroup attribute set to this group, otherwise the group cannot be removed.

Parameters

name

Name of the content group to be removed.

[Top](#)

set cache contentGroup

Synopsis

```
set cache contentGroup <name> [-weakPosRelExpiry <secs> | -relExpiry <secs> | -
relExpiryMilliSec <msecs> | -absExpiry <HH:MM> ... | -absExpiryGMT <HH:MM> ...] [-
heurExpiryParam <positive_integer>] [-weakNegRelExpiry <secs>] [-hitParams
<string> ... | -hitSelector <string> | -invalSelector <string>] [-invalParams <string> ...]
[-ignoreParamValueCase ( YES | NO )] [-matchCookies ( YES | NO )] [-
invalRestrictedToHost ( YES | NO )] [-pollEveryTime ( YES | NO )] [-ignoreReloadReq
( YES | NO )] [-removeCookies ( YES | NO )] [-prefetch ( YES | NO )] [-prefetchPeriod
<secs> | -prefetchPeriodMilliSec <msecs>] [-prefetchMaxPending <positive_integer>] [-
flashCache ( YES | NO )] [-expireAtLastByte ( YES | NO )] [-insertVia ( YES | NO )] [-
insertAge ( YES | NO )] [-insertETag ( YES | NO )] [-cacheControl <string>] [-
quickAbortSize <KBytes>] [-minResSize <KBytes>] [-maxResSize <KBytes>] [-memLimit
<MBytes>] [-ignoreReqCachingHdrs ( YES | NO )] [-minHits <integer>] [-
alwaysEvalPolicies ( YES | NO )] [-persist ( YES | NO )] [-pinned ( YES | NO )] [-
lazyDnsResolve ( YES | NO )]
```

Description

Modifies the specified attributes of the content group.

Parameters

name

Name of the content group to be modified.

weakPosRelExpiry

Relative expiry time, in seconds, for expiring positive responses with response codes between 200 and 399. Cannot be used in combination with other Expiry attributes. Similar to -relExpiry but has lower precedence. Maximum value: 31536000

heurExpiryParam

Heuristic expiry time, in percent of the duration, since the object was last modified. Maximum value: 100

relExpiry

Relative expiry time, in seconds, after which to expire an object cached in this content group. Default value: VAL_NOT_SET Maximum value: 31536000

relExpiryMilliSec

Relative expiry time, in milliseconds, after which to expire an object cached in this content group. Default value: VAL_NOT_SET Maximum value: 86400000

absExpiry

Local time, up to 4 times a day, at which all objects in the content group must expire. CLI Users: For example, to specify that the objects in the content group should expire by 11:00 PM, type the following command: add cache contentgroup <contentgroup name> -absexpiry 23:00 To specify that the objects in the content group should expire at 10:00 AM, 3 PM, 6 PM, and 11:00 PM, type: add cache contentgroup <contentgroup name> -absexpiry 10:00 15:00 18:00 23:00

absExpiryGMT

Coordinated Universal Time (GMT), up to 4 times a day, when all objects in the content group must expire.

weakNegRelExpiry

Relative expiry time, in seconds, for expiring negative responses. This value is used only if the expiry time cannot be determined from any other source. It is applicable only to the following status codes: 307, 403, 404, and 410. Maximum value: 31536000

hitParams

Parameters to use for parameterized hit evaluation of an object. Up to 128 parameters can be specified. Mutually exclusive with the Hit Selector parameter.

invalidParams

Parameters for parameterized invalidation of an object. You can specify up to 8 parameters. Mutually exclusive with invalidSelector.

ignoreParamValueCase

Ignore case when comparing parameter values during parameterized hit evaluation. (Parameter value case is ignored by default during parameterized invalidation.) Possible values: YES, NO

matchCookies

Evaluate for parameters in the cookie header also. Possible values: YES, NO

invalidRestrictedToHost

Take the host header into account during parameterized invalidation. Possible values: YES, NO

pollEveryTime

Always poll for the objects in this content group. That is, retrieve the objects from the origin server whenever they are requested. Possible values: YES, NO Default value: NO

ignoreReloadReq

Ignore any request to reload a cached object from the origin server. To guard against Denial of Service attacks, set this parameter to YES. For RFC-compliant behavior, set it to NO. Possible values: YES, NO Default value: YES

removeCookies

Remove cookies from responses. Possible values: YES, NO Default value: YES

prefetch

Attempt to refresh objects that are about to go stale. Possible values: YES, NO Default value: YES

prefetchPeriod

Time period, in seconds before an object's calculated expiry time, during which to attempt prefetch. Default value: VAL_NOT_SET Maximum value: 4294967294

prefetchPeriodMilliSec

Time period, in milliseconds before an object's calculated expiry time, during which to attempt prefetch. Default value: VAL_NOT_SET Maximum value: 4294967290

prefetchMaxPending

Maximum number of outstanding prefetches that can be queued for the content group. Maximum value: 4294967294

flashCache

Perform flash cache. Mutually exclusive with Poll Every Time (PET) on the same content group. Possible values: YES, NO Default value: NO

expireAtLastByte

Force expiration of the content immediately after the response is downloaded (upon receipt of the last byte of the response body). Applicable only to positive responses. Possible values: YES, NO Default value: NO

insertVia

Insert a Via header into the response. Possible values: YES, NO Default value: YES

insertAge

Insert an Age header into the response. An Age header contains information about the age of the object, in seconds, as calculated by the integrated cache. Possible values: YES, NO Default value: YES

insertETag

Insert an ETag header in the response. With ETag header insertion, the integrated cache does not serve full responses on repeat requests. Possible values: YES, NO Default value: YES

cacheControl

Insert a Cache-Control header into the response.

quickAbortSize

If the size of an object that is being downloaded is less than or equal to the quick abort value, and a client aborts during the download, the cache stops downloading the response. If the object is larger than the quick abort size, the cache continues to download the response. Maximum value: 4194303

minResSize

Minimum size of a response that can be cached in this content group. Default minimum response size is 0. Maximum value: 2097151

maxResSize

Maximum size of a response that can be cached in this content group. Default value: 80 Maximum value: 2097151

memLimit

Maximum amount of memory that the cache can use. The effective limit is based on the available memory of the NetScaler appliance. Default value: 65536

ignoreReqCachingHdrs

Ignore Cache-Control and Pragma headers in the incoming request. Possible values: YES, NO Default value: YES

minHits

Number of hits that qualifies a response for storage in this content group.

alwaysEvalPolicies

Force policy evaluation for each response arriving from the origin server. Cannot be set to YES if the Prefetch parameter is also set to YES. Possible values: YES, NO
Default value: NO

persist

The option for IC objects to save objects to disk. Set YES for IC to take this state.
Possible values: YES, NO Default value: NO

pinned

The option for IC from flushing objects from this contentgroup under memory pressure. Set YES for IC to take this state. Possible values: YES, NO Default value: NO

lazyDnsResolve

Perform DNS resolution for responses only if the destination IP address in the request does not match the destination IP address of the cached response. Possible values: YES, NO Default value: YES

hitSelector

Selector for evaluating whether an object gets stored in a particular content group. A selector is an abstraction for a collection of PIXL expressions.

invalSelector

Selector for invalidating objects in the content group. A selector is an abstraction for a collection of PIXL expressions.

[Top](#)

unset cache contentGroup

Synopsis

```
unset cache contentGroup <name> [-weakPosRelExpiry] [-heurExpiryParam] [-relExpiry]
[-relExpiryMilliSec] [-absExpiry] [-absExpiryGMT] [-weakNegRelExpiry] [-hitParams] [-
invalParams] [-ignoreParamValueCase] [-matchCookies] [-invalRestrictedToHost] [-
pollEveryTime] [-ignoreReloadReq] [-removeCookies] [-prefetch] [-prefetchPeriod] [-
prefetchPeriodMilliSec] [-prefetchMaxPending] [-flashCache] [-expireAtLastByte] [-
insertVia] [-insertAge] [-insertETag] [-cacheControl] [-quickAbortSize] [-minResSize] [-
maxResSize] [-memLimit] [-ignoreReqCachingHdrs] [-minHits] [-alwaysEvalPolicies] [-
persist] [-pinned] [-lazyDnsResolve] [-hitSelector] [-invalSelector]
```

Description

Use this command to remove cache contentGroup settings. Refer to the set cache contentGroup command for meanings of the arguments.

[Top](#)

show cache contentGroup

Synopsis

```
show cache contentGroup [<name>]
```

Description

Displays information about all content groups, or about the specified content group.

Parameters

name

Name of the content group about which to display information.

[Top](#)

expire cache contentGroup

Synopsis

```
expire cache contentGroup <name>
```

Description

Forces expiration of all the objects in the specified content group. The next request for any object in the group is sent to the origin server.

Parameters

name

Name of the content group whose objects are to be expired.

[Top](#)

flush cache contentGroup

Synopsis

```
flush cache contentGroup <name> [-query <string> | -selectorValue <string>] [-host  
<string>] [-force]
```

Description

Flush the objects in the specified content group from memory and disk (if it has a disk copy).

Parameters

name

Name of the content group from which to flush objects, or "all" to flush all content groups.

query

Query string specifying individual objects to flush from this group by using parameterized invalidation. If this parameter is not set, all objects are flushed from the group.

host

Flush only objects that belong to the specified host. Do not use except with parameterized invalidation. Also, the Invalidation Restricted to Host parameter for the group must be set to YES.

selectorValue

Value of the selector to be used for flushing objects from the content group. Requires that an invalidation selector be configured for the content group.

force

Force all copies to be flushed including on disk.

[Top](#)

save cache contentGroup

Synopsis

save cache contentGroup <name>

Description

Save the objects in the specified content group.

Parameters

name

The name of the content group whose objects are to be save.

[Top](#)

cache forwardProxy

[[add](#) | [rm](#) | [show](#)]

add cache forwardProxy

Synopsis

add cache forwardProxy <IPAddress> <port>

Description

Allows the cache to act as a forward proxy for other NetScaler appliances or cache servers.

Parameters

IPAddress

IP address of the NetScaler appliance or a cache server for which the cache acts as a proxy. Requests coming to the NetScaler with the configured IP address are forwarded to the particular address, without involving the Integrated Cache in any way.

port

Port on the NetScaler appliance or a server for which the cache acts as a proxy
Minimum value: 1

[Top](#)

rm cache forwardProxy

Synopsis

rm cache forwardProxy <IPAddress> <port>

Description

Removes the forward proxy address from the Integrated Cache. The cache does not act as a proxy to the specified IP address.

Parameters

IPAddress

IP address of the NetScaler appliance or a server for which the cache was as a proxy.

port

Port on the NetScaler appliance or a server for which the cache acts as a proxy
Minimum value: 1

[Top](#)

show cache forwardProxy

Synopsis

show cache forwardProxy

Description

Displays the IP address and the corresponding ports for which the cache acted as a forward proxy.

[Top](#)

cache selector

[[add](#) | [rm](#) | [set](#) | [show](#)]

add cache selector

Synopsis

add cache selector <selectorName> <rule> ...

Description

Creates an Integrated Cache selector. A selector is an abstraction for a collection of PIXL expressions. After creating a selector, you can use it as a hit selector, invalidation selector, or both. You must specify at least one expression when you create a selector.

Parameters

selectorName

Name for the selector. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

rule

One or multiple PIXL expressions for evaluating an HTTP request or response.

[Top](#)

rm cache selector

Synopsis

rm cache selector <selectorName>

Description

Removes cache selectors. Note: A selector being used as a hit or invalidation selector in any content group cannot be removed without unsetting it from the content group.

Parameters

selectorName

Name of the selector.

[Top](#)

set cache selector

Synopsis

set cache selector <selectorName> <rule> ...

Description

Modify the set of PIXL expressions associated with a cache selector.

Parameters

selectorName

Name of the selector to be modified.

rule

One or multiple PIXL expressions for evaluating an HTTP request or response.

[Top](#)

show cache selector

Synopsis

show cache selector [<selectorName>]

Description

Displays all cache selectors, or the specified.

Parameters

selectorName

Name of the selector to display.

[Top](#)

cache object

[[show](#) | [expire](#) | [flush](#) | [save](#)]

show cache object

Synopsis

```
show cache object [(-url <URL> (-host <string> [-port <port>] [-groupName <string>] [-httpMethod ( GET | POST )])) | -locator <positive_integer> | -httpStatus <positive_integer> | -group <string> | -ignoreMarkerObjects ( ON | OFF ) | -includeNotReadyObjects ( ON | OFF )]
```

Description

Displays a list of all cached objects. The list displays the unique locator ID of each cached object along with the content group in which it was cached, and other details. To view more details of a specific cached object, use the -locator parameter along with this command.

Parameters

url

URL of the particular object whose details is required. Parameter "host" must be specified along with the URL.

locator

ID of the cached object.

httpStatus

HTTP status of the object.

host

Host name of the object. Parameter "url" must be specified.

port

Host port of the object. You must also set the Host parameter. Default value: 80
Minimum value: 1

groupName

Name of the content group to which the object belongs. It will display only the objects belonging to the specified content group. You must also set the Host parameter.

httpMethod

HTTP request method that caused the object to be stored. Possible values: GET, POST
Default value: NS_HTTP_METHOD_GET

group

Name of the content group whose objects should be listed.

ignoreMarkerObjects

Ignore marker objects. Marker objects are created when a response exceeds the maximum or minimum response size for the content group or has not yet received the minimum number of hits for the content group. Possible values: ON, OFF

includeNotReadyObjects

Include responses that have not yet reached a minimum number of hits before being cached. Possible values: ON, OFF

[Top](#)

expire cache object

Synopsis

expire cache object (-locator <positive_integer> | (-url <URL> (-host <string> [-port <port>] [-groupName <string>] [-httpMethod (GET | POST)])))

Description

Forces expiry of a cached object. You have to specify the locator ID of the cached object by using the -locator parameter.

Parameters

locator

ID of the cached object to be expired To view the locator ID of the cached objects, use the show cache object command.

url

The URL of the object to be expired.

host

The host of the object to be expired.

port

The host port of the object to be expired. Default value: 80 Minimum value: 1

groupName

Name of the content group to which the object belongs.

httpMethod

HTTP request method that caused the object to be stored. Possible values: GET, POST Default value: NS_HTTP_METHOD_GET

[Top](#)

flush cache object

Synopsis

flush cache object (-locator <positive_integer> | (-url <URL> (-host <string> [-port <port>] [-groupName <string>] [-httpMethod (GET | POST)]))) [-force]

Description

Removes a cached object from memory and from disk (if it has a disk copy). You have to specify the locator ID of the cached object by using the -locator parameter

Parameters

locator

ID of the cached object. To view the locator ID of the cached objects, use the show cache object command.

url

URL of the object to be flushed. You must also set the Host parameter.

host

Host of the object to be flushed. Must provide the "url" parameter along with the host.

port

Host port of the object to be flushed. Must provide the "host" parameter along with the port. Default value: 80 Minimum value: 1

groupName

Name of the content group to which the object belongs. Must provide the \"host\" parameter along with the group name.

httpMethod

HTTP request method that caused the object to be stored. All objects cached by that method will be flushed. Possible values: GET, POST Default value: NS_HTTP_METHOD_GET

force

Force all copies to be flushed including on disk.

[Top](#)

save cache object

Synopsis

save cache object [-locator <positive_integer>]

Description

Save a cached object to local disk.

Parameters**locator**

The ID of the cached object.

[Top](#)

cache stats

show cache stats

Synopsis

show cache stats - alias for 'stat cache'

Description

show cache stats is an alias for stat cache

cache global

[[bind](#) | [unbind](#) | [show](#)]

bind cache global

Synopsis

`bind cache global <policy> -priority <positive_integer> [-gotoPriorityExpression <expression>] [-type <type>] [-invoke (<labelType> <labelName>)]`

Description

Binds the cache policy to one of the two global bind points (an unnamed policy label invoked at request time and an unnamed policy label invoked at the response time). The flow type of the policy implicitly determines which label it gets bound to. A policy becomes active only when it is bound. A globally bound policy, it is available to all virtual servers on the NetScaler appliance. All HTTP traffic is evaluated against the global policy labels. Each label contains an ordered list ordered by policies' priority values.

Parameters

policy

Name of the policy to bind. (A policy must be created before it can be bound.)

[Top](#)

unbind cache global

Synopsis

`unbind cache global <policy> [-type <type>] [-priority <positive_integer>]`

Description

Deactivate the policy by unbinding it from a global bind point.

Parameters

policy

Name of the policy to unbind.

priority

Priority of the NOPOLICY to be unbound. Required only you want to unbind a NOPOLICY that might have been bound to this policy label. Minimum value: 1
Maximum value: 2147483647

[Top](#)

show cache global

Synopsis

`show cache global [-type <type>]`

Description

Displays the global bindings for cache policies.

Parameters

type

The bind point to which policy is bound. When you specify the type, detailed information about that bind point appears. Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT

Example

```
show cache global
```

[Top](#)

cache parameter

[[set](#) | [unset](#) | [show](#)]

set cache parameter

Synopsis

```
set cache parameter [-memLimit <MBytes>] [-via <string>] [-verifyUsing <verifyUsing>]
[-maxPostLen <positive_integer>] [-prefetchMaxPending <positive_integer>] [-
enableBypass ( YES | NO )] [-undefAction ( NOCACHE | RESET )] [-enableDiskCache
( YES | NO )]
```

Description

Modifies the global configuration of the integrated cache. You can modify the settings of various parameters.

Parameters

memLimit

Amount of memory available for storing the cache objects. In practice, the amount of memory available for caching can be less than half the total memory of the NetScaler appliance.

via

String to include in the Via header. A Via header is inserted into all responses served from a content group if its Insert Via flag is set.

verifyUsing

Criteria for deciding whether a cached object can be served for an incoming HTTP request. Available settings function as follows: HOSTNAME - The URL, host name, and host port values in the incoming HTTP request header must match the cache policy. The IP address and the TCP port of the destination host are not evaluated. Do not use the HOSTNAME setting unless you are certain that no rogue client can access a rogue server through the cache. HOSTNAME_AND_IP - The URL, host name, host port in the incoming HTTP request header, and the IP address and TCP port of the destination server, must match the cache policy. DNS - The URL, host name and host port in the incoming HTTP request, and the TCP port must match the cache policy. The host name is used for DNS lookup of the destination server's IP address, and is

compared with the set of addresses returned by the DNS lookup. Possible values: HOSTNAME, HOSTNAME_AND_IP, DNS

maxPostLen

Maximum number of POST body bytes to consider when evaluating parameters for a content group for which you have configured hit parameters and invalidation parameters. Default value: 4096 Maximum value: 131072

prefetchMaxPending

Maximum number of outstanding prefetches in the Integrated Cache.

enableBypass

Evaluate the request-time policies before attempting hit selection. If set to NO, an incoming request for which a matching object is found in cache storage results in a response regardless of the policy configuration. If the request matches a policy with a NOCACHE action, the request bypasses all cache processing. This parameter does not affect processing of requests that match any invalidation policy. Possible values: YES, NO

undefAction

Action to take when a policy cannot be evaluated. Possible values: NOCACHE, RESET

enableDiskCache

The disk cache parameter. When this value is set to YES, cache objects can be saved on disk. If set to NO, objects will never be stored in disk. Possible values: YES, NO
Default value: NO

[Top](#)

unset cache parameter

Synopsis

```
unset cache parameter [-memLimit] [-via] [-verifyUsing] [-maxPostLen] [-prefetchMaxPending] [-enableBypass] [-undefAction] [-enableDiskCache]
```

Description

Use this command to remove cache parameter settings. Refer to the set cache parameter command for meanings of the arguments.

[Top](#)

show cache parameter

Synopsis

```
show cache parameter
```

Description

Displays the global configuration of the Integrated Cache.

[Top](#)

CLI Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [config](#)
- ♦ [whoami](#)
- ♦ [exit](#)
- ♦ [quit](#)
- ♦ [man](#)
- ♦ [history](#)
- ♦ [help](#)
- ♦ [source](#)
- ♦ [batch](#)
- ♦ [backup](#)
- ♦ [unalias](#)
- ♦ [alias](#)
- ♦ [cls](#)
- ♦ [cli attribute](#)
- ♦ [cli prompt](#)
- ♦ [cli mode](#)

config

config

Synopsis

config

Description

Enter this command to enter contextual mode.

whoami

whoami

Synopsis

whoami

Description

Show the current user.

exit

exit

Synopsis

exit

Description

Use this command to back out one level in config mode, or to terminate the CLI when not in config mode.);

quit

quit

Synopsis

quit

Description

Use this command to terminate the CLI. Note: typing <Ctrl>+<d> will also terminate the CLI.

man

man

Synopsis

man [(commandName)]

Description

Use this command to invoke the man page for the specified command. You can specify the command in full, or partially, if it is uniquely resolvable.

Parameters

commandName

The name of the command.

Example

```
man add vs
```

history

history

Synopsis

history

Description

Use this command to see the history of the commands executed on CLI.

Example

```
history
SPECIFIC 10.102.130.228
1 add snmp trap
2 save config
3 show system session
4 shell
5 shell
6 what
7 shell
8 help stat lbvserver
...
```

help

help

Synopsis

help [(commandName) | <groupName> | -all]

Description

Use this command to display help information for a CLI command, for a group of commands, or for all CLI commands.

Parameters

commandName

The name of a command for which you want full usage information.

groupName

The name of a command group for which you want basic usage information.

all

Use this option to request basic usage information for all commands.

Example

```

1.To view help information for adding a virtual
server, enter the following CLI command:
help add vserver
The following information is displayed:
Usage:  add vserver <vServerName> <serviceType>
[<IPAddress> port] [-type ( CONTENT | ADDRESS )]
[-cacheType <cacheType>] [-backupVServerName
<string>] [-redirectURL <URL>] [-cacheable ( ON |
OFF )] [-state ( ENABLED | DISABLED )]

where:
serviceType = ( HTTP | FTP | TCP | UDP | SSL |
SSL_BRIDGE | SSL_TCP | NNTP | DNS | ANY )
<cacheType> = ( TRANSPARENT | REVERSE | FORWARD )
Done
2.To view help information for all DNS commands,
enter the following command:
help dns
The following information is displayed:
add aaaaRec <hostname> <IPv6Address> ... [-TTL
<secs>]
rm aaaaRec <hostname> [<IPv6Address> ...]
show aaaaRec [<hostname> | -type <type>]
add addRec <hostname> <IPAddress> ... [-TTL
<secs>] [-private <ip_addr>]
rm addRec <hostname> [<IPAddress> ...]
show addRec [<hostname> | -type <type>]
add cnameRec <aliasName> <canonicalName> [-TTL
<secs>]
rm cnameRec <aliasName>
show cnameRec [<aliasName> | -type <type>]
add mxRec <domain> -mx <string> -pref
<positive_integer> [-TTL <secs>]
rm mxRec <domain> <mx>
set mxRec <domain> -mx <string> [-pref
<positive_integer>] [-TTL <secs>]
show mxRec [<domain> | -type <type>]
add nsRec <domain> [-p <string>] [-s <string>] [-
TTL <secs>]
rm nsRec <domain> [-p <string> | -s <string>]
show nsRec [<domain> | -type <type>]
set dns parameter [-timeout <secs>] [-retries
<positive_integer>] [-minTTL <secs>] [-maxTTL
<secs>] [-TTL ( ENABLED | DISABLED )] [-
cacheRecords ( YES | NO )]
show dns parameter
add soaRec <domain> -contact <string> -serial
<positive_integer> -refresh <secs> -retry <secs> -
expire <secs> -minimum <secs> -TTL <secs>
rm soaRec <domain>
set soaRec <domain> [-contact <string>] [-serial
<positive_integer>] [-refresh <secs>] [-retry
<secs>] [-expire <secs>] [-minimum <secs>] [-TTL
<secs>]

```



```

show soaRec [<domain> | -type <type>]
add dns ptrRec <reverseDomain> <domain> ... [-TTL
<secs>]
rm dns ptrRec <reverseDomain> [<domain> ...]
show dns ptrRec [<reverseDomain> | -type <type>]
add dns srvRec <domain> <target> -priority
<positive_integer>
    -weight <positive_integer> -port
<positive_integer>
rm dns srvRec <domain> [<target> ...]
set dns srvRec <domain> <target> [-priority
<positive_integer>]
    [-weight <positive_integer>] [-port
<positive_integer>] [-TTL <secs>]
show dns srvRec [(<domain> [<target>]) | -type
<type>]
Done

```

source

source

Synopsis

source <fileName>

Description

Use this command to read the contents of a file and execute each line as a separate CLI command. Each command in the file being read must be on a separate line. Lines starting with # are considered comments.

Parameters

fileName

The name of the file to be sourced.

Example

```
source cmds.txt
```

batch

batch

Synopsis

batch -fileName <input_filename> [-outfile <output_filename>] [-ntimes
<positive_integer>]

Description

Use this command to read the contents of a file and execute each line as a separate CLI command. Each command in the file must be on a separate line. Lines starting with # are considered comments.

Parameters

fileName

The name of the batch file.

outfile

The name of the file where the executed batch file will write its output. The default is standard output.

ntimes

The number of times the batch file will be executed. Default value: 1

Example

```
batch -f cmds.txt
```

backup

backup

Synopsis

```
backup -pattern <string>
```

Description

backup cache object to local disk

Parameters

pattern

Name of the alias

Example

```
backup cache object -locator <id>
```

unalias

unalias

Synopsis

```
unalias <pattern>
```

Description

Remove an alias

Parameters

pattern

Name of the alias

Example

```
unalias info
```

alias

alias

Synopsis

alias [<pattern> [(command)]]

Description

Create (short) aliases for (long) commands. Aliases are saved across NSCLI sessions. If no argument is specified, the alias command will display existing aliases.

Parameters

pattern

Alias name. (Can be a regular expression.)

Example

```
alias info "show ns info"
```

cls

cls

Synopsis

cls

Description

Clear the screen and reposition cursor at top right.

cli attribute

show cli attribute

Synopsis

show cli attribute

Description

Display attributes of the NetScaler CLI

cli prompt

[[clear](#) | [set](#) | [show](#)]

clear cli prompt

Synopsis

clear cli prompt

Description

Use this command to return the CLI prompt to the default (a single '>').

[Top](#)

set cli prompt

Synopsis

set cli prompt <promptString>

Description

Use this command to customize the CLI prompt.

Parameters

promptString

The prompt string. The following special values are allowed: %! - will be replaced by the history event number %u - will be replaced by the NetScaler user name %h - will be replaced by the NetScaler hostname %t - will be replaced by the current time %T - will be replaced by the current time (24 hr format) %d - will be replaced by the current date %s - will be replaced by the node state

Example

```
> set cli prompt "%h %T"
Done
lb-ns1 15:16>
```

[Top](#)

show cli prompt

Synopsis

show cli prompt

Description

Use this command to display the current CLI prompt, with special values like '%h' unexpanded.

Example

```
10.101.4.22 15:20> sh cli prompt
      CLI prompt is set to "%h %T"
Done
```

[Top](#)

cli mode

[[set](#) | [unset](#) | [show](#)]

set cli mode

Synopsis

set cli mode [-page (ON | OFF)] [-total (ON | OFF)] [-color (ON | OFF)] [-disabledFeatureAction <disabledFeatureAction>] [-timeout <secs>] [-regex (ON | OFF)]

Description

Use this command to specify how the CLI should display command output.

Parameters

page

Determines whether output that spans more than one screen is "paged". Specify ON to pause the display after each screen of output. Possible values: ON, OFF Default value: OFF

total

Determines whether CLI "show" commands display a total count of objects before displaying the objects themselves. Possible values: ON, OFF Default value: OFF

color

Specifies whether output can be shown in color, if the terminal supports it. Possible values: ON, OFF Default value: OFF

disabledFeatureAction

Specifies what will happen when a configuration command is issued for a disabled feature. The following values are allowed: NONE - The action is allowed, and no warning message is issued.; ALLOW - The action is allowed, but a warning message is issued.; DENY - The action is not allowed.; HIDE - Commands that configure disabled

features are hidden, and the CLI behaves as if they did not exist. Possible values: NONE, ALLOW, DENY, HIDE Default value: NS_ALLOW

timeout

CLI session inactivity timeout, in seconds. Timeout cannot have values in between 1 and 9. Default value: 300 Maximum value: 100000000

regex

If ON, regular expressions can be used as argument values Possible values: ON, OFF Default value: ON

[Top](#)

unset cli mode

Synopsis

unset cli mode [-page] [-total] [-color] [-disabledFeatureAction] [-timeout] [-regex]

Description

Use this command to remove cli mode settings. Refer to the set cli mode command for meanings of the arguments.

[Top](#)

show cli mode

Synopsis

show cli mode

Description

Use this command to display the current settings of parameters that can be set with the 'set cli mode' command.

[Top](#)

Cluster Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [cluster](#)
- ♦ [cluster instance](#)
- ♦ [cluster node](#)
- ♦ [cluster nodegroup](#)
- ♦ [cluster files](#)
- ♦ [cluster sync](#)

cluster

join cluster

Synopsis

```
join cluster -clip <ip_addr> {-password }
```

Description

Joins the appliance to the cluster. You must execute this command from the NetScaler IP (NSIP) address of the node that you want to add to the cluster. This command is the second part of the two-step process of adding a cluster node. The first part is adding this node to the cluster by using the add cluster node command from the cluster IP address. This operation is not permitted if any node in the cluster is in the Sync state.

Parameters

clip

Cluster IP address to which to add the node.

password

Password for the nsroot account of the configuration coordinator (CCO).

cluster instance

[[add](#) | [rm](#) | [set](#) | [unset](#) | [enable](#) | [disable](#) | [show](#) | [stat](#)]

add cluster instance

Synopsis

```
add cluster instance <cld> [-deadInterval <secs>] [-helloInterval <msecs>] [-preemption ( ENABLED | DISABLED )]
```

Description

Adds a cluster instance to the appliance. Execute this command on only the first node that you add to the cluster.

Parameters

cld

Unique number that identifies the cluster. Minimum value: 1 Maximum value: 16

deadInterval

Amount of time, in seconds, after which nodes that do not respond to the heartbeats are assumed to be down. Default value: 3 Minimum value: 3 Maximum value: 60

helloInterval

Interval, in milliseconds, at which heartbeats are sent to each cluster node to check the health status. Default value: 200 Minimum value: 200 Maximum value: 1000

preemption

Preempt a cluster node that is configured as a SPARE if an ACTIVE node becomes available. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

```
add cluster instance 1
```

[Top](#)

rm cluster instance

Synopsis

rm cluster instance <cld>

Description

Removes the cluster instance from the node. You must execute this command on the NetScaler IP (NSIP) address of the node.

Parameters

cld

Unique number that identifies the cluster. Minimum value: 1 Maximum value: 16

Example

```
rm cluster instance 1
```

[Top](#)

set cluster instance

Synopsis

set cluster instance <cld> [-deadInterval <secs>] [-helloInterval <msecs>] [-preemption (ENABLED | DISABLED)]

Description

Modifies the specified attributes of a cluster instance.

Parameters

cld

ID of the cluster instance to be modified. Minimum value: 1 Maximum value: 16

deadInterval

Amount of time, in seconds, after which nodes that do not respond to the heartbeats are assumed to be down. Default value: 3 Minimum value: 3 Maximum value: 60

helloInterval

Interval, in milliseconds, at which heartbeats are sent to each cluster node to check the health status. Default value: 200 Minimum value: 200 Maximum value: 1000

preemption

Preempt a cluster node that is configured as a SPARE if an ACTIVE node becomes available. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

```
set cluster instance 1 -preemption ENABLED
```

[Top](#)**unset cluster instance****Synopsis**

```
unset cluster instance <clld> [-deadInterval] [-helloInterval] [-preemption]
```

Description

Use this command to remove cluster instance settings. Refer to the set cluster instance command for meanings of the arguments.

[Top](#)**enable cluster instance****Synopsis**

```
enable cluster instance <clld>
```

Description

Enables a cluster instance.

Parameters

clld

ID of the cluster instance that you want to enable. Minimum value: 1 Maximum value: 16

Example

```
enable cluster instance 1
```

[Top](#)**disable cluster instance****Synopsis**

```
disable cluster instance <clld>
```

Description

Disables a cluster instance.

Parameters

clld

ID of the cluster instance that you want to disable. Minimum value: 1 Maximum value: 16

Example

```
disable cluster instance 1
```

[Top](#)

show cluster instance

Synopsis

show cluster instance [<clld>]

Description

Displays information about the cluster instance and its nodes.

Parameters

clld

Unique number that identifies the cluster. Minimum value: 1 Maximum value: 16

Example

An example of the command's output is as follows:

```
1)Cluster ID: 1
    Dead Interval: 3 secs
    Hello Interval: 200 msec
    Preemption: DISABLED
    Propagation: ENABLED
    Cluster Status: ENABLED(admin),
ENABLED(operational), UP
    Member Nodes:
    Node ID      Node IP
Health  Admin State  Operational State
-----
1)      1           1.1.1.1*
UP      ACTIVE      ACTIVE (Configuration
Coordinator)
2)      2           1.1.1.2
UP      ACTIVE      ACTIVE
Done
*: Local node
```

[Top](#)

stat cluster instance

Synopsis

```
stat cluster instance [<clld>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-clearstats ( basic | full )]
```

Description

Displays statistics for a cluster instance.

Parameters

clld

ID of the cluster instance for which to display statistics. Minimum value: 1 Maximum value: 16

clearstats

Clear the statistics / counters Possible values: basic, full

[Top](#)

cluster node

[[add](#) | [set](#) | [unset](#) | [rm](#) | [show](#) | [stat](#)]

add cluster node

Synopsis

```
add cluster node <nodeId>@ <IPAddress>@ [-state <state>] [-backplane <interface_name>@] [-priority <positive_integer>]
```

Description

Adds a NetScaler appliance to a cluster.

Parameters

nodeId

Unique number that identifies the cluster node. Maximum value: 31

IPAddress

NetScaler IP (NSIP) address of the appliance to add to the cluster. Must be an IPv4 address.

state

Admin state of the cluster node. The available settings function as follows: ACTIVE - The node serves traffic. SPARE - The node does not serve traffic unless an ACTIVE node goes down. PASSIVE - The node does not serve traffic, unless you change its state. PASSIVE state is useful during temporary maintenance activities in which you want the node to take part in the consensus protocol but not to serve traffic. Possible values: ACTIVE, SPARE, PASSIVE Default value: NSACL_NODEEST_PASSIVE

backplane

Interface through which the node communicates with the other nodes in the cluster. Must be specified in the three-tuple form n/c/u, where n represents the node ID and c/u refers to the interface on the appliance. Minimum value: 1

priority

Preference for selecting a node as the configuration coordinator. The node with the lowest priority value is selected as the configuration coordinator. When the current configuration coordinator goes down, the node with the next lowest priority is made the new configuration coordinator. When the original node comes back up, it will preempt the new configuration coordinator and take over as the configuration coordinator. Note: When priority is not configured for any of the nodes or if multiple nodes have the same priority, the cluster elects one of the nodes as the configuration coordinator. Default value: 31 Maximum value: 31

Example

```
add cluster node 1 1.1.1.1 -backplane 1/1/1 -state
ACTIVE
```

[Top](#)

set cluster node

Synopsis

```
set cluster node <nodeld>@ [-state <state>] [-backplane <interface_name>@] [-priority
<positive_integer>]
```

Description

Modifies the attributes of a cluster node.

Parameters

nodeld

ID of the cluster node to be modified. Maximum value: 31

state

Admin state of the cluster node. The available settings function as follows: ACTIVE - The node serves traffic. SPARE - The node does not serve traffic unless an ACTIVE node goes down. PASSIVE - The node does not serve traffic, unless you change its state. PASSIVE state is useful during temporary maintenance activities in which you want the node to take part in the consensus protocol but not to serve traffic. Possible values: ACTIVE, SPARE, PASSIVE Default value: NSACL_NODEST_PASSIVE

backplane

Interface through which the node communicates with the other nodes in the cluster. Must be specified in the three-tuple form n/c/u, where n represents the node ID and c/u refers to the interface on the appliance. Minimum value: 1

priority

Preference for selecting a node as the configuration coordinator. The node with the lowest priority value is selected as the configuration coordinator. When the current

configuration coordinator goes down, the node with the next lowest priority is made the new configuration coordinator. When the original node comes back up, it will preempt the new configuration coordinator and take over as the configuration coordinator. Note: When priority is not configured for any of the nodes or if multiple nodes have the same priority, the cluster elects one of the nodes as the configuration coordinator. Default value: 31 Maximum value: 31

Example

```
set cluster node 1 -state PASSIVE
```

[Top](#)**unset cluster node****Synopsis**

```
unset cluster node <nodeld>@ [-state] [-backplane] [-priority]
```

Description

Use this command to remove cluster node settings. Refer to the set cluster node command for meanings of the arguments.

[Top](#)**rm cluster node****Synopsis**

```
rm cluster node <nodeld>
```

Description

Removes a node from the cluster and removes the cluster instance from the node. You must execute this command on the cluster IP address.

Parameters**nodeld**

ID of the cluster node to be removed from the cluster. Maximum value: 31

Example

```
rm cluster node 1
```

[Top](#)**show cluster node****Synopsis**

```
show cluster node [<nodeld>@]
```

Description

Displays information about the cluster node.

Parameters

nodeId

ID of the cluster node for which to display information. If an ID is not provided, information about all nodes is shown. Default value: 255 Maximum value: 31

Example

```
An example of the command's output is as follows:
  1 cluster node:
1)Node ID: 1
    IP: 1.1.1.1*
    Backplane: 1/1/1
    Health: UP
    Admin State: ACTIVE
    Operational State: ACTIVE (Configuration
Coordinator)
    Sync State: DISABLED
Done
*: Local node
```

[Top](#)

stat cluster node

Synopsis

```
stat cluster node [<nodeId>@] [-detail] [-fullValues] [-ntimes <positive_integer>] [-
logFile <input_filename>] [-clearstats ( basic | full )]
```

Description

Displays statistics for a cluster node.

Parameters

nodeId

ID of the cluster node for which to display statistics. If an ID is not provided, statistics are shown for all nodes. Maximum value: 31

clearstats

Clear the statistics / counters Possible values: basic, full

[Top](#)

cluster nodegroup

[[add](#) | [show](#) | [set](#) | [unset](#) | [bind](#) | [unbind](#) | [rm](#)]

add cluster nodegroup

Synopsis

add cluster nodegroup <name>@ [-strict (YES | NO)]

Description

Adds a nodegroup to the cluster. A nodegroup is a set of cluster nodes to which entities can be bound. Entities that are bound to a specific nodegroup are active on all the nodes of the group and not active on the nodes that are not part of the group.

Parameters

name

Name of the nodegroup. The name uniquely identifies the nodegroup on the cluster.

strict

Specifies whether cluster nodes, that are not part of the nodegroup, will be used as backup for the nodegroup. * Enabled - When one of the nodes goes down, no other cluster node is picked up to replace it. When the node comes up, it will continue being part of the nodegroup. * Disabled - When one of the nodes goes down, a non-nodegroup cluster node is picked up and acts as part of the nodegroup. When the original node of the nodegroup comes up, the backup node will be replaced. Possible values: YES, NO Default value: NO

Example

```
add cluster nodegroup ng1 -strict yes
```

[Top](#)

show cluster nodegroup

Synopsis

show cluster nodegroup [<name>]

Description

Displays information about the available nodegroups.

Parameters

name

Name of the nodegroup to be displayed. If a name is not provided, information about all nodegroups is displayed.

[Top](#)

set cluster nodegroup

Synopsis

set cluster nodegroup <name>@ [-strict (YES | NO)]

Description

Modifies the attributes of a cluster nodegroup.

Parameters

name

Name of the nodegroup to be modified.

strict

Specifies whether cluster nodes, that are not part of the nodegroup, will be used as backup for the nodegroup. * Enabled - When one of the nodes goes down, no other cluster node is picked up to replace it. When the node comes up, it will continue being part of the nodegroup. * Disabled - When one of the nodes goes down, a non-nodegroup cluster node is picked up and acts as part of the nodegroup. When the original node of the nodegroup comes up, the backup node will be replaced. Possible values: YES, NO Default value: NO

Example

```
set cluster nodegroup ng1 -strict yes
```

[Top](#)

unset cluster nodegroup

Synopsis

```
unset cluster nodegroup <name>@ [-strict]
```

Description

Unset nodes from the given nodegroup or unset strict option. Refer to the set cluster nodegroup command for meanings of the arguments.

Example

```
unset cluster nodegroup ng1 -strict
```

[Top](#)

bind cluster nodegroup

Synopsis

```
bind cluster nodegroup <name> (-node <positive_integer>@ | -vServer <string> | -  
identifierName <string>)
```

Description

Binds a cluster node or an entity to the given nodegroup. A node can be bound to more than one nodegroup.

Parameters

name

Name of the nodegroup to which you want to bind a cluster node or an entity.

node

ID of the node to be bound to the nodegroup. Maximum value: 31

vServer

Name of the virtual server to be bound to the nodegroup.

identifierName

Name of stream or limit identifier to be bound to the nodegroup.

Example

```
bind cluster nodegroup ng1 -vserver v1
```

[Top](#)

unbind cluster nodegroup

Synopsis

unbind cluster nodegroup <name> (-node <positive_integer>@ | -vServer <string> | -identifierName <string>)

Description

Unbinds a cluster node or an entity from a given nodegroup.

Parameters

name

Name of the nodegroup from which you want to unbind a cluster node or an entity.

node

ID of the node to be unbound from the nodegroup. Maximum value: 31

vServer

Name of the virtual server to be unbound from the nodegroup.

identifierName

Name of stream or limit identifier to be unbound from the nodegroup.

Example

```
unbind cluster nodegroup ng1 -vserver v1
```

[Top](#)

rm cluster nodegroup

Synopsis

rm cluster nodegroup <name>@

Description

Removes a nodegroup from the cluster.

Parameters

name

Name of the nodegroup to be removed.

Example

```
rm cluster nodegroup ng1
```

[Top](#)

cluster files

sync cluster files

Synopsis

sync cluster files [<Mode> ...]

Description

Synchronizes SSL Certificates, SSL CRL lists, SSL VPN bookmarks, and other files from the configuration coordinator (CCO) to the other cluster nodes. Execute this command from the cluster IP address only. This command is automatically triggered from the CCO when a new node is added to a cluster and periodically triggered to synchronize updated files between the cluster nodes. Note: Files on non-CCO nodes are not deleted if they do not exist on the CCO.

Parameters

Mode

The directories and files to be synchronized. The available settings function as follows: Mode Paths all /nsconfig/ssl/ /var/netScaler/ssl/ /var/vpn/bookmark/ /nsconfig/dns/ /nsconfig/htmlinjection/ /netScaler/htmlinjection/ens/ /nsconfig/monitors/ /nsconfig/nstemplates/ /nsconfig/ssh/ /nsconfig/rc.netScaler /nsconfig/resolv.conf /nsconfig/inetd.conf /nsconfig/syslog.conf /nsconfig/snmpd.conf /nsconfig/ntp.conf /nsconfig/httpd.conf /nsconfig/sshd_config /nsconfig/hosts /nsconfig/enckey /var/nslw.bin/etc/krb5.conf /var/nslw.bin/etc/krb5.keytab /var/lib/likewise/db/ /var/download/ /var/wi/tomcat/webapps/ /var/wi/tomcat/conf/Catalina/localhost/ /var/wi/java_home/lib/security/cacerts /var/wi/java_home/jre/lib/security/cacerts ssl /nsconfig/ssl/ /var/netScaler/ssl/ bookmarks /var/vpn/bookmark/ dns /nsconfig/dns/htmlinjection /nsconfig/htmlinjection/ imports /var/download/ misc /nsconfig/

license/ /nsconfig/rc.conf all_plus_misc Includes *all* files and /nsconfig/license/ and /nsconfig/rc.conf. Default value: all

Example

```
sync cluster files ssl or sync cluster files all
```

cluster sync

force cluster sync

Synopsis

force cluster sync

Description

Synchronize the configurations of a cluster node from the configuration coordinator (CCO). This command must be executed from the NSIP of the node that is to be synchronized.

Example

```
force cluster sync
```

Compression Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [cmp](#)
- ♦ [cmp action](#)
- ♦ [cmp policy](#)
- ♦ [cmp policylabel](#)
- ♦ [cmp stats](#)
- ♦ [cmp global](#)
- ♦ [cmp parameter](#)

cmp

stat cmp

Synopsis

```
stat cmp [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]
[-clearstats ( basic | full )]
```

Description

Display compression statistics.

Parameters

clearstats

Clear the statistics / counters Possible values: basic, full

cmp action

[[add](#) | [rm](#) | [show](#) | [rename](#)]

add cmp action

Synopsis

```
add cmp action <name> <cmpType>
```

Description

Creates a compression action. Note: User-defined compression actions supplement the built-in compression actions. The built-in compression actions, NOCOMPRESS, COMPRESS, GZIP, and DEFLATE, are always available. Available settings functions as follows: * NOCOMPRESS - Disables compression for data that matches the associated policy. * COMPRESS - Enable GZIP or DEFLATE compression, depending on which is supported by the browser. * GZIP - Enable GZIP compression. For browsers that do not support GZIP, compression is disabled. * DEFLATE - Enable DEFLATE compression for a specific policy. For browsers that do not support DEFLATE, compression is disabled.

Parameters

name

Name of the compression action. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the action is added. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cmp action" or 'my cmp action').

cmpType

Type of compression performed by this action. Available settings function as follows: * COMPRESS - Apply GZIP or DEFLATE compression to the response, depending on the request header. Prefer GZIP. * GZIP - Apply GZIP compression. * DEFLATE - Apply DEFLATE compression. * NOCOMPRESS - Do not compress the response if the request matches a policy that uses this action. Possible values: compress, gzip, deflate, nocompress

deltaType

The type of delta action (if delta type compression action is defined). Possible values: PERURL, PERPOLICY Default value: NS_ACT_CMP_DELTA_TYPE_PERURL

Example

```
add cmp action nocmp NOCOMPRESS
```

[Top](#)**rm cmp action****Synopsis**

```
rm cmp action <name>
```

Description

Removes the specified compression action.

Parameters**name**

Name of the action to be removed.

Example

```
rm cmp action cmp_action_name
```

[Top](#)**show cmp action****Synopsis**

```
show cmp action [<name>]
```

Description

Displays information about all the built-in and user-defined compression actions, or detailed information about the specified action.

Parameters**name**

Name of the action for which to display detailed information.

Example

Example 1

The following example shows output from the show

```
cmp action command when no custom cmp actions have
been defined:
```

```
> show cmp action
      3 Compression actions:
1)      Name: GZIP      Compression Type: gzip
2)      Name: NOCOMPRESS      Compression Type:
nocompress
3)      Name: DEFLATE   Compression Type: deflate
4)      Name: COMPRESS  Compression Type: compress
Done
```

Done

Example 2

The following command creates a compression action:

```
add cmp action nocmp NOCOMPRESS
```

The following example shows output from the show cmp action command after the previous command has been issued:

```
> show cmp action
      3 Compression actions:
1)      Name: GZIP      Compression Type: gzip
2)      Name: NOCOMPRESS      Compression Type:
nocompress
3)      Name: DEFLATE   Compression Type: deflate
4)      Name: COMPRESS  Compression Type: compress
```

```
      1 Compression action:
1)      Name: nocmp      Compression Type:
nocompress
Done
```

[Top](#)

rename cmp action

Synopsis

```
rename cmp action <name>@ <newName>@
```

Description

Renames a compression action.

Parameters

name

Existing name of the action.

newName

New name for the compression action. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Choose a name that can be correlated with the function that the action performs. The following requirement applies only to the NetScaler CLI: If the name includes

one or more spaces, enclose the name in double or single quotation marks (for example, "my cmp action" or 'my cmp action').

Example

```
rename cmp policy oldname newname
```

[Top](#)

cmp policy

[[add](#) | [rm](#) | [set](#) | [show](#) | [stat](#) | [rename](#)]

add cmp policy

Synopsis

```
add cmp policy <name> -rule <expression> -resAction <string>
```

Description

Creates a classic or default syntax HTTP compression policy. When the policy matches an HTTP request or response, the action specified in the policy is performed on the transaction. The policy can be bound globally or to an entity. For the policy to have an effect, compression must be enabled on the service.

Parameters

name

Name of the HTTP compression policy. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the policy is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cmp policy" or 'my cmp policy').

rule

Expression that determines which HTTP requests or responses match the compression policy. Can be a classic expression or a default-syntax expression. Note: Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>". The following requirements apply only to the NetScaler CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

resAction

The built-in or user-defined compression action to apply to the response when the policy matches a request or response.

Example

Example 1:

```
add cmp policy pdf_cmp -rule "RES.HTTP.HEADER
Content-Type CONTAINS application/pdf" -resAction
COMPRESS
```

After creating the above compression policy, you must activate it by binding it globally:

```
bind cmp global pdf_cmp
```

The NetScaler system will use the configured pdf_cmp compression policy to perform compression of pdf files.

Example 2:

The following command disables compression for all the access from the specific subnet.

```
add cmp policy local_sub_nocmp -rule "SOURCEIP ==
10.1.1.0 -netmask 255.255.255.0" -resAction
NOCOMPRESS
bind cmp global local_sub_nocmp
```

[Top](#)

rm cmp policy

Synopsis

rm cmp policy <name>

Description

Removes a user-defined HTTP compression policy.

Parameters

name

Name of the HTTP compression policy to be removed.

Example

```
rm cmp policy cmp_policy_name
The "show cmp policy" command shows all currently
defined HTTP compression policies.
```

[Top](#)

set cmp policy

Synopsis

```
set cmp policy <name> [-rule <expression>] [-resAction <string>]
```

Description

Modifies the specified parameters of an HTTP compression policy. Note: Use the show cmp policy command to view all configured HTTP compression policies.

Parameters

name

Name of the HTTP compression policy to be modified.

rule

New rule to be associated with the HTTP compression policy. You can modify the existing rule or create a new rule.

resAction

The built-in or user-defined compression action to be associated with the policy.

Example

Example 1:

```
add cmp policy pdf_cmp -rule "RES.HTTP.HEADER
Content-Type CONTAINS application/pdf" -resAction
COMPRESS
```

After creating the above compression policy, you must activate it by binding it globally:

```
bind cmp global pdf_cmp
```

The NetScaler system will use the configured pdf_cmp compression policy to perform compression for pdf files.

To disable pdf compression for Internet Explorer, you can change the above compression policy by issuing the following command:

```
set cmp policy pdf_cmp -rule "RES.HTTP.HEADER
Content-Type CONTAINS application/pdf &&
RES.HTTP.HEADER User-Agent NOTCONTAINS MSIE"
```

To view the changed cmp policy, enter the following command:

```
>show cmp policy pdf_cmp
      Name: pdf_cmp      Rule: (RES.HTTP.HEADER
Content-Type CONTAINS application/pdf &&
REQ.HTTP.HEADER User-Agent NOTCONTAINS MSIE)
      Response action: COMPRESS      Hits: 2
      Bytes In:...609284      Bytes Out:...
```

```

443998      Bandwidth saving...27.13%      Ratio
1.37:1
Done

```

[Top](#)

show cmp policy

Synopsis

show cmp policy [<name>] show cmp policy stats - alias for 'stat cmp policy'

Description

Displays details of all HTTP compression policies.

Parameters

name

Name of the HTTP compression policy for which to display details.

Example

```

> show cmp policy
  4 Compression policies:
1)      Name: ns_cmp_content_type      Rule:
ns_content_type
      Response action: COMPRESS      Hits: 1
      Bytes In:...4325      Bytes Out:... 1530
      Bandwidth saving...64.62%      Ratio
2.83:1
2)      Name: ns_cmp_msapp      Rule: (ns_msie &&
ns_msword || (ns_msexcel || ns_msppt))
      Response action: COMPRESS      Hits: 7
      Bytes In:...796160      Bytes Out:...
197730
      Bandwidth saving...75.16%      Ratio
4.03:1
3)      Name: ns_cmp_mscss      Rule: (ns_msie &&
ns_css)
      Response action: COMPRESS      Hits: 0
4)      Name: ns_nocmp_mozilla_47      Rule:
(ns_mozilla_47 && ns_css)
      Response action: NOCOMPRESS      Hits: 0
Done

You can also view an individual cmp policy by
giving the cmp policy name as an argument:
> show cmp policy ns_cmp_msapp
      Name: ns_cmp_msapp      Rule: (ns_msie &&
ns_msword || (ns_msexcel || ns_msppt))
      Response action: COMPRESS      Hits: 7
      Bytes In:...796160      Bytes Out:...
197730
      Bandwidth saving...75.16%      Ratio

```

```
4.03:1
Done
```

[Top](#)

stat cmp policy

Synopsis

```
stat cmp policy [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile
<input_filename>] [-clearstats ( basic | full )]
```

Description

Displays compression statistics for all advanced compression policies, or for only the specified policy.

Parameters

name

Name of the advanced compression policy for which to display statistics. If no name is specified, statistics for all advanced compression policies are shown.

clearstats

Clear the statistics / counters Possible values: basic, full

Example

```
stat cmp policy
```

[Top](#)

rename cmp policy

Synopsis

```
rename cmp policy <name>@ <newName>@
```

Description

Renames a compression policy.

Parameters

name

Existing name of the policy.

newName

New name for the compression policy. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Choose a name that reflects the function that the policy performs. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cmp policy" or 'my cmp policy').

Example

```
rename cmp policy oldname newname
```

[Top](#)

cmp policylabel

[[add](#) | [rm](#) | [bind](#) | [unbind](#) | [show](#) | [stat](#) | [rename](#)]

add cmp policylabel

Synopsis

```
add cmp policylabel <labelName> -type ( REQ | RES )
```

Description

Creates a user-defined HTTP compression policy label for default-syntax policies. Policies that you bind to the label are evaluated only if you call the label from another policy.

Parameters**labelName**

Name of the HTTP compression policy label. Must begin with a letter, number, or the underscore character (_). Additional characters allowed, after the first character, are the hyphen (-), period (.) pound sign (#), space (), at sign (@), equals (=), and colon (:). The name must be unique within the list of policy labels for compression policies. Can be renamed after the policy label is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cmp policylabel" or 'my cmp policylabel').

type

Type of packets (request packets or response) against which to match the policies bound to this policy label. Possible values: REQ, RES

Example

```
add cmp policylabel cmp_pol_label -type REQ
```

[Top](#)

rm cmp policylabel

Synopsis

```
rm cmp policylabel <labelName>
```

Description

Removes an HTTP compression policy label.

Parameters

labelName

Name of the HTTP compression policy label to be removed.

Example

```
rm cmp policylabel cmp_pol_label
```

[Top](#)

bind cmp policylabel

Synopsis

```
bind cmp policylabel <labelName> -policyName <string> -priority <positive_integer> [-gotoPriorityExpression <expression>] [-invoke (<labelType> <labelName>)]
```

Description

Binds a default-syntax HTTP compression policy to an HTTP compression policy label.

Parameters

labelName

Name of the HTTP compression policy label to which to bind the policy.

policyName

Name of the compression policy to bind to the label.

Example

```
bind cmp policylabel cmp_pol_label -policyName  
cmp_pol -priority 1
```

[Top](#)

unbind cmp policylabel

Synopsis

```
unbind cmp policylabel <labelName> <policyName> [-priority <positive_integer>]
```

Description

Unbinds a default-syntax HTTP compression policy from an HTTP compression policy label.

Parameters

labelName

Name of the HTTP compression policy label from which to unbind the policy.

policyName

Name of the HTTP compression policy to unbind from the policy label.

priority

Priority of the NOPOLICY to unbind. Required only to unbind a NOPOLICY, if it has been bound to this policy label. Minimum value: 1 Maximum value: 2147483647

Example

```
unbind cmp policylabel cmp_pol_label cmp_pol
```

[Top](#)

show cmp policylabel

Synopsis

```
show cmp policylabel [<labelName>]
```

Description

Displays details of configured HTTP compression policy labels.

Parameters

labelName

Name of the HTTP compression policy label for which to display details.

Example

```
i)    show cmp policylabel cmp_pol_label
ii)   show cmp policylabel
```

[Top](#)

stat cmp policylabel

Synopsis

```
stat cmp policylabel [<labelName>] [-detail] [-fullValues] [-ntimes <positive_integer>]
[-logFile <input_filename>] [-clearstats ( basic | full )]
```

Description

Displays statistics for all compression policy labels.

Parameters

labelName

Name of the compression policy label for which to display statistics. If not specified, statistics are displayed for all compression policy labels.

clearstats

Clear the statistics / counters Possible values: basic, full

[Top](#)

rename cmp policylabel

Synopsis

```
rename cmp policylabel <labelName>@ <newName>@
```

Description

Renames a compression policylabel.

Parameters

labelName

Existing name of the policy label.

newName

New name for the compression policy label. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cmp policylabel" or 'my cmp policylabel').

Example

```
rename cmp policylabel oldname newname
```

[Top](#)

cmp stats

show cmp stats

Synopsis

```
show cmp stats - alias for 'stat cmp'
```

Description

show cmp stats is an alias for stat cmp Displays compression statistics.

cmp global

[[bind](#) | [unbind](#) | [show](#)]

bind cmp global

Synopsis

```
bind cmp global <policyName> [-priority <positive_integer>] [-state ( ENABLED |
DISABLED )] [-gotoPriorityExpression <expression>] [-type <type>] [-invoke (<labelType>
<labelName>)]
```

Description

Binds (activates) the compression policy globally. Note that the compression feature requires a compression license. When you enable the compression feature, all of the built-in compression policies are bound globally.

Parameters

policyName

Name of the policy to bind globally.

Example

```
add cmp policy pdf_cmp -rule "RES.HTTP.HEADER
Content-Type CONTAINS application/pdf" -resAction
COMPRESS
```

After creating the above compression policy, you must activate it by binding it globally:

```
bind cmp global pdf_cmp
```

After binding pdf_cmp compression policy globally, the policy gets activated and the NetScaler system will perform compression for the pdf files.

To view the globally active compression policies, enter the following command:

```
> show cmp global
      5 Globally Active Compression Policies:
1)      Policy Name: ns_cmp_content_type
Priority: 0
2)      Policy Name: ns_nocmp_mozilla_47
Priority: 0
3)      Policy Name: ns_cmp_mscss           Priority: 0
4)      Policy Name: ns_cmp_msapp          Priority: 0
5)      Policy Name: pdf_cmp               Priority: 0
      Done
```

[Top](#)

unbind cmp global

Synopsis

unbind cmp global <policyName> [-type <type> [-priority <positive_integer>]]

Description

Deactivates a globally bound HTTP compression policy.

Parameters

policyName

Name of the compression policy to unbind.

Example

```
To view the globally active compression policies,
enter the following command:
> show cmp global
      5 Globally Active Compression Policies:
1)      Policy Name: ns_cmp_content_type
Priority: 0
2)      Policy Name: ns_nocmp_mozilla_47
Priority: 0
3)      Policy Name: ns_cmp_mscss           Priority: 0
4)      Policy Name: ns_cmp_msapp          Priority: 0
5)      Policy Name: pdf_cmp               Priority: 0
Done

To deactivate this globally active compression
policy on the NetScaler system, enter the
following command:
unbind cmp global pdf_cmp
```

[Top](#)

show cmp global

Synopsis

show cmp global [-type <type>]

Description

Displays the globally bound HTTP compression policies.

Parameters

type

Bind point to which the policy is bound. Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT

Example

```
> show cmp global
      4 Globally Active Compression Policies:
1)      Policy Name: ns_cmp_content_type
Priority: 0
2)      Policy Name: ns_nocmp_mozilla_47
Priority: 0
3)      Policy Name: ns_cmp_mscss           Priority: 0
4)      Policy Name: ns_cmp_msapp          Priority: 0
Done
```

[Top](#)

cmp parameter

[[set](#) | [unset](#) | [show](#)]

set cmp parameter

Synopsis

```
set cmp parameter [-cmpLevel <cmpLevel>] [-quantumSize <positive_integer>] [-
serverCmp ( ON | OFF )] [-minResSize <positive_integer>] [-cmpBypassPct
<positive_integer>] [-cmpOnPush ( ENABLED | DISABLED )] [-policyType ( CLASSIC |
ADVANCED )] [-addVaryHeader ( ENABLED | DISABLED )] [-externalCache ( YES | NO )]
```

Description

Configures the compression parameters.

Parameters

cmpLevel

Specify a compression level. Available settings function as follows: * Optimal - Corresponds to a gzip GZIP level of 5-7. * Best speed - Corresponds to a gzip level of 1. * Best compression - Corresponds to a gzip level of 9. Possible values: optimal, bestspeed, bestcompression, spdy Default value: NSCMPLVL_OPTIMAL

quantumSize

Minimum quantum of data to be filled before compression begins. Default value: 57344 Minimum value: 8 Maximum value: 63488

serverCmp

Allow the server to send compressed data to the NetScaler appliance. With the default setting, the NetScaler appliance handles all compression. Possible values: ON, OFF Default value: ON

heurExpiry

Heuristic basefile expiry. Possible values: ON, OFF Default value: OFF

heurExpiryThres

Threshold compression ratio for heuristic basefile expiry, multiplied by 100. For example, to set the threshold ratio to 1.25, specify 125. Default value: 100 Minimum value: 1 Maximum value: 1000

heurExpiryHistWt

For heuristic basefile expiry, weightage to be given to historical delta compression ratio, specified as percentage. For example, to give 25% weightage to historical ratio (and therefore 75% weightage to the ratio for current delta compression transaction), specify 25. Default value: 50 Minimum value: 1 Maximum value: 100

minResSize

Smallest response size, in bytes, to be compressed.

cmpBypassPct

NetScaler CPU threshold after which compression is not performed. Range: 0 - 100
Default value: 100 Maximum value: 100

cmpOnPush

NetScaler appliance does not wait for the quantum to be filled before starting to compress data. Upon receipt of a packet with a PUSH flag, the appliance immediately begins compression of the accumulated packets. Possible values: ENABLED, DISABLED Default value: DISABLED

policyType

Type of policy. Available settings function as follows: * Classic - Classic policies evaluate basic characteristics of traffic and other data. * Advanced - Advanced policies (which have been renamed as default syntax policies) can perform the same type of evaluations as classic policies. They also enable you to analyze more data (for example, the body of an HTTP request) and to configure more operations in the policy rule (for example, transforming data in the body of a request into an HTTP header). Possible values: CLASSIC, ADVANCED Default value: NS_EXPR_TYPE_CLASSIC

addVaryHeader

Add the Vary header to HTTP responses being compressed. To HTTP 1.1 responses, add a Vary: User-Agent, Accept-Encoding header. Intermediate caches store different versions of the response for different values of the headers present in the Vary response header. Possible values: ENABLED, DISABLED Default value: DISABLED

externalCache

Enable insertion of Cache-Control: private response directive to indicate response message is intended for a single user and must not be cached by a shared or proxy cache. Possible values: YES, NO Default value: NO

Example

```
set cmp param -cmpLevel bestspeed -quantumSize 20480
```

[Top](#)

unset cmp parameter

Synopsis

unset cmp parameter [-cmpLevel] [-quantumSize] [-serverCmp] [-minResSize] [-cmpBypassPct] [-cmpOnPush] [-policyType] [-addVaryHeader] [-externalCache]

Description

Use this command to remove cmp parameter settings. Refer to the set cmp parameter command for meanings of the arguments.

[Top](#)

show cmp parameter

Synopsis

show cmp parameter

Description

Displays the values of the compression parameters. Example: > show cmp parameter
Configured compression parameters: Compression level: optimal Quantum size: 4555
Server-side compression: ON Minimum HTTP response size for compression: 0 CPU load
at which to bypass compression: 100% Compression on PUSH: DISABLED Compression
policy type: CLASSIC Vary header insertion: DISABLED Disable external cache: NO

[Top](#)

CO Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [co policy](#)
- ♦ [co parameter](#)

co policy

unset co policy

Synopsis

unset co policy <name> [-rule] [-action]

Description

Use this command to remove co policy settings. Refer to the set co policy command for meanings of the arguments.

co parameter

unset co parameter

Synopsis

unset co parameter [-cacheMaxage] [-imgType] [-JpegQualityPercent] [-inlineCssThresSize] [-inlineJsThresSize] [-inlineImgThresSize]

Description

Use this command to remove co parameter settings. Refer to the set co parameter command for meanings of the arguments.

Cache Redirection Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [cr policy](#)
- ♦ [cr vserver](#)

cr policy

[[add](#) | [rm](#) | [set](#) | [show](#)]

add cr policy

Synopsis

add cr policy <policyName> -rule <expression>

Description

Creates a cache redirection policy. To associate the new policy with a cache redirection virtual server, use the bind cr vserver command.

Parameters

policyName

Name for the cache redirection policy. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Cannot be changed after the policy is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy').

rule

Expression, or name of a named expression, against which traffic is evaluated. Written in the classic syntax. Note: Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>". The following requirements apply only to the NetScaler CLI: * If the expression includes one or more spaces, enclose the entire

expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

[Top](#)

rm cr policy

Synopsis

```
rm cr policy <policyName>
```

Description

Removes a cache redirection policy. You can delete a user-defined cache redirection policy that is not bound to a cache redirection virtual server. If the policy is bound to a virtual server, you must first unbind the policy, and then remove it.

Parameters

policyName

Name of the cache redirection policy to remove.

[Top](#)

set cr policy

Synopsis

```
set cr policy <policyName> -rule <expression>
```

Description

Changes the specified parameters of an existing cache redirection policy.

Parameters

policyName

Name of the cache redirection policy to change.

rule

Expression, or name of a named expression, against which traffic is evaluated. Written in the classic syntax. Note: Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>" The following requirements apply only to the NetScaler CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

[Top](#)

show cr policy

Synopsis

show cr policy [<policyName>]

Description

Displays all existing cache redirection policies, or just the specified policy.

Parameters

policyName

Name of the cache redirection policy to display. If this parameter is omitted, details of all the policies are displayed.

[Top](#)

cr vserver

[[add](#) | [rm](#) | [set](#) | [unset](#) | [bind](#) | [unbind](#) | [enable](#) | [disable](#) | [show](#) | [stat](#) | [rename](#)]

add cr vserver

Synopsis

```
add cr vserver <name> [-td <positive_integer>] <serviceType> [<IPAddress> <port> [-
range <positive_integer>]] [-cacheType <cacheType>] [-redirect <redirect>] [-
onPolicyMatch ( CACHE | ORIGIN )] [-redirectURL <URL>] [-cltTimeout <secs>] [-
precedence ( RULE | URL )] [-arp ( ON | OFF )] [-map ( ON | OFF )] [-format ( ON |
OFF )] [-via ( ON | OFF )] [-dnsVserverName <string>] [-destinationVServer <string>] [-
domain <string>] [-soPersistenceTimeOut <positive_integer>] [-soThreshold
<positive_integer>] [-reuse ( ON | OFF )] [-state ( ENABLED | DISABLED )] [-
downStateFlush ( ENABLED | DISABLED )] [-backupVServer <string>] [-
disablePrimaryOnDown ( ENABLED | DISABLED )] [-l2Conn ( ON | OFF )] [-backendssl
( ENABLED | DISABLED )] [-Listenpolicy <expression>] [-Listenpriority
<positive_integer>] [-tcpProfileName <string>] [-httpProfileName <string>] [-comment
<string>] [-srcIPExpr <expression>] [-originUSIP ( ON | OFF )] [-usePortRange ( ON |
OFF )] [-appflowLog ( ENABLED | DISABLED )] [-netProfile <string>] [-icmpVsrResponse
( PASSIVE | ACTIVE )]
```

Description

Creates a cache redirection virtual server.

Parameters

name

Name for the cache redirection virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the cache redirection virtual server is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my server" or 'my server').

td

Traffic Domain ID Maximum value: 4094

serviceType

Protocol (type of service) handled by the virtual server. Possible values: HTTP, SSL, NNTP

IPAddress

IPv4 or IPv6 address of the cache redirection virtual server. Usually a public IP address. Clients send connection requests to this IP address. Note: For a transparent cache redirection virtual server, use an asterisk (*) to specify a wildcard virtual server address.

cacheType

Mode of operation for the cache redirection virtual server. Available settings function as follows: * TRANSPARENT - Intercept all traffic flowing to the appliance and apply cache redirection policies to determine whether content should be served from the cache or from the origin server. * FORWARD - Resolve the hostname of the incoming request, by using a DNS server, and forward requests for non-cacheable content to the resolved origin servers. Cacheable requests are sent to the configured cache servers. * REVERSE - Configure reverse proxy caches for specific origin servers. Incoming traffic directed to the reverse proxy can either be served from a cache server or be sent to the origin server with or without modification to the URL. Possible values: TRANSPARENT, REVERSE, FORWARD Default value: CRD_TRANSPARENT

redirect

Type of cache server to which to redirect HTTP requests. Available settings function as follows: * CACHE - Direct all requests to the cache. * POLICY - Apply the cache redirection policy to determine whether the request should be directed to the cache or to the origin. * ORIGIN - Direct all requests to the origin server. Possible values: CACHE, POLICY, ORIGIN Default value: CRD_POLICY

onPolicyMatch

Redirect requests that match the policy to either the cache or the origin server, as specified. Note: For this option to work, you must set the cache redirection type to POLICY. Possible values: CACHE, ORIGIN Default value: CRD_ORIGIN

redirectURL

URL of the server to which to redirect traffic if the cache redirection virtual server configured on the NetScaler appliance becomes unavailable.

cltTimeout

Time-out value, in seconds, after which to terminate an idle client connection. Maximum value: 31536000

precedence

Type of policy (URL or RULE) that takes precedence on the cache redirection virtual server. Applies only to cache redirection virtual servers that have both URL and RULE based policies. If you specify URL, URL based policies are applied first, in the following order: 1. Domain and exact URL 2. Domain, prefix and suffix 3. Domain and suffix 4. Domain and prefix 5. Domain only 6. Exact URL 7. Prefix and suffix 8. Suffix only 9. Prefix only 10. Default If you specify RULE, the rule based policies are applied

before URL based policies are applied. Possible values: RULE, URL Default value: CS_PRIORITY_RULE

arp

Use ARP to determine the destination MAC address. Possible values: ON, OFF

map

Obsolete. Possible values: ON, OFF

via

Insert a via header in each HTTP request. In the case of a cache miss, the request is redirected from the cache server to the origin server. This header indicates whether the request is being sent from a cache server. Possible values: ON, OFF Default value: ON

cacheVserver

Name of the default cache virtual server to which to redirect requests (the default target of the cache redirection virtual server).

dnsVserverName

Name of the DNS virtual server that resolves domain names arriving at the forward proxy virtual server. Note: This parameter applies only to forward proxy virtual servers, not reverse or transparent.

destinationVServer

Destination virtual server for a transparent or forward proxy cache redirection virtual server.

domain

Default domain for reverse proxies. Domains are configured to direct an incoming request from a specified source domain to a specified target domain. There can be several configured pairs of source and target domains. You can select one pair to be the default. If the host header or URL of an incoming request does not include a source domain, this option sends the request to the specified target domain.

soPersistenceTimeOut

Time-out, in minutes, for spillover persistence. Minimum value: 2 Maximum value: 24

soThreshold

For CONNECTION (or) DYNAMICCONNECTION spillover, the number of connections above which the virtual server enters spillover mode. For BANDWIDTH spillover, the amount of incoming and outgoing traffic (in Kbps) before spillover. For HEALTH spillover, the percentage of active services (by weight) below which spillover occurs. Minimum value: 1

reuse

Reuse TCP connections to the origin server across client connections. Do not set this parameter unless the Service Type parameter is set to HTTP. If you set this parameter to OFF, the possible settings of the Redirect parameter function as follows: * CACHE - TCP connections to the cache servers are not reused. * ORIGIN - TCP connections to the origin servers are not reused. * POLICY - TCP connections to the origin servers are not reused. If you set the Reuse parameter to ON, connections to origin servers and connections to cache servers are reused. Possible values: ON, OFF Default value: ON

state

Initial state of the cache redirection virtual server. Possible values: ENABLED, DISABLED Default value: ENABLED

downStateFlush

Perform delayed cleanup of connections to this virtual server. Possible values: ENABLED, DISABLED Default value: ENABLED

backupVServer

Name of the backup virtual server to which traffic is forwarded if the active server becomes unavailable.

disablePrimaryOnDown

Continue sending traffic to a backup virtual server even after the primary virtual server comes UP from the DOWN state. Possible values: ENABLED, DISABLED Default value: DISABLED

l2Conn

Use L2 parameters, such as MAC, VLAN, and channel to identify a connection. Possible values: ON, OFF

backendssl

Decides whether the backend connection made by NS to the origin server will be HTTP or SSL. Applicable only for SSL type CR Forward proxy vserver. Possible values: ENABLED, DISABLED Default value: DISABLED

Listenpolicy

String specifying the listen policy for the cache redirection virtual server. Can be either an in-line expression or the name of a named expression. Default value: "none"

Listenpriority

Priority of the listen policy specified by the Listen Policy parameter. The lower the number, higher the priority. Default value: 101 Maximum value: 100

tcpProfileName

Name of the profile containing TCP configuration information for the cache redirection virtual server.

httpProfileName

Name of the profile containing HTTP configuration information for cache redirection virtual server.

comment

Comments associated with this virtual server.

srcIPExpr

Expression used to extract the source IP addresses from the requests originating from the cache. Can be either an in-line expression or the name of a named expression.

originUSIP

Use the client's IP address as the source IP address in requests sent to the origin server. Note: You can enable this parameter to implement fully transparent CR deployment. Possible values: ON, OFF Default value: OFF

usePortRange

Use a port number from the port range (set by using the set ns param command, or in the Create Virtual Server (Cache Redirection) dialog box) as the source port in the requests sent to the origin server. Possible values: ON, OFF Default value: OFF

appflowLog

Enable logging of AppFlow information. Possible values: ENABLED, DISABLED Default value: ENABLED

netProfile

Name of the network profile containing network configurations for the cache redirection virtual server.

icmpVsrResponse

Criterion for responding to PING requests sent to this virtual server. If ACTIVE, respond only if the virtual server is available. If PASSIVE, respond even if the virtual server is not available. Possible values: PASSIVE, ACTIVE Default value: NS_VSR_PASSIVE

[Top](#)

rm cr vsrserver**Synopsis**

```
rm cr vsrserver <name>@ ...
```

Description

Removes a virtual server.

Parameters**name**

Name of the virtual server to be removed.

Example

```
rm vsrserver cr_vip
```

[Top](#)

set cr vsrserver**Synopsis**

```
set cr vsrserver <name> [-IPAddress <ip_addr|ipv6_addr|*>] [-redirect <redirect>] [-onPolicyMatch ( CACHE | ORIGIN )] [-precedence ( RULE | URL )] [-arp ( ON | OFF )] [-via ( ON | OFF )] [-dnsVserverName <string>] [-destinationVServer <string>] [-domain <string>] [-reuse ( ON | OFF )] [-backupVServer <string>] [-disablePrimaryOnDown ( ENABLED | DISABLED )] [-redirectURL <URL>] [-cltTimeout <secs>] [-downStateFlush ( ENABLED | DISABLED )] [-l2Conn ( ON | OFF )] [-backendssl ( ENABLED | DISABLED )] [-Listenpolicy <expression>] [-Listenpriority <positive_integer>] [-tcpProfileName <string>] [-httpProfileName <string>] [-netProfile <string>] [-comment <string>] [-
```

```
srcIPExpr <expression>] [-originUSIP ( ON | OFF )] [-usePortRange ( ON | OFF )] [-  
appflowLog ( ENABLED | DISABLED )] [-icmpVsrResponse ( PASSIVE | ACTIVE )]
```

Description

Changes the specified settings of the cache redirection virtual server.

Parameters

name

Name of the cache redirection virtual server.

IPAddress

New IPv4 or IPv6 address of the cache redirection virtual server. Usually a public IP address. Clients send connection requests to this IP address.

redirect

Type of server to which to redirect HTTP requests. Available settings function as follows: * CACHE - Direct all requests to the cache. * POLICY - Apply the cache redirection policy to determine whether the request should be directed to the cache or to the origin. * ORIGIN - Direct all requests to the origin server. Possible values: CACHE, POLICY, ORIGIN Default value: CRD_POLICY

onPolicyMatch

Redirect requests that match the policy to either the cache or the origin server, as specified. Note: For this option to work, you must set the cache redirection type to POLICY. Possible values: CACHE, ORIGIN Default value: CRD_ORIGIN

precedence

Type of policy (URL or RULE) that takes precedence on the cache redirection virtual server. You can use this argument only when configuring cache redirection on the specified virtual server. It applies only if both URL and RULE based policies have been configured on the same virtual server. Available settings function as follows: URL - The incoming request is matched against the URL-based policies before it is matched against the rule-based policies. For URL based policies, the precedence hierarchy is: 1. Domain and exact URL 2. Domain, prefix and suffix 3. Domain and suffix 4. Domain and prefix 5. Domain only 6. Exact URL 7. Prefix and suffix 8. Suffix only 9. Prefix only 10. Default RULE - The incoming request is matched against the rule-based policies before it is matched against the URL-based policies. Possible values: RULE, URL Default value: CS_PRIORITY_RULE

arp

Use ARP to determine the destination MAC address. Specify OFF to use the incoming destination MAC address, or ON to use ARP to determine the destination MAC address. Possible values: ON, OFF

via

Insert a via header in each HTTP request. In the case of a cache miss, the request is redirected from the cache server to the origin server. This header indicates whether the request is being sent from a cache server. Possible values: ON, OFF Default value: ON

cacheVserver

Name of the default target cache virtual server to which to redirect requests.

dnsVserverName

Name of the DNS virtual server that resolves domain names arriving at the forward proxy virtual server. Note: This parameter applies only to forward proxy virtual servers, not reverse or transparent.

destinationVServer

Destination virtual server for a transparent or forward proxy cache redirection virtual server.

domain

Default domain for reverse proxies. Domains are configured to direct incoming requests from a specified source domain to a specified target domain. There can be several configured pairs of source and target domains. You can select one pair to be the default. If the host header or URL of an incoming request does not include a source domain, this option sends the request to the specified target domain.

reuse

Reuse TCP connections to the origin server across client connections Possible values: ON, OFF Default value: ON

backupVServer

Name of the backup virtual server to which traffic is forwarded if the active server becomes unavailable.

disablePrimaryOnDown

Continue sending traffic to a backup virtual server even after the primary virtual server comes UP from the DOWN state. Possible values: ENABLED, DISABLED Default value: DISABLED

redirectURL

URL of the server to which to redirect traffic if the cache redirection virtual server in the NetScaler becomes unavailable.

cltTimeout

Time-out value, in seconds, after which an idle client connection is terminated. Maximum value: 31536000

downStateFlush

Perform delayed cleanup of connections to this virtual server. Possible values: ENABLED, DISABLED Default value: ENABLED

l2Conn

Use L2 parameters, such as MAC, VLAN, and channel to identify a connection. Possible values: ON, OFF

backendssl

Decides whether the backend connection made by NS to the origin server will be HTTP or SSL. Applicable only for SSL type CR Forward proxy vserver. Possible values: ENABLED, DISABLED Default value: DISABLED

listenpolicy

String specifying the listen policy for the cache redirection virtual server. Can be either an in-line expression or the name of a named expression. Default value: "none"

Listenpriority

Priority of the listen policy specified by the Listen Policy parameter. The lower the number, higher the priority. Default value: 101 Maximum value: 100

tcpProfileName

Name of the profile containing TCP configuration information for the cache redirection virtual server.

httpProfileName

Name of the profile containing HTTP configuration information for cache redirection virtual server.

netProfile

Name of the network profile containing network configurations for the cache redirection virtual server.

comment

Comments associated with this virtual server.

srcIPExpr

Expression used to extract the source IP addresses from the requests originating from the cache. Can be either an in-line expression or the name of a named expression.

originUSIP

Use the client's IP address as the source IP address in requests sent to the origin server. Note: You can enable this parameter to implement fully transparent CR deployment. Possible values: ON, OFF Default value: OFF

usePortRange

Use a port number from the port range (set by using the set ns param command, or in the Create Virtual Server (Cache Redirection) dialog box) as the source port in the requests sent to the origin server. Possible values: ON, OFF Default value: OFF

appflowLog

Enable logging of AppFlow information. Possible values: ENABLED, DISABLED Default value: ENABLED

icmpVsrResponse

Criterion for responding to PING requests sent to this virtual server. If ACTIVE, respond only if the virtual server is available. If PASSIVE, respond even if the virtual server is not available. Possible values: PASSIVE, ACTIVE Default value: NS_VSR_PASSIVE

[Top](#)

unset cr vsrserver

Synopsis

```
unset cr vsrserver <name> [-dnsVserverName] [-destinationVServer] [-domain] [-
backupVServer] [-cltTimeout] [-redirectURL] [-l2Conn] [-backendssl] [-originUSIP] [-
usePortRange] [-srcIPExpr] [-tcpProfileName] [-httpProfileName] [-appflowLog] [-
netProfile] [-icmpVsrResponse] [-redirect] [-onPolicyMatch] [-precedence] [-arp] [-via]
[-reuse] [-disablePrimaryOnDown] [-downStateFlush] [-Listenpolicy] [-Listenpriority] [-
comment]
```

Description

Restores the specified parameters of a cache redirection virtual server to their default values. To unset all except the Name parameter, do not specify a value for any other parameter. Refer to the set cr vserver command for a description of the parameters..Refer to the set cr vserver command for meanings of the arguments.

[Top](#)

bind cr vserver

Synopsis

```
bind cr vserver <name> [-lbvserver <string> | (-policyName <string> [-priority
<positive_integer>]) | <targetVserver>]
```

Description

Binds a cache redirection policy to a cache redirection virtual server.

Parameters

name

Name of the cache redirection virtual server to which to bind the cache redirection policy.

lbvserver

Name of the virtual server to which content is forwarded. Applicable only if the policy is a map policy and the cache redirection virtual server is of type REVERSE.

policyName

Name of the cache redirection policy that you are binding.

[Top](#)

unbind cr vserver

Synopsis

```
unbind cr vserver <name> [-policyName <string> | -lbvserver <string>]
```

Description

Unbinds a cache redirection policy from a cache redirection virtual server.

Parameters

name

Name of the cache redirection virtual server from which to unbind the policy.

policyName

Name of the cache redirection policy that you are unbinding.

lbvserver

The virtual server name (created with the add lb vserver command) to which content will be switched. Default value: "default_lb"

[Top](#)

enable cr vserver

Synopsis

enable cr vserver <name>@

Description

Enables a cache redirection virtual server. Note: Virtual servers, when added, are enabled by default.

Parameters

name

Name of the cache redirection virtual server to be enabled.

Example

```
enable vserver cr_vip
```

[Top](#)

disable cr vserver

Synopsis

disable cr vserver <name>@

Description

Disables a cache redirection virtual server.

Parameters

name

Name of the cache redirection virtual server to be disabled. (Because the virtual server is still configured, you can reenable it.) Note: The appliance still responds to ARP and ping requests sent to the IP address of this virtual server.

Example

```
disable vserver cr_vip
```

[Top](#)

show cr vserver

Synopsis

show cr vserver [<name>]

Description

Displays cache redirection virtual server information. To display information about all configured cache redirection virtual servers, do not include a parameter. To display detailed information about a specific virtual server, use the name parameter to specify the name of the virtual server.

Parameters

name

Name of a cache redirection virtual server about which to display detailed information.

[Top](#)

stat cr vserver

Synopsis

```
stat cr vserver [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-clearstats ( basic | full )]
```

Description

Displays statistics for all cache redirection virtual servers or for the cache redirection virtual server specified by the name parameter.

Parameters

name

Name of a specific cache redirection virtual server.

clearstats

Clear the statistics / counters Possible values: basic, full

[Top](#)

rename cr vserver

Synopsis

```
rename cr vserver <name>@ <newName>@
```

Description

Renames a cache redirection virtual server.

Parameters

name

Existing name of the cache redirection virtual server.

newName

New name for the cache redirection virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my name" or 'my name').

Example

```
rename cr vserver vscr1 vscrnew
```

[Top](#)

Content Switching Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [cs policy](#)
- ♦ [cs policylabel](#)
- ♦ [cs vserver](#)
- ♦ [cs parameter](#)
- ♦ [cs action](#)

cs policy

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#) | [rename](#)]

add cs policy

Synopsis

```
add cs policy <policyName> [-url <string> | -rule <expression> | -action <string>] [-domain <string>] [-logAction <string>]
```

Description

Creates a new content switching policy. You use this policy to manage content switching on a virtual server.

Parameters

policyName

Name for the content switching policy. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Cannot be changed after a policy is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy').

url

URL string that is matched with the URL of a request. Can contain a wildcard character. Specify the string value in the following format: [[prefix] [*]] [.suffix].

rule

Expression, or name of a named expression, against which traffic is evaluated. Written in the classic or default syntax. Note: Maximum length of a string literal in

the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>". The following requirements apply only to the NetScaler CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

domain

The domain name. The string value can range to 63 characters.

action

Content switching action that names the target load balancing virtual server to which the traffic is switched.

logAction

The log action associated with the content switching policy

Example

```
To match the requests that have URL "/", you would
enter the following command:
add cs policy <policyName> -url /
To match with all URLs that start with "/sports/",
you would enter the following command:
add cs policy <policyName> -url /sports/*
To match requests with URLs that start with "/"
sports", you would enter the following command:
add cs policy <policyName> -url /sports*
To match requests with the URL "/sports/tennis/
index.html", you would enter the following command:
add cs policy <policyName> -url /sports/tennis/
index.html
To match requests that have URLs with the
extension ".jsp", you would enter the following
command:
add cs policy <policyName> -url /*.jsp
To match requests with URLs that start with "/"
sports/" and the file extension ".jsp", you would
enter the following command:
add cs policy <policyName> -url /sports/*.jsp
To match requests with URLs that contain "sports",
you would enter the following commands:
add pol expression sports_url "URL contains sports"
add cs policy <policyName> -rule sports_url
To match requests with URL queries that contain
"gold" or cookie headers that contain "gold", you
would enter the following commands:
add pol expression gold_query "URLQUERY contains
gold"
add pol expression gold_cookie "Header COOKIE
contains gold"
add cs policy <policyName> -rule "(gold_query ||
```

```
gold_cookie)"
To match requests with the domain name
www.domainxyz.com, you enter the following command:
add cs policy <policyName> -domain
"www.domainxyz.com"
To match requests with the domain name
www.domainxyz.com and URLs with the extension
".jsp", you would enter the following command:
add cs policy <policyName> -url /*.jsp -domain
"www.domainxyz.com"
To match requests with the domain name
www.domainxyz.com and URLs that contain "sports",
you would enter the following commands:
add pol expression sports_url "URL contains sports"
add cs policy <policyName> -rule sports_url -
domain "www.domainxyz.com"
To match a policy with a rule and provide action:
add cs policy <policyname> -rule
"http.req.method.eq(GET)" -action act1
```

[Top](#)

rm cs policy

Synopsis

```
rm cs policy <policyName>
```

Description

Removes a content switching policy. You can delete a user-defined content switching policy that is not bound to a content switching virtual server. If the policy is bound to a virtual server, you must first unbind the policy, and then remove it.

Parameters

policyName

Name of the content switching policy to be removed.

[Top](#)

set cs policy

Synopsis

```
set cs policy <policyName> [-url <string> | -rule <expression>] [-domain <string>] [-
action <string>] [-logAction <string>]
```

Description

Changes an existing content switching policy.

Parameters

policyName

Name of the content switching policy.

url

The URL, with wildcards.

rule

The condition for applying this policy.

domain

The domain name.

action

The content switching action name.

logAction

The log action associated with the content switching policy

[Top](#)

unset cs policy

Synopsis

```
unset cs policy <policyName> [-logAction] [-url] [-rule] [-domain] [-action]
```

Description

Unset logaction for existing content switching policy..Refer to the set cs policy command for meanings of the arguments.

Example

```
unset cs policy pol9 -logAction
```

[Top](#)

show cs policy

Synopsis

```
show cs policy [<policyName>]
```

Description

Displays all existing content switching policies, or just the specified policy.

Parameters

policyName

Name of the content switching policy to display. If this parameter is omitted, details of all the policies are displayed.

[Top](#)

rename cs policy

Synopsis

```
rename cs policy <policyName>@ <newName>@
```

Description

Rename a content switching policy.

Parameters

policyName

The name of the content switching policy.

newName

The new name of the content switching policy.

Example

```
rename cs policy oldname newname
```

[Top](#)

cs policylabel

[[add](#) | [rm](#) | [bind](#) | [unbind](#) | [show](#) | [rename](#)]

add cs policylabel

Synopsis

add cs policylabel <labelName> <cspolicylabeltype>

Description

Adds a content switching policy label.

Parameters

labelName

Name for the policy label. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. The label name must be unique within the list of policy labels for content switching. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, \"my label\" or 'my policylabel').

cspolicylabeltype

Protocol supported by the policy label. All policies bound to the policy label must either match the specified protocol or be a subtype of that protocol. Available settings function as follows: * HTTP - Supports policies that process HTTP traffic. Used to access unencrypted Web sites. (The default.) * SSL - Supports policies that process HTTPS/SSL encrypted traffic. Used to access encrypted Web sites. * TCP - Supports policies that process any type of TCP traffic, including HTTP. * SSL_TCP - Supports policies that process SSL-encrypted TCP traffic, including SSL. * UDP - Supports policies that process any type of UDP-based traffic, including DNS. * DNS - Supports policies that process DNS traffic. * ANY - Supports all types of policies

except HTTP, SSL, and TCP. * SIP_UDP - Supports policies that process UDP based Session Initiation Protocol (SIP) traffic. SIP initiates, manages, and terminates multimedia communications sessions, and has emerged as the standard for Internet telephony (VoIP). * RTSP - Supports policies that process Real Time Streaming Protocol (RTSP) traffic. RTSP provides delivery of multimedia and other streaming data, such as audio, video, and other types of streamed media. * RADIUS - Supports policies that process Remote Authentication Dial In User Service (RADIUS) traffic. RADIUS supports combined authentication, authorization, and auditing services for network management. * MYSQL - Supports policies that process MYSQL traffic. * MSSQL - Supports policies that process Microsoft SQL traffic. Possible values: HTTP, TCP, RTSP, SSL, SSL_TCP, UDP, DNS, SIP_UDP, ANY, RADIUS, RDP, MYSQL, MSSQL, DIAMETER, SSL_DIAMETER, FTP

Example

```
add cs policylabel trans_http_url HTTP
```

[Top](#)
rm cs policylabel**Synopsis**

```
rm cs policylabel <labelName>
```

Description

Removes a content switching policy label.

Parameters

labelName

Name of the label to be removed.

Example

```
rm cs policylabel trans_http_url
```

[Top](#)
bind cs policylabel**Synopsis**

```
bind cs policylabel <labelName> <policyName> <priority> [-targetVserver <string> | -gotoPriorityExpression <expression> | (-invoke (<labelType> <labelName>) )]
```

Description

Binds a content switching policy to a content switching policy label.

Parameters

labelName

Name of the policy label to which to bind a content switching policy.

policyName

Name of the content switching policy to bind to the content switching policy label.

priority

Unsigned integer that determines the priority of the policy relative to other policies in this policy label. Smaller the number, higher the priority. Minimum value: 1

Maximum value: 2147483647

targetVserver

Name of the virtual server to which to forward requests that match the policy.

gotoPriorityExpression

Expression or other value specifying the priority of the next policy to be evaluated if the current policy rule evaluates to TRUE. Alternatively, you can specify one of the following values: * NEXT - Go to the policy with the next higher priority. * END - End evaluation. (This is the default. Evaluation stops if the gotoPriorityExpression parameter is not set.) * USE_INVOCATION_RESULT - Applicable if this entry invokes another policy label. If the final goto in the invoked policy label has a value of END, evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. If you specify an expression, its result must be a number. In that case, the next action is determined as follows: * If the expression evaluates to the priority of a policy with a lower priority (larger priority number) than the current policy, that policy is evaluated next. * If the expression evaluates to a priority of the current policy, policy with the next highest priority is evaluated. An UNDEF event is triggered if: * The expression cannot be evaluated. * The expression evaluates to a number that is smaller than the highest priority in the policy bank but is not same as any policy's priority. * The expression evaluates to a number that is smaller than the current policy's priority.

invoke

Invoke other policy labels. After evaluating the policies in the invoked policy label, the appliance continues to evaluate policies that are bound to the current policy label (the selected bind point).

Example

```
i)      bind cs policylabel cs_lab lbvs_1 pol_cs 1
2
```

[Top](#)

unbind cs policylabel

Synopsis

unbind cs policylabel <labelName> <policyName>

Description

Unbinds a content switching policy from a content switching policy label.

Parameters

labelName

Name of the policy label from which to unbind a content switching policy.

policyName

Name of the content switching policy to unbind from the label.

Example

```
unbind cs policylabel cs_lab pol_cs
```

[Top](#)

show cs policylabel

Synopsis

```
show cs policylabel [<labelName>]
```

Description

Displays all the content switching policy labels, or just the specified policy label.

Parameters

labelName

Name of the content switching policy label to display.

Example

```
i)      show cs policylabel cs_lab
ii)     show cs policylabel
```

[Top](#)

rename cs policylabel

Synopsis

```
rename cs policylabel <labelName>@ <newName>@
```

Description

Rename a content switching policy label.

Parameters

labelName

The name of the content switching policylabel.

newName

The new name of the content switching policylabel.

Example

```
rename cs policylabel oldname newname
```

[Top](#)

cs vserver

[[add](#) | [rm](#) | [set](#) | [unset](#) | [bind](#) | [unbind](#) | [enable](#) | [disable](#) | [show](#) | [stat](#) | [rename](#)]

add cs vserver

Synopsis

```
add cs vserver <name> [-td <positive_integer>] <serviceType> ((<IPAddress> [-range
<positive_integer>]) | (-IPPattern <ippat> -IPMask <ipmask>)) <port> [-state ( ENABLED
| DISABLED )] [-stateupdate ( ENABLED | DISABLED )] [-cacheable ( YES | NO )] [-
redirectURL <URL>] [-cltTimeout <secs>] [-precedence ( RULE | URL )] [-caseSensitive
( ON | OFF )] [-soMethod <soMethod>] [-soPersistence ( ENABLED | DISABLED )] [-
soPersistenceTimeOut <positive_integer>] [-soThreshold <positive_integer>] [-
soBackupAction <soBackupAction>] [-redirectPortRewrite ( ENABLED | DISABLED )] [-
downStateFlush ( ENABLED | DISABLED )] [-backupVServer <string>] [-
disablePrimaryOnDown ( ENABLED | DISABLED )] [-insertVserverIPPort
<insertVserverIPPort> [<vipHeader>] ] [-rtspNat ( ON | OFF )] [-AuthenticationHost
<string>] [-Authentication ( ON | OFF )] [-Listenpolicy <expression>] [-Listenpriority
<positive_integer>] [-authn401 ( ON | OFF )] [-authnVsName <string>] [-push
( ENABLED | DISABLED )] [-pushVserver <string>] [-pushLabel <expression>] [-
pushMultiClients ( YES | NO )] [-tcpProfileName <string>] [-httpProfileName <string>] [-
dbProfileName <string>] [-comment <string>] [-mssqlServerVersion
<mssqlServerVersion>] [-l2Conn ( ON | OFF )] [-mysqlProtocolVersion
<positive_integer>] [-mysqlServerVersion <string>] [-mysqlCharacterSet
<positive_integer>] [-mysqlServerCapabilities <positive_integer>] [-appflowLog
( ENABLED | DISABLED )] [-netProfile <string>] [-icmpVsrResponse ( PASSIVE | ACTIVE )]
[-authnProfile <string>]
```

Description

Creates a content switching virtual server.

Parameters

name

Name for the content switching virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Cannot be changed after the CS virtual server is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more

spaces, enclose the name in double or single quotation marks (for example, \"my server\" or \'my server\').

td

Traffic Domain ID Maximum value: 4094

serviceType

Protocol used by the virtual server. Possible values: HTTP, SSL, TCP, FTP, RTSP, SSL_TCP, UDP, DNS, SIP_UDP, ANY, RADIUS, RDP, MYSQL, MSSQL, DIAMETER, SSL_DIAMETER

IPAddress

IP address of the content switching virtual server.

IPPattern

IP address pattern, in dotted decimal notation, for identifying packets to be accepted by the virtual server. The IP Mask parameter specifies which part of the destination IP address is matched against the pattern. Mutually exclusive with the IP Address parameter. For example, if the IP pattern assigned to the virtual server is 198.51.100.0 and the IP mask is 255.255.240.0 (a forward mask), the first 20 bits in the destination IP addresses are matched with the first 20 bits in the pattern. The virtual server accepts requests with IP addresses that range from 198.51.96.1 to 198.51.111.254. You can also use a pattern such as 0.0.2.2 and a mask such as 0.0.255.255 (a reverse mask). If a destination IP address matches more than one IP pattern, the pattern with the longest match is selected, and the associated virtual server processes the request. For example, if the virtual servers, vs1 and vs2, have the same IP pattern, 0.0.100.128, but different IP masks of 0.0.255.255 and 0.0.224.255, a destination IP address of 198.51.100.128 has the longest match with the IP pattern of vs1. If a destination IP address matches two or more virtual servers to the same extent, the request is processed by the virtual server whose port number matches the port number in the request.

range

Number of consecutive IP addresses, starting with the address specified by the IP Address parameter, to include in a range of addresses assigned to this virtual server. Default value: 1 Minimum value: 1 Maximum value: 254

port

Port number for content switching virtual server. Minimum value: 1

state

Initial state of the load balancing virtual server. Possible values: ENABLED, DISABLED Default value: ENABLED

stateupdate

Enable state updates for a specific content switching virtual server. By default, the Content Switching virtual server is always UP, regardless of the state of the Load Balancing virtual servers bound to it. This parameter interacts with the global setting as follows: Global Level | Vserver Level | Result
 ENABLED ENABLED ENABLED
 ENABLED DISABLED ENABLED DISABLED ENABLED ENABLED DISABLED DISABLED
 DISABLED If you want to enable state updates for only some content switching virtual servers, be sure to disable the state update parameter. Possible values: ENABLED, DISABLED Default value: DISABLED

cacheable

Use this option to specify whether a virtual server, used for load balancing or content switching, routes requests to the cache redirection virtual server before sending it to the configured servers. Possible values: YES, NO Default value: NO

redirectURL

URL to which traffic is redirected if the virtual server becomes unavailable. The service type of the virtual server should be either HTTP or SSL. Caution: Make sure that the domain in the URL does not match the domain specified for a content switching policy. If it does, requests are continuously redirected to the unavailable virtual server.

cltTimeout

Idle time, in seconds, after which the client connection is terminated. The default values are: 180 seconds for HTTP/SSL-based services. 9000 seconds for other TCP-based services. 120 seconds for DNS-based services. 120 seconds for other UDP-based services. Default value: VAL_NOT_SET Maximum value: 31536000

precedence

Type of precedence to use for both RULE-based and URL-based policies on the content switching virtual server. With the default (RULE) setting, incoming requests are evaluated against the rule-based content switching policies. If none of the rules match, the URL in the request is evaluated against the URL-based content switching policies. Possible values: RULE, URL Default value: CS_PRIORITY_RULE

caseSensitive

Consider case in URLs (for policies that use URLs instead of RULES). For example, with the ON setting, the URLs /a/1.html and /A/1.HTML are treated differently and can have different targets (set by content switching policies). With the OFF setting, /a/1.html and /A/1.HTML are switched to the same target. Possible values: ON, OFF Default value: ON

soMethod

Type of spillover used to divert traffic to the backup virtual server when the primary virtual server reaches the spillover threshold. Connection spillover is based on the number of connections. Bandwidth spillover is based on the total Kbps of incoming and outgoing traffic. Possible values: CONNECTION, DYNAMICCONNECTION, BANDWIDTH, HEALTH, NONE

soPersistence

Maintain source-IP based persistence on primary and backup virtual servers. Possible values: ENABLED, DISABLED Default value: DISABLED

soPersistenceTimeOut

Time-out value, in minutes, for spillover persistence. Default value: 2 Minimum value: 2 Maximum value: 1440

soThreshold

Depending on the spillover method, the maximum number of connections or the maximum total bandwidth (Kbps) that a virtual server can handle before spillover occurs. Minimum value: 1 Maximum value: 4294967287

soBackupAction

Action to be performed if spillover is to take effect, but no backup chain to spillover is usable or exists Possible values: DROP, ACCEPT, REDIRECT

redirectPortRewrite

State of port rewrite while performing HTTP redirect. Possible values: ENABLED, DISABLED Default value: DISABLED

downStateFlush

Perform delayed cleanup of connections on this vserver. Possible values: ENABLED, DISABLED Default value: ENABLED

backupVServer

Name of the backup virtual server that you are configuring. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the backup virtual server is created. You can assign a different backup virtual server or rename the existing virtual server. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks.

disablePrimaryOnDown

Continue forwarding the traffic to backup virtual server even after the primary server comes UP from the DOWN state. Possible values: ENABLED, DISABLED Default value: DISABLED

insertVserverIPPort

Insert the virtual server's VIP address and port number in the request header. Available values function as follows: VIPADDR - Header contains the vserver's IP address and port number without any translation. OFF - The virtual IP and port header insertion option is disabled. V6TOV4MAPPING - Header contains the mapped IPv4 address corresponding to the IPv6 address of the vserver and the port number. An IPv6 address can be mapped to a user-specified IPv4 address using the set ns ip6 command. Possible values: OFF, VIPADDR, V6TOV4MAPPING

rtspNat

Enable network address translation (NAT) for real-time streaming protocol (RTSP) connections. Possible values: ON, OFF Default value: OFF

AuthenticationHost

FQDN of the authentication virtual server. The service type of the virtual server should be either HTTP or SSL.

Authentication

Authenticate users who request a connection to the content switching virtual server. Possible values: ON, OFF Default value: OFF

Listenpolicy

String specifying the listen policy for the content switching virtual server. Can be either the name of an existing expression or an in-line expression. Default value: "none"

Listenpriority

Integer specifying the priority of the listen policy. A higher number specifies a lower priority. If a request matches the listen policies of more than one virtual server the

virtual server whose listen policy has the highest priority (the lowest priority number) accepts the request. Default value: 101 Maximum value: 100

authn401

Enable HTTP 401-response based authentication. Possible values: ON, OFF Default value: OFF

authnVsName

Name of authentication virtual server that authenticates the incoming user requests to this content switching virtual server.

push

Process traffic with the push virtual server that is bound to this content switching virtual server (specified by the Push VServer parameter). The service type of the push virtual server should be either HTTP or SSL. Possible values: ENABLED, DISABLED Default value: DISABLED

pushVserver

Name of the load balancing virtual server, of type PUSH or SSL_PUSH, to which the server pushes updates received on the client-facing load balancing virtual server.

pushLabel

Expression for extracting the label from the response received from server. This string can be either an existing rule name or an inline expression. The service type of the virtual server should be either HTTP or SSL. Default value: "none"

pushMultiClients

Allow multiple Web 2.0 connections from the same client to connect to the virtual server and expect updates. Possible values: YES, NO Default value: NO

tcpProfileName

Name of the TCP profile containing TCP configuration settings for the virtual server.

httpProfileName

Name of the HTTP profile containing HTTP configuration settings for the virtual server. The service type of the virtual server should be either HTTP or SSL.

dbProfileName

Name of the DB profile.

comment

Information about this virtual server.

mssqlServerVersion

The version of the MSSQL server Possible values: 70, 2000, 2000SP1, 2005, 2008, 2008R2, 2012 Default value: TDS_PROT_2008B

l2Conn

Use L2 Parameters to identify a connection Possible values: ON, OFF

mysqlProtocolVersion

The protocol version returned by the mysql vserver. Default value: 10

mysqlServerVersion

The server version string returned by the mysql vserver. Default value: NSA_MYSQL_SERVER_VER_DEFAULT

mysqlCharacterSet

The character set returned by the mysql vserver. Default value: 8

mysqlServerCapabilities

The server capabilities returned by the mysql vserver. Default value: 41613

appflowLog

Enable logging appflow flow information Possible values: ENABLED, DISABLED Default value: ENABLED

netProfile

The name of the network profile.

icmpVsrResponse

Can be active or passive Possible values: PASSIVE, ACTIVE Default value: NS_VSR_PASSIVE

authnProfile

Name of the authentication profile to be used when authentication is turned on.

Example

1. You can use precedence when certain client attributes (e.g., browser type) require to be served with different content. All other clients can then be served from content distributed among the servers.
If the precedence is configured as URL, the incoming request URL is evaluated against the content switching policies created with the `-url` argument. If none of the policies match, the request is applied against the content any switching policies created with the `-rule` argument.

2. Precedence can also be used when certain content (such as images) is the same for all clients, but other content (such as text) is different for different clients. In this case, the images will be served to all clients, but the text will be served to specific clients based on attributes such as Accept-Language.

[Top](#)

rm cs vserver**Synopsis**

```
rm cs vserver <name>@ ...
```

Description

Removes a content switching virtual server.

Parameters

name

Name of the virtual server to be removed.

Example

```
rm vserver cs_vip
```

[Top](#)

set cs vserver

Synopsis

```
set cs vserver <name> [-IPAddress <ip_addr|ipv6_addr|*>] [-IPPattern <ippat>] [-IPMask
<ipmask>] [-stateupdate ( ENABLED | DISABLED )] [-precedence ( RULE | URL )] [-
caseSensitive ( ON | OFF )] [-backupVServer <string>] [-redirectURL <URL>] [-cacheable
( YES | NO )] [-cltTimeout <secs>] [-soMethod <soMethod>] [-soPersistence ( ENABLED |
DISABLED )] [-soPersistenceTimeOut <positive_integer>] [-soThreshold
<positive_integer>] [-soBackupAction <soBackupAction>] [-redirectPortRewrite
( ENABLED | DISABLED )] [-downStateFlush ( ENABLED | DISABLED )] [-
disablePrimaryOnDown ( ENABLED | DISABLED )] [-insertVserverIPPort
<insertVserverIPPort> [<vipHeader>]] [-rtspNat ( ON | OFF )] [-AuthenticationHost
<string>] [-Authentication ( ON | OFF )] [-Listenpolicy <expression>] [-Listenpriority
<positive_integer>] [-authn401 ( ON | OFF )] [-authnVsName <string>] [-push ( ENABLED
| DISABLED )] [-pushVserver <string>] [-pushLabel <expression>] [-pushMultiClients
( YES | NO )] [-tcpProfileName <string>] [-httpProfileName <string>] [-dbProfileName
<string>] [-comment <string>] [-l2Conn ( ON | OFF )] [-mssqlServerVersion
<mssqlServerVersion>] [-mysqlProtocolVersion <positive_integer>] [-mysqlServerVersion
<string>] [-mysqlCharacterSet <positive_integer>] [-mysqlServerCapabilities
<positive_integer>] [-appflowLog ( ENABLED | DISABLED )] [-netProfile <string>] [-
authnProfile <string>] [-icmpVsrResponse ( PASSIVE | ACTIVE )]
```

Description

Modifies the configuration of a content switching virtual server.

Parameters

name

Identifies the virtual server name (created with the add cs vserver command).

IPAddress

The new IP address of the virtual server.

IPPattern

IP address pattern, in dotted decimal notation, for identifying packets to be accepted by the virtual server. The IP Mask parameter specifies which part of the destination IP address is matched against the pattern. Mutually exclusive with the IP Address parameter. For example, if the IP pattern assigned to the virtual server is 198.51.100.0 and the IP mask is 255.255.240.0 (a forward mask), the first 20 bits in the destination IP addresses are matched with the first 20 bits in the pattern. The

virtual server accepts requests with IP addresses that range from 198.51.96.1 to 198.51.111.254. You can also use a pattern such as 0.0.2.2 and a mask such as 0.0.255.255 (a reverse mask). If a destination IP address matches more than one IP pattern, the pattern with the longest match is selected, and the associated virtual server processes the request. For example, if the virtual servers, vs1 and vs2, have the same IP pattern, 0.0.100.128, but different IP masks of 0.0.255.255 and 0.0.224.255, a destination IP address of 198.51.100.128 has the longest match with the IP pattern of vs1. If a destination IP address matches two or more virtual servers to the same extent, the request is processed by the virtual server whose port number matches the port number in the request.

IPMask

IP mask, in dotted decimal notation, for the IP Pattern parameter. Can have leading or trailing non-zero octets (for example, 255.255.240.0 or 0.0.255.255). Accordingly, the mask specifies whether the first n bits or the last n bits of the destination IP address in a client request are to be matched with the corresponding bits in the IP pattern. The former is called a forward mask. The latter is called a reverse mask.

stateupdate

Enable state updates for a specific content switching virtual server. By default, the Content Switching virtual server is always UP, regardless of the state of the Load Balancing virtual servers bound to it. This parameter interacts with the global setting as follows: Global Level | Vserver Level | Result
 ENABLED ENABLED ENABLED
 ENABLED DISABLED ENABLED DISABLED ENABLED ENABLED DISABLED DISABLED
 DISABLED If you want to enable state updates for only some content switching virtual servers, be sure to disable the state update parameter. Possible values: ENABLED, DISABLED Default value: DISABLED

precedence

The precedence on the content switching virtual server between rule-based and URL-based policies. The default precedence is set to RULE. If the precedence is configured as RULE, the incoming request is applied against the content switching policies created with the -rule argument. If none of the rules match, then the URL in the request is applied against the content switching policies created with the -url option. For example, this precedence can be used if certain client attributes (such as a specific type of browser) need to be served different content and all other clients can be served from the content distributed among the servers. If the precedence is configured as URL, the incoming request URL is applied against the content switching policies created with the -url option. If none of the policies match, then the request is applied against the content switching policies created with the -rule option. Also, this precedence can be used if some content (such as images) is the same for all clients, but other content (such as text) is different for different clients. In this case, the images will be served to all clients, but the text will be served to specific clients based on specific attributes, such as Accept-Language. Possible values: RULE, URL Default value: CS_PRIORITY_RULE

caseSensitive

The URL lookup case option on the content switching vserver. If case sensitivity of a content switching virtual server is set to 'ON', the URLs /a/1.html and /A/1.HTML are treated differently and may have different targets (set by content switching policies). If case sensitivity is set to 'OFF', the URLs /a/1.html and /A/1.HTML are

treated the same, and will be switched to the same target. Possible values: ON, OFF
Default value: ON

backupVServer

Name of the backup virtual server that you are configuring. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the backup virtual server is created. You can assign a different backup virtual server or rename the existing virtual server. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks.

redirectURL

The redirect URL for content switching.

cacheable

The option to specify whether a virtual server used for content switching will route requests to the cache redirection virtual server before sending it to the configured servers. Possible values: YES, NO Default value: NO

cltTimeout

Client timeout in seconds. Default value: VAL_NOT_SET Maximum value: 31536000

soMethod

The spillover factor. When traffic on the main virtual server reaches this threshold, additional traffic is sent to the backupvserver. Possible values: CONNECTION, DYNAMICCONNECTION, BANDWIDTH, HEALTH, NONE

soPersistence

Maintain source-IP based persistence on primary and backup virtual servers. Possible values: ENABLED, DISABLED Default value: DISABLED

soPersistenceTimeOut

The spillover persistency entry timeout. Default value: 2 Minimum value: 2 Maximum value: 1440

soThreshold

Depending on the spillover method, the maximum number of connections or the maximum total bandwidth (Kbps) that a virtual server can handle before spillover occurs. Minimum value: 1 Maximum value: 4294967287

soBackupAction

Action to be performed if spillover is to take effect, but no backup chain to spillover is usable or exists Possible values: DROP, ACCEPT, REDIRECT

redirectPortRewrite

SSL redirect port rewrite. Possible values: ENABLED, DISABLED Default value: DISABLED

downStateFlush

Perform delayed clean up of connections on this vserver. Possible values: ENABLED, DISABLED Default value: ENABLED

disablePrimaryOnDown

Continue forwarding the traffic to backup virtual server even after the primary server comes UP from the DOWN state. Possible values: ENABLED, DISABLED Default value: DISABLED

insertVserverIPPort

The virtual IP and port header insertion option for the vserver. * VIPADDR - Header contains the vserver's IP address and port number without any translation. * OFF - The virtual IP and port header insertion option is disabled. * V6TOV4MAPPING - Header contains the mapped IPv4 address that corresponds to the IPv6 address of the vserver and the port number. An IPv6 address can be mapped to a user-specified IPv4 address using the set ns ip6 command. Possible values: OFF, VIPADDR, V6TOV4MAPPING

rtspNat

Enable network address translation (NAT) for real-time streaming protocol (RTSP) connections. Possible values: ON, OFF Default value: OFF

AuthenticationHost

FQDN of the authentication virtual server. The service type of the virtual server should be either HTTP or SSL.

Authentication

Authenticate users who request a connection to the content switching virtual server. Possible values: ON, OFF Default value: OFF

Listenpolicy

String specifying the listen policy for the content switching virtual server. Can be either the name of an existing expression or an in-line expression. Default value: "none"

Listenpriority

Integer specifying the priority of the listen policy. A higher number specifies a lower priority. If a request matches the listen policies of more than one virtual server the virtual server whose listen policy has the highest priority (the lowest priority number) accepts the request. Default value: 101 Maximum value: 100

authn401

Enable HTTP 401-response based authentication. Possible values: ON, OFF Default value: OFF

authnVsName

Name of authentication virtual server that authenticates the incoming user requests to this content switching virtual server.

push

Process traffic with the push virtual server that is bound to this content switching virtual server (specified by the Push VServer parameter). The service type of the push virtual server should be either HTTP or SSL. Possible values: ENABLED, DISABLED Default value: DISABLED

pushVserver

Name of the load balancing virtual server, of type PUSH or SSL_PUSH, to which the server pushes updates received on the client-facing load balancing virtual server.

pushLabel

Expression for extracting the label from the response received from server. This string can be either an existing rule name or an inline expression. The service type of the virtual server should be either HTTP or SSL. Default value: "none"

pushMultiClients

Allow multiple Web 2.0 connections from the same client to connect to the virtual server and expect updates. Possible values: YES, NO Default value: NO

tcpProfileName

Name of the TCP profile containing TCP configuration settings for the virtual server.

httpProfileName

Name of the HTTP profile containing HTTP configuration settings for the virtual server. The service type of the virtual server should be either HTTP or SSL.

dbProfileName

Name of the DB profile.

comment

Information about this virtual server.

l2Conn

Use L2 Parameters to identify a connection Possible values: ON, OFF

mssqlServerVersion

The version of the MSSQL server Possible values: 70, 2000, 2000SP1, 2005, 2008, 2008R2, 2012 Default value: TDS_PROT_2008B

mysqlProtocolVersion

The protocol version returned by the mysql vserver. Default value: 10

mysqlServerVersion

The server version string returned by the mysql vserver. Default value: NSA_MYSQL_SERVER_VER_DEFAULT

mysqlCharacterSet

The character set returned by the mysql vserver. Default value: 8

mysqlServerCapabilities

The server capabilities returned by the mysql vserver. Default value: 41613

appflowLog

Enable logging appflow flow information Possible values: ENABLED, DISABLED Default value: ENABLED

netProfile

The name of the network profile.

authnProfile

Name of the authentication profile to be used when authentication is turned on.

icmpVsrResponse

Can be active or passive Possible values: PASSIVE, ACTIVE Default value: NS_VSR_PASSIVE

[Top](#)

unset cs vserver

Synopsis

```
unset cs vserver <name> [-caseSensitive] [-backupVServer] [-cltTimeout] [-redirectURL]
[-authn401] [-Authentication] [-AuthenticationHost] [-authnVsName] [-pushVserver] [-
pushLabel] [-tcpProfileName] [-httpProfileName] [-dbProfileName] [-l2Conn] [-
mysqlProtocolVersion] [-mysqlServerVersion] [-mysqlCharacterSet] [-
mysqlServerCapabilities] [-appflowLog] [-netProfile] [-icmpVsrResponse] [-authnProfile]
[-stateupdate] [-precedence] [-cacheable] [-soMethod] [-soPersistence] [-
soPersistenceTimeOut] [-soThreshold] [-soBackupAction] [-redirectPortRewrite] [-
downStateFlush] [-disablePrimaryOnDown] [-insertVserverIPPort] [-vipHeader] [-
rtspNat] [-Listenpolicy] [-Listenpriority] [-push] [-pushMultiClients] [-comment] [-
mssqlServerVersion]
```

Description

Unset the parameters of a content switching virtual server..Refer to the set cs vserver command for meanings of the arguments.

[Top](#)

bind cs vserver

Synopsis

```
bind cs vserver <name> [-lbvserver <string> | (-policyName <string> [-targetLBVserver
<string>] [-priority <positive_integer>] [-gotoPriorityExpression <expression>] [-type
( REQUEST | RESPONSE )] [-invoke (<labelType> <labelName> ) ] )]
```

Description

Binds a content switching virtual server to a content switching policy.

Parameters

name

Name of the content switching virtual server to which the content switching policy applies.

lbvserver

Name of the default Load Balancing vserver bound. If for a particular content none of the Content Switching policies is evaluated to TRUE, that traffic is switched to default Load Balancing vserver. . Example: bind cs vserver cs1 -lbvserver lb1 Note: Use this parameter for default binding only.

policyName

Name of the content switching policy to bind to the content switching virtual server Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Cannot be changed after a policy is created. To bind a content switching policy, you need a content-based virtual server (content switching virtual server) and an address-based virtual server (load balancing virtual server). You can assign multiple policies to the virtual server pair. Note: When binding a CS virtual server to a default LB virtual server, the Policy Name parameter is optional. The following requirement applies only to the NetScaler CLI: If the name

includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy').

targetVserver

The virtual server name (created with the add lb vserver command) to which content will be switched.

Example

```
i) bind cs vserver csw-vip1 -policyname csw-
policy1 -priority 13
ii) bind cs vserver csw-vip2 -policyname csw-
ape-policy2 -priority 14 -gotoPriorityExpression
NEXT
iii) bind cs vserver csw-vip3 -policyname
rewrite-policy1 -priority 17 -
gotoPriorityExpression
'HTTP.REQ.HEADER("a").COUNT' -flowtype REQUEST -
invoke policylabel label1
```

[Top](#)

unbind cs vserver

Synopsis

```
unbind cs vserver <name> [(-policyName <string> [-type ( REQUEST | RESPONSE )]) | -
lbvserver <string>] [-priority <positive_integer>]
```

Description

Unbinds the virtual server from the content switching policy.

Parameters

name

Name of the virtual server to unbind from the policy.

policyName

Name of the policy from which to unbind the content switching virtual server. Note: To unbind the content switching virtual server from the default policy, do not specify a value for this parameter.

lbvserver

The virtual server name (created with the add lb vserver command) to which content will be switched. Default value: "default_lb"

[Top](#)

enable cs vserver

Synopsis

```
enable cs vserver <name>@
```

Description

Enables a content switching virtual server.

Parameters

name

Name of the content switching virtual server to enable. Note: Virtual servers, when added, are enabled by default.

Example

```
enable vserver cs_vip
```

[Top](#)

disable cs vserver

Synopsis

disable cs vserver <name>@

Description

Disables a content switching virtual server.

Parameters

name

Name of the virtual server to be disabled.

Example

```
disable vserver cs_vip
```

[Top](#)

show cs vserver

Synopsis

show cs vserver [<name>] show cs vserver stats - alias for 'stat cs vserver'

Description

Displays all existing content switching virtual servers, or just the specified virtual server.

Parameters

name

Name of a content switching virtual server for which to display information, including the policies bound to the virtual server. To display a list of all configured Content Switching virtual servers, do not specify a value for this parameter.

[Top](#)

stat cs vserver

Synopsis

```
stat cs vserver [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile  
<input_filename>] [-clearstats ( basic | full )]
```

Description

Displays statistics of all content switching virtual servers, or statistics for just the specified content switching virtual server.

Parameters

name

Name of the content switching virtual server for which to display statistics. To display statistics for all configured Content Switching virtual servers, do not specify a value for this parameter.

clearstats

Clear the statistics / counters Possible values: basic, full

[Top](#)

rename cs vserver

Synopsis

```
rename cs vserver <name>@ <newName>@
```

Description

Renames a content switching virtual server.

Parameters

name

Existing name of the content switching virtual server.

newName

New name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my name" or 'my name').

Example

```
rename cs vserver cs1 cs2
```

[Top](#)

cs parameter

[[set](#) | [unset](#) | [show](#)]

set cs parameter

Synopsis

```
set cs parameter -stateupdate ( ENABLED | DISABLED )
```

Description

Sets the status of the state update parameter for the server. By default, the content switching virtual server is always UP, regardless of the state of the load balancing virtual servers bound to it. This command enables the virtual server to check the status of the attached load balancing server for state information.

Parameters

stateupdate

Specifies whether the virtual server checks the attached load balancing server for state information. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

```
set cs parameter -stateupdate (ENABLED|DISABLED)
```

[Top](#)

unset cs parameter

Synopsis

```
unset cs parameter -stateupdate
```

Description

Use this command to remove cs parameter settings. Refer to the set cs parameter command for meanings of the arguments.

[Top](#)

show cs parameter

Synopsis

```
show cs parameter
```

Description

Show CS parameters

Example

```
show cs parameter
```

[Top](#)

cs action

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#) | [rename](#)]

add cs action

Synopsis

add cs action <name> (-targetLBVserver <string> | -targetVserverExpr <expression>) [-comment <string>]

Description

Creates an action that indicates the target load balancing virtual server. This action is used to specify the target load balancing virtual server while defining a policy to support multiple policy bind support.

Parameters

name

Name for the content switching action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the content switching action is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

targetLBVserver

Name of the load balancing virtual server to which the content is switched.

targetVserverExpr

Information about this content switching action.

comment

Comments associated with this cs action.

Example

```
add cs action -targetLBVserver act1 lb1
```

[Top](#)

rm cs action

Synopsis

```
rm cs action <name>
```

Description

Removes a content switching action.

Parameters

name

Name of the cs action.

Example

```
rm cs action act_before
```

[Top](#)

set cs action

Synopsis

```
set cs action <name> (-targetLBVserver <string> | -targetVserverExpr <expression>) [-comment <string>]
```

Description

Modifies the configuration settings of a content switching action.

Parameters

name

Name for the content switching action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the content switching action is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

targetLBVserver

Name of the load balancing virtual server to which the content is switched.

targetVserverExpr

Information about this content switching action.

comment

Comments associated with this cs action.

Example

```
set cs action act1 -targetLBVserver lb2 -comment  
'for url'
```

[Top](#)

unset cs action**Synopsis**

unset cs action <name> -comment

Description

Use this command to remove cs action settings. Refer to the set cs action command for meanings of the arguments.

[Top](#)

show cs action**Synopsis**

show cs action [<name>]

Description

Displays the configuration settings of the specified content switching action or lists all the content switching actions configured on the appliance.

Parameters

name

Name of the content switching action.

Example

```
show cs action
```

[Top](#)

rename cs action**Synopsis**

rename cs action <name>@ <newName>@

Description

Renames a content switching action.

Parameters

name

Existing name of the content switching action.

newName

New name for the content switching action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my name" or 'my name').

Example

```
rename cs action oldname newname
```

[Top](#)

DB Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [db user](#)
- ♦ [db dbProfile](#)

db user

[[add](#) | [rm](#) | [set](#) | [show](#)]

add db user

Synopsis

```
add db user <userName> {-password }
```

Description

Adds a database user. The user name and password that you specify in this command are added to the nsconfig file and used to authenticate the user.

Parameters

userName

Name of the database user. Must be the same as the user name specified in the database.

password

Password for logging on to the database. Must be the same as the password specified in the database.

Example

```
add db user johndoe -password secret
```

[Top](#)

rm db user

Synopsis

```
rm db user <userName>
```

Description

Removes a database user from the NetScaler appliance. Requests from the user are no longer authenticated or routed to the database server.

Parameters

userName

Name of the database user to remove.

[Top](#)

set db user

Synopsis

```
set db user <userName>
```

Description

Modifies the password of an existing database user.

Parameters

userName

Name of the database user.

password

The database users password. If you use the CLI, you are prompted for this password after specifying the user name.

Example

```
set db user johndoe
The above command sets the password for johndoe to
abcd (Password to be supplied on prompt)
```

[Top](#)

show db user

Synopsis

show db user [<userName>] [-loggedIn]

Description

Displays the specified database user or, if no user is specified, all the database users configured on the appliance.

Parameters

userName

Name of the database user.

loggedIn

Display the names of all database users currently logged on to the NetScaler appliance.

[Top](#)

db dbProfile

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add db dbProfile

Synopsis

add db dbProfile <name> [-interpretQuery (YES | NO)] [-stickiness (YES | NO)] [-kcdAccount <string>] [-conMultiplex (ENABLED | DISABLED)]

Description

Add a new DB profile on the Netscaler

Parameters

name

Name of the DB profile

interpretQuery

Enables/Disables Interpret Query Possible values: YES, NO Default value: YES

stickiness

Enables/Disables Stickyness of Query Possible values: YES, NO Default value: NO

kcdAccount

Enables/Disables KCD account

conMultiplex

Reuse server connections for requests from more than one client connections.
Possible values: ENABLED, DISABLED Default value: ENABLED

Example

```
add dbprofile <profile name> -interpretQuery YES -
stickyness YES -kcdaccount account
```

[Top](#)

rm db dbProfile

Synopsis

```
rm db dbProfile <name>
```

Description

Remove a DB profile on the Netscaler

Parameters

name
Name of the DB profile

Example

```
rm dbprofile <profile name>
```

[Top](#)

set db dbProfile

Synopsis

```
set db dbProfile <name> [-interpretQuery ( YES | NO )] [-stickiness ( YES | NO )] [-
kcdAccount <string>] [-conMultiplex ( ENABLED | DISABLED )]
```

Description

Set/modify DB profile values

Parameters

name
Name of the DB profile

interpretQuery
Enables/Disables Interpret Query Possible values: YES, NO Default value: YES

stickiness
Enables/Disables Stickyness of Query Possible values: YES, NO Default value: NO

kcdAccount
Enables/Disables KCD account

conMultiplex

Reuse server connections for requests from more than one client connections.
Possible values: ENABLED, DISABLED Default value: ENABLED

Example

```
set dbprofile <profile name> -interpretQuery YES -
stickyness YES
```

[Top](#)

unset db dbProfile**Synopsis**

```
unset db dbProfile <name> [-interpretQuery] [-stickiness] [-kcdAccount] [-conMultiplex]
```

Description

Unset DB profile values. Refer to the set db dbProfile command for meanings of the arguments.

[Top](#)

show db dbProfile**Synopsis**

```
show db dbProfile [<name>]
```

Description

Display all the configured DB profiles in the system. If a name is specified, then only that profile is shown.

Parameters**name**

Name of the DB profile.

Example

```
show dbprofile [profile name]
```

[Top](#)

DNS Commands

This group of commands can be used to perform operations on the following entities:

- ◆ [dns](#)

- ♦ [dns aaaaRec](#)
- ♦ [dns addRec](#)
- ♦ [dns txtRec](#)
- ♦ [dns cnameRec](#)
- ♦ [dns mxRec](#)
- ♦ [dns nsRec](#)
- ♦ [dns ptrRec](#)
- ♦ [dns srvRec](#)
- ♦ [dns soaRec](#)
- ♦ [dns suffix](#)
- ♦ [dns nameServer](#)
- ♦ [dns view](#)
- ♦ [dns policy](#)
- ♦ [dns action64](#)
- ♦ [dns policy64](#)
- ♦ [dns zone](#)
- ♦ [dns key](#)
- ♦ [dns proxyRecords](#)
- ♦ [dns records](#)
- ♦ [dns stats](#)
- ♦ [dns parameter](#)
- ♦ [dns policylabel](#)
- ♦ [dns global](#)
- ♦ [dns action](#)
- ♦ [dns nsecRec](#)

dns

stat dns

Synopsis

```
stat dns [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]  
[-clearstats ( basic | full )]
```

Description

Displays DNS statistics.

Parameters

clearstats

Clear the statistics / counters Possible values: basic, full

dns aaaaRec

[[add](#) | [rm](#) | [show](#)]

add dns aaaaRec

Synopsis

```
add dns aaaaRec <hostName> <IPv6Address> ... [-TTL <secs>]
```

Description

Creates a AAAA address record for the specified domain name. You cannot modify a AAAA address record.

Parameters

hostName

Domain name.

IPv6Address

One or more IPv6 addresses to assign to the domain name.

TTL

Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the NetScaler appliance uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Maximum value: 2147483647

Example

```
add dns aaaarec www.mynw.com 3::4:5 -ttl 10
```

[Top](#)

rm dns aaaaRec

Synopsis

```
rm dns aaaaRec <hostName> [<IPv6Address> ...]
```

Description

Removes an IPv6 address from a AAAA address record. The associated domain name must be specified. If no IPv6 address is specified, all AAAA records that belong to the specified domain name are removed.

Parameters

hostName

Domain name.

IPv6Address

IPv6 address(es) of the AAAA record(s) to remove from the specified domain name.

Example

```
rm dns aaaarec www.mynw.com
```

[Top](#)

show dns aaaRec

Synopsis

```
show dns aaaRec [<hostName> | -type <type>] [<IPv6Address>]
```

Description

Displays the AAAA (IPv6) address record for the specified host name. If a hostname is not specified, all configured AAAA records are shown.

Parameters

hostName

Domain name.

IPv6Address

One or more IPv6 addresses to assign to the domain name.

type

Type of records to display. Available settings function as follows: * ADNS - Display all authoritative address records. * PROXY - Display all proxy address records. * ALL - Display all address records. Possible values: ALL, ADNS, PROXY

[Top](#)

dns addRec

[[add](#) | [rm](#) | [show](#)]

add dns addRec

Synopsis

```
add dns addRec <hostName> <IPAddress> ... [-TTL <secs>]
```

Description

Creates an IPv4 address record for the specified domain name. You cannot modify an address resource record.

Parameters

hostName

Domain name.

IPAddress

One or more IPv4 addresses to assign to the domain name.

TTL

Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the NetScaler appliance uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Maximum value: 2147483647

Example

```
Add dns addrec www.mynw.com 65.200.211.139 -ttl 10
```

[Top](#)

rm dns addRec

Synopsis

```
rm dns addRec <hostName> [<IPAddress> ...]
```

Description

Removes an IPv4 address from an address record. The associated domain name must be specified. If no IPv4 address is specified, all records that belong to the specified domain name are removed.

Parameters

hostName

Domain name.

IPAddress

IPv4 address(es) of the address records to remove from the specified domain name.

Example

```
rm dns addrec www.mynw.com
```

[Top](#)

show dns addRec

Synopsis

show dns addRec [<hostName> | -type <type>]

Description

Displays the IPv4 address record for the specified host name. If a hostname is not specified, all configured address records are shown.

Parameters

hostName

Domain name.

type

The address record type. The type can take 3 values: ADNS - If this is specified, all of the authoritative address records will be displayed. PROXY - If this is specified, all of the proxy address records will be displayed. ALL - If this is specified, all of the address records will be displayed. Possible values: ALL, ADNS, PROXY

[Top](#)

dns txtRec

[[add](#) | [rm](#) | [show](#)]

add dns txtRec

Synopsis

add dns txtRec <domain> <string> ... [-TTL <secs>]

Description

Creates a text (TXT) record for the specified domain name. Each resource record is stored with a unique, internally generated record ID, which you can view and use to delete the record. You cannot modify a TXT resource record.

Parameters

domain

Name of the domain for the TXT record.

string

Information to store in the TXT resource record. Enclose the string in single or double quotation marks. A TXT resource record can contain up to six strings, each of which can contain up to 255 characters. If you want to add a string of more than 255 characters, evaluate whether splitting it into two or more smaller strings, subject to the six-string limit, works for you.

TTL

Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name.

For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the NetScaler appliance uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Maximum value: 2147483647

Example

```
add dns txtRec spf.m.test. "v=spf1 ip4:1.2.3.0/24
ip4:1.3.4.0/24 ?all"
add dns txtRec comments.m.test. "This is a
CHARSTR" "This is another CHARSTR"
```

[Top](#)

rm dns txtRec

Synopsis

```
rm dns txtRec <domain> (<string> ... | -recordId <positive_integer>@)
```

Description

Removes the specified TXT record from the specified domain.

Parameters

domain

Name of the domain for the TXT record.

string

Complete set of text strings in the TXT record, entered in the order in which they are stored in the record. Mutually exclusive with the record ID parameter.

recordId

Unique, internally generated record ID. View the details of the TXT record to obtain its record ID. Mutually exclusive with the string parameter. Minimum value: 1 Maximum value: 65535

Example

```
rm dns txtRec spf.m.test. "v=spf1 ip4:1.2.3.0/24
ip4:1.3.4.0/24 ?all"
rm dns txtRec comments.m.test. "This is a
CHARSTR" "This is another CHARSTR"
rm dns txtRec comments.m.test. -recordId 1411
```

[Top](#)

show dns txtRec

Synopsis

show dns txtRec [<domain> | -type <type>]

Description

Displays TXT records owned by the specified domain. If no domain name is specified, all configured TXT records are shown.

Parameters

domain

Name of the domain for the TXT record.

type

Type of records to display. Available settings function as follows: * ADNS - Display all authoritative address records. * PROXY - Display all proxy address records. * ALL - Display all address records. Possible values: ALL, ADNS, PROXY Default value: NSDNS_AUTH_HOST

Example

```
show dns txtRec spf.m.test.  
show dns txtRec
```

[Top](#)

dns cnameRec

[[add](#) | [rm](#) | [show](#)]

add dns cnameRec

Synopsis

add dns cnameRec <aliasName> <canonicalName> [-TTL <secs>]

Description

Creates a canonical name (CNAME) record, or alias, for the specified domain name.

Parameters

aliasName

Alias for the canonical domain name.

canonicalName

Canonical domain name.

TTL

Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name.

For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the NetScaler appliance uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Maximum value: 2147483647

Example

```
add dns cnameRec www.mynw.org www.mynw.com -ttl 20
```

[Top](#)

rm dns cnameRec

Synopsis

```
rm dns cnameRec <aliasName>
```

Description

Removes a canonical name (CNAME) record.

Parameters

aliasName

Alias for which to remove the CNAME record.

Example

```
rm dns cnamerec www.mynw.org
```

[Top](#)

show dns cnameRec

Synopsis

```
show dns cnameRec [<aliasName> | -type <type>]
```

Description

Displays the canonical name (CNAME) records configured for the specified alias. If no alias is specified, all configured CNAME records are displayed

Parameters

aliasName

Alias for which to display CNAME records.

type

Type of records to display. Available settings function as follows: * ADNS - Display all authoritative address records. * PROXY - Display all proxy address records. * ALL -

Display all address records. Possible values: ALL, ADNS, PROXY Default value: NSDNS_AUTH_HOST

Example

```
show dns cnameRec www.mynw.org
```

[Top](#)

dns mxRec

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add dns mxRec

Synopsis

```
add dns mxRec <domain> -mx <string> -pref <positive_integer> [-TTL <secs>]
```

Description

Creates a mail exchange (MX) record for the specified domain name.

Parameters

domain

Domain name for which to add the MX record.

mx

Host name of the mail exchange server.

pref

Priority number to assign to the mail exchange server. A domain name can have multiple mail servers, with a priority number assigned to each server. The lower the priority number, the higher the mail server's priority. When other mail servers have to deliver mail to the specified domain, they begin with the mail server with the lowest priority number, and use other configured mail servers, in priority order, as backups. Maximum value: 65535

TTL

Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the NetScaler appliance uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Maximum value: 2147483647

[Top](#)

rm dns mxRec

Synopsis

rm dns mxRec <domain> <mx>

Description

Removes the specified mail exchange (MX) record from the specified domain.

Parameters

domain

Domain name.

mx

Host name of the mail exchange server.

[Top](#)

set dns mxRec

Synopsis

set dns mxRec <domain> -mx <string> [-pref <positive_integer>] [-TTL <secs>]

Description

Modifies the priority number and TTL of the mail exchange (MX) record.

Parameters

domain

Domain of the MX record to be modified.

mx

Host name of the mail exchange server to be modified.

pref

Priority number to assign to the mail exchange server. A domain name can have multiple mail servers, with a priority number assigned to each server. The lower the priority number, the higher the mail server's priority. When other mail servers have to deliver mail to the specified domain, they begin with the mail server with the lowest priority number, and use other configured mail servers, in priority order, as backups. Maximum value: 65535

TTL

Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the NetScaler appliance uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Maximum value: 2147483647

[Top](#)

unset dns mxRec

Synopsis

unset dns mxRec <domain> -mx <string> -TTL

Description

Use this command to remove dns mxRec settings. Refer to the set dns mxRec command for meanings of the arguments.

[Top](#)

show dns mxRec

Synopsis

show dns mxRec [<domain> | -type <type>]

Description

Displays the mail exchange (MX) records for the specified domain. If no domain name is specified, all configured mail exchange records are shown.

Parameters

domain

Domain name.

type

Type of records to display. Available settings function as follows: * ADNS - Display all authoritative address records. * PROXY - Display all proxy address records. * ALL - Display all address records. Possible values: ALL, ADNS, PROXY Default value: NSDNS_AUTH_HOST

[Top](#)

dns nsRec

[[add](#) | [rm](#) | [show](#)]

add dns nsRec

Synopsis

add dns nsRec <domain> <nameServer> [-TTL <secs>]

Description

Creates a name server record for the specified domain.

Parameters

domain

Domain name.

nameServer

Host name of the name server to add to the domain.

TTL

Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the NetScaler appliance uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Maximum value: 2147483647

[Top](#)**rm dns nsRec****Synopsis**

```
rm dns nsRec <domain> <nameServer>
```

Description

Removes the specified name server record from the specified domain.

Parameters**domain**

Domain name.

nameServer

Name server to remove.

[Top](#)**show dns nsRec****Synopsis**

```
show dns nsRec [<domain> | -type <type>]
```

Description

Displays the name server records for the specified domain. If no domain name is specified, all configured name server records are shown.

Parameters**domain**

Domain name.

type

Type of records to display. Available settings function as follows: * ADNS - Display all authoritative address records. * PROXY - Display all proxy address records. * ALL - Display all address records. Possible values: ALL, ADNS, PROXY

[Top](#)

dns ptrRec

[[add](#) | [rm](#) | [show](#)]

add dns ptrRec

Synopsis

add dns ptrRec <reverseDomain> <domain> ... [-TTL <secs>]

Description

Creates a pointer (PTR) record for the specified reverse domain name.

Parameters

reverseDomain

Reversed domain name representation of the IPv4 or IPv6 address for which to create the PTR record. Use the "in-addr.arpa." suffix for IPv4 addresses and the "ip6.arpa." suffix for IPv6 addresses.

domain

Domain name for which to configure reverse mapping.

TTL

Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the NetScaler appliance uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Maximum value: 2147483647

Example

```
add dns ptrrec 1.1.1.in-addr.arpa. abc.com
```

[Top](#)

rm dns ptrRec

Synopsis

rm dns ptrRec <reverseDomain> [<domain> ...]

Description

Removes a pointer (PTR) record for the specified domain name and reverse domain name.

Parameters

reverseDomain

Reverse domain name of the PTR record.

domain

Domain name for which to remove reverse mapping.

Example

```
rm dns ptrrec 1.1.1.1.in-addr.arpa. ptr.com
```

[Top](#)

show dns ptrRec**Synopsis**

show dns ptrRec [<reverseDomain> | -type <type>]

Description

Displays the pointer (PTR) record for the specified reverse domain name and domain name.

Parameters**reverseDomain**

Reversed domain name representation of the IPv4 or IPv6 address for which to create the PTR record. Use the "in-addr.arpa." suffix for IPv4 addresses and the "ip6.arpa." suffix for IPv6 addresses.

type

Type of records to display. Available settings function as follows: * ADNS - Display all authoritative address records. * PROXY - Display all proxy address records. * ALL - Display all address records. Possible values: ALL, ADNS, PROXY

[Top](#)

dns srvRec

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add dns srvRec**Synopsis**

add dns srvRec <domain> <target> -priority <positive_integer> -weight <positive_integer> -port <positive_integer> [-TTL <secs>]

Description

Creates a service (SRV) record for the service offered by the specified target host, in the specified domain.

Parameters**domain**

Domain name, which, by convention, is prefixed by the symbolic name of the desired service and the symbolic name of the desired protocol, each with an underscore (_)

prepended. For example, if an SRV-aware client wants to discover a SIP service that is provided over UDP, in the domain example.com, the client performs a lookup for _sip._udp.example.com.

target

Target host for the specified service.

priority

Integer specifying the priority of the target host. The lower the number, the higher the priority. If multiple target hosts have the same priority, selection is based on the Weight parameter. Maximum value: 65535

weight

Weight for the target host. Aids host selection when two or more hosts have the same priority. A larger number indicates greater weight. Maximum value: 65535

port

Port on which the target host listens for client requests. Maximum value: 65535

TTL

Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the NetScaler appliance uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Maximum value: 2147483647

[Top](#)

rm dns srvRec

Synopsis

```
rm dns srvRec <domain> <target> ...
```

Description

Removes, from the specified domain, the SRV record created for the service provided by the specified target host.

Parameters

domain

Domain name of the SRV record.

target

Target host for the specified service.

[Top](#)

set dns srvRec

Synopsis

```
set dns srvRec <domain> <target> [-priority <positive_integer>] [-weight  
<positive_integer>] [-port <positive_integer>] [-TTL <secs>]
```

Description

Modifies the parameters of the specified service (SRV) record.

Parameters

domain

Name of the SRV record to be modified.

target

Target of the SRV record to be modified.

priority

Integer specifying the priority of the target host. The lower the number, the higher the priority. If multiple target hosts have the same priority, selection is based on the Weight parameter. Maximum value: 65535

weight

Weight for the target host. Aids host selection when two or more hosts have the same priority. A larger number indicates greater weight. Maximum value: 65535

port

Port on which the target host listens for client requests. Maximum value: 65535

TTL

Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the NetScaler appliance uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Maximum value: 2147483647

[Top](#)

unset dns srvRec

Synopsis

```
unset dns srvRec <domain> <target> -TTL
```

Description

Use this command to remove dns srvRec settings. Refer to the set dns srvRec command for meanings of the arguments.

[Top](#)

show dns srvRec

Synopsis

show dns srvRec [(**<domain>** [**<target>**])] | -type **<type>**]

Description

Displays the service (SRV) record configured for the specified target host and domain. If the domain name is not specified, all of the SRV records are shown.

Parameters

domain

Domain name for which to display the SRV record.

target

Target host for the specified service.

type

Type of records to display. Available settings function as follows: * ADNS - Display all authoritative address records. * PROXY - Display all proxy address records. * ALL - Display all address records. Possible values: ALL, ADNS, PROXY

[Top](#)

dns soaRec

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add dns soaRec

Synopsis

add dns soaRec **<domain>** -originServer **<string>** -contact **<string>** [-serial **<positive_integer>**] [-refresh **<secs>**] [-retry **<secs>**] [-expire **<secs>**] [-minimum **<secs>**] [-TTL **<secs>**]

Description

Creates a Start of Authority (SOA) record. Note: You can set the SOA parameters that are associated with zone transfers. However, the NetScaler appliance currently does not support zone transfers.

Parameters

domain

Domain name for which to add the SOA record.

originServer

Domain name of the name server that responds authoritatively for the domain.

contact

Email address of the contact to whom domain issues can be addressed. In the email address, replace the @ sign with a period (.). For example, enter domainadmin.example.com instead of domainadmin@example.com.

serial

The secondary server uses this parameter to determine whether it requires a zone transfer from the primary server. Default value: 100 Maximum value: 4294967294

refresh

Time, in seconds, for which a secondary server must wait between successive checks on the value of the serial number. Default value: 3600 Maximum value: 4294967294

retry

Time, in seconds, between retries if a secondary server's attempt to contact the primary server for a zone refresh fails. Default value: 3 Maximum value: 4294967294

expire

Time, in seconds, after which the zone data on a secondary name server can no longer be considered authoritative because all refresh and retry attempts made during the period have failed. After the expiry period, the secondary server stops serving the zone. Typically one week. Not used by the primary server. Default value: 3600 Maximum value: 4294967294

minimum

Default time to live (TTL) for all records in the zone. Can be overridden for individual records. Default value: 5 Maximum value: 2147483647

TTL

Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the NetScaler appliance uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Maximum value: 2147483647

[Top](#)

rm dns soaRec

Synopsis

```
rm dns soaRec <domain>
```

Description

Removes the Start of Authority (SOA) record for the specified domain name.

Parameters

domain

Domain name of the SOA record.

[Top](#)

set dns soaRec

Synopsis

```
set dns soaRec <domain> [-originServer <string>] [-contact <string>] [-serial  
<positive_integer>] [-refresh <secs>] [-retry <secs>] [-expire <secs>] [-minimum <secs>]  
[-TTL <secs>]
```

Description

Modifies the parameters of the specified Start Of Authority (SOA) record.

Parameters

domain

Domain of the SOA record to be modified.

originServer

Domain name of the name server that responds authoritatively for the domain.

contact

Email address of the contact to whom domain issues can be addressed. In the email address, replace the @ sign with a period (.). For example, enter domainadmin.example.com instead of domainadmin@example.com.

serial

The secondary server uses this parameter to determine whether it requires a zone transfer from the primary server. Default value: 100 Minimum value: 1 Maximum value: 4294967294

refresh

Time, in seconds, for which a secondary server must wait between successive checks on the value of the serial number. Default value: 3600 Maximum value: 4294967294

retry

Time, in seconds, between retries if a secondary server's attempt to contact the primary server for a zone refresh fails. Default value: 3 Maximum value: 4294967294

expire

Time, in seconds, after which the zone data on a secondary name server can no longer be considered authoritative because all refresh and retry attempts made during the period have failed. After the expiry period, the secondary server stops serving the zone. Typically one week. Not used by the primary server. Default value: 3600 Maximum value: 4294967294

minimum

Default time to live (TTL) for all records in the zone. Can be overridden for individual records. Default value: 5 Maximum value: 2147483647

TTL

Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the NetScaler appliance uses either the DNS zone's

minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Maximum value: 2147483647

[Top](#)

unset dns soaRec

Synopsis

```
unset dns soaRec <domain> [-serial] [-refresh] [-retry] [-expire] [-minimum] [-TTL]
```

Description

Use this command to remove dns soaRec settings. Refer to the set dns soaRec command for meanings of the arguments.

[Top](#)

show dns soaRec

Synopsis

```
show dns soaRec [<domain> | -type <type>]
```

Description

Displays the parameters of the specified Start of Authority (SOA) record. If no domain name is specified, all SOA records are displayed.

Parameters

domain

The domain name.

type

Type of records to display. Available settings function as follows: * ADNS - Display all authoritative address records. * PROXY - Display all proxy address records. * ALL - Display all address records. Possible values: ALL, ADNS, PROXY

[Top](#)

dns suffix

[[add](#) | [rm](#) | [show](#)]

add dns suffix

Synopsis

```
add dns suffix <dnsSuffix>
```

Description

Specifies a suffix that can be used to complete domain names that are not fully qualified. For example, if you specify the example.com suffix, and the NetScaler appliance is required to resolve the incomplete domain name "myhost," it attempts to resolve "myhost.example.com."

Parameters

dnsSuffix

Suffix to be appended when resolving domain names that are not fully qualified.

Example

```
add dns suffix netScaler.com
```

If the incoming domain name "engineering" is not resolved by itself, the system will append the suffix netScaler.com and attempt to resolve the name engineering.netScaler.com.

[Top](#)

rm dns suffix

Synopsis

```
rm dns suffix <dnsSuffix>
```

Description

Removes a DNS suffix.

Parameters

dnsSuffix

DNS suffix to remove.

[Top](#)

show dns suffix

Synopsis

```
show dns suffix [<dnsSuffix>]
```

Description

Displays the specified DNS suffix or, if no DNS suffix is specified, all configured DNS suffixes.

Parameters

dnsSuffix

DNS suffix to display.

[Top](#)

dns nameServer

[[add](#) | [rm](#) | [enable](#) | [disable](#) | [show](#)]

add dns nameServer

Synopsis

```
add dns nameServer ((<IP> [-local]) | <dnsVserverName>) [-state ( ENABLED |
DISABLED )] [-type <type>]
```

Description

Adds a name server to the appliance. Following are the two types of name servers that can be added:

- * IP address-based name server - An external name server to contact for domain name resolution. If multiple IP address-based name servers are configured on the appliance, and the local parameter is not set on any of them, incoming DNS queries are load balanced across all the name servers, in round robin fashion.
- * Virtual server-based name server - A DNS virtual server configured in the NetScaler appliance. If you want more fine-grained control on how external DNS name servers are load balanced (for example, you want a load balancing method other than round robin), you configure a DNS virtual server on the appliance, bind the external name servers as its services, and then specify the name of the virtual server in this command.

Parameters

IP

IP address of an external name server or, if the Local parameter is set, IP address of a local DNS server (LDNS).

dnsVserverName

Name of a DNS virtual server. Overrides any IP address-based name servers configured on the NetScaler appliance.

local

Mark the IP address as one that belongs to a local recursive DNS server on the NetScaler appliance. The appliance recursively resolves queries received on an IP address that is marked as being local. For recursive resolution to work, the global DNS parameter, Recursion, must also be set. If no name server is marked as being local, the appliance functions as a stub resolver and load balances the name servers.

state

Administrative state of the name server. Possible values: ENABLED, DISABLED Default value: ENABLED

type

Protocol used by the name server. UDP_TCP is not valid if the name server is a DNS virtual server configured on the appliance. Possible values: UDP, TCP, UDP_TCP Default value: NSA_UDP

Example

```
Adding an-IP based nameserver IP:
  add nameserver 10.102.4.1,
Adding a vsrver-based name server:
  add nameserver dns_vsvr
```

```
where dns_vsvr is the name of a DNS vserver
created in the system.
```

[Top](#)

rm dns nameServer

Synopsis

```
rm dns nameServer (<IP> | <dnsVserverName>)
```

Description

Removes a name server from the NetScaler appliance. If the name server is an IP-address based external name server, the name server entry is removed. If the name server is a DNS virtual server on the appliance, the virtual server is not removed, but it is no longer used to resolve domain names.

Parameters

IP

IP address of the name server.

dnsVserverName

Name of the DNS virtual server.

Example

```
Deleting an IP-based nameserver:
rm nameserver 10.102.4.1,
Deleting a vserver-based nameserver:
rm nameserver dns_vsvr
```

[Top](#)

enable dns nameServer

Synopsis

```
enable dns nameServer (<IP> | <dnsVserverName>)
```

Description

Enables a name server.

Parameters

IP

IP address of the name server.

dnsVserverName

Name of the DNS virtual server.

Example

```
enable dns nameserver 10.14.43.149
```

[Top](#)**disable dns nameServer****Synopsis**

disable dns nameServer (<IP> | <dnsVserverName>)

Description

Disables a name server.

Parameters**IP**

IP address of the name server.

dnsVserverName

Name of the DNS virtual server.

Example

```
disable dns nameserver 10.14.43.149
```

[Top](#)**show dns nameServer****Synopsis**

show dns nameServer [<IP> | <dnsVserverName>]

Description

Displays the name servers configured on the NetScaler appliance, along with their administrative states.

Parameters**IP**

IP address of the name server.

dnsVserverName

Name of the DNS virtual server.

[Top](#)**dns view**

[[add](#) | [rm](#) | [show](#)]

add dns view

Synopsis

add dns view <viewName>

Description

Creates a DNS view. A DNS view is used in global server load balancing (GSLB) to return a predetermined IP address to a specific group of clients, which are identified by using a DNS policy.

Parameters

viewName

Name for the DNS view.

Example

```
add dns view privateview
```

[Top](#)

rm dns view

Synopsis

rm dns view <viewName>

Description

Removes a DNS view.

Parameters

viewName

Name for the DNS view.

Example

```
rm dns view privateview
```

[Top](#)

show dns view

Synopsis

show dns view [<viewName>]

Description

Displays the specified DNS view or, if no DNS view name is specified, all the DNS views configured on the NetScaler appliance.

Parameters

viewName

Name of the view to display.

[Top](#)

dns policy

[[add](#) | [rm](#) | [set](#) | [show](#)]

add dns policy

Synopsis

add dns policy <name> <rule> <actionName>

Description

Creates a DNS policy.

Parameters

name

Name for the DNS policy.

rule

Expression against which DNS traffic is evaluated. Written in the default syntax.

Note: * On the command line interface, if the expression includes blank spaces, the entire expression must be enclosed in double quotation marks. * If the expression itself includes double quotation marks, you must escape the quotations by using the character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks. Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>" Example: CLIENT.UDP.DNS.DOMAIN.EQ("domainname")

viewName

The view name that must be used for the given policy.

preferredLocation

The location used for the given policy. This is deprecated attribute. Please use - prefLocList

preferredLocList

The location list in priority order used for the given policy.

drop

The dns packet must be dropped. Possible values: YES, NO

cacheBypass

By pass dns cache for this. Possible values: YES, NO

actionName

Name of the DNS action to perform when the rule evaluates to TRUE. The built in actions function as follows: * `dns_default_act_Drop`. Drop the DNS request. * `dns_default_act_Cachebypass`. Bypass the DNS cache and forward the request to the name server. You can create custom actions by using the `add dns action` command in the CLI or the DNS > Actions > Create DNS Action dialog box in the NetScaler configuration utility.

Example

```
add dns policy pol1
"dns.req.question.type.ne(aaaa)" -actionName act1
add dns policy pol2
"CLIENT.IP.SRC.IN_SUBNET(1.1.1.1/24)" -actionName
action1
add dns policy pol1
dns.res.question.domain.contains("citrix") -
actionName act2
```

[Top](#)

rm dns policy

Synopsis

`rm dns policy <name>`

Description

Removes a DNS policy.

Parameters

name

Name of the DNS policy to remove.

[Top](#)

set dns policy

Synopsis

`set dns policy <name> [<rule>] [-actionName <string>]`

Description

Modifies the parameters of the specified DNS policy.

Parameters

name

Name of the DNS policy.

rule

Expression against which DNS traffic is evaluated. Written in the default syntax.

Note: * On the command line interface, if the expression includes blank spaces, the

entire expression must be enclosed in double quotation marks. * If the expression itself includes double quotation marks, you must escape the quotations by using the character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks. Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>" Example: CLIENT.UDP.DNS.DOMAIN.EQ("domainname")

viewName

The view name that must be used for the given policy

preferredLocation

The location used for the given policy. This is deprecated attribute. Please use - prefLocList

preferredLocList

The location list in priority order used for the given policy.

drop

The dns packet must be dropped. Possible values: YES, NO

cacheBypass

By pass dns cache for this. Possible values: YES, NO

actionName

Name of the DNS action to perform when the rule evaluates to TRUE. The built in actions function as follows: * dns_default_act_Drop. Drop the DNS request. * dns_default_act_Cachebypass. Bypass the DNS cache and forward the request to the name server. You can create custom actions by using the add dns action command in the CLI or the DNS > Actions > Create DNS Action dialog box in the NetScaler configuration utility.

Example

```
set dns policy pol1 -rule
"dns.req.question.type.ne (aaaa) "
set dns policy pol2 -rule
"CLIENT.IP.SRC.IN_SUBNET(1.1.1.1/24) "
set dns policy pol1 -rule
dns.res.header.rcode.eq (nxdomain)
```

[Top](#)

show dns policy**Synopsis**

show dns policy [<name>]

Description

Displays the parameters of the specified DNS policy or, if no policy name is specified, all configured DNS policies.

Parameters

name

Name of the DNS policy.

[Top](#)

dns action64

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add dns action64

Synopsis

add dns action64 <actionName> -Prefix <ipv6_addr|*> [-mappedRule <expression>] [-excludeRule <expression>]

Description

Add a dns64 action.

Parameters

actionName

Name of the dns64 action.

Prefix

The dns64 prefix to be used if the after evaluating the rules

mappedRule

The expression to select the criteria for ipv4 addresses to be used for synthesis. Only if the mappedrule is evaluated to true the corresponding ipv4 address is used for synthesis using respective prefix, otherwise the A RR is discarded

excludeRule

The expression to select the criteria for eliminating the corresponding ipv6 addresses from the response.

Example

```
add dns dns64action <actionName> -prefix
f23d:f43e::0/32 [-mappedRule <expr>] [-excludeRule
<expr>]
```

[Top](#)

rm dns action64

Synopsis

rm dns action64 <actionName>

Description

Removes a dns64 Action.

Parameters

actionName

Name of the dns64 action.

Example

```
rm dns dns64action action1
```

[Top](#)

set dns action64

Synopsis

set dns action64 <actionName> [-Prefix <ipv6_addr|*>] [-mappedRule <expression>] [-excludeRule <expression>]

Description

Set a DNS64 Action

Parameters

actionName

Name of the dns64 action.

Prefix

The dns64 prefix to be used if the after evaluating the rules

mappedRule

The expression to select the criteria for ipv4 addresses to be used for synthesis. Only if the mappedrule is evaluated to true the corresponding ipv4 address is used for synthesis using respective prefix, otherwise the A RR is discarded

excludeRule

The expression to select the criteria for eliminating the corresponding ipv6 addresses from the response.

Example

```
set dns dns64action -prefix -mappedrule -  
excluderule
```

[Top](#)

unset dns action64

Synopsis

unset dns action64 <actionName> [-Prefix] [-mappedRule] [-excludeRule]

Description

Use this command to remove dns action64 settings. Refer to the set dns action64 command for meanings of the arguments.

[Top](#)

show dns action64

Synopsis

show dns action64 [<actionName>]

Description

Used to display the action-related information.

Parameters

actionName

Name of the dns64 action.

Example

```
show dns dns64action
```

[Top](#)

dns policy64

[[add](#) | [rm](#) | [set](#) | [show](#)]

add dns policy64

Synopsis

add dns policy64 <name> -rule <expression> -action <string>

Description

Creates a DNS64 Policy.

Parameters

name

Name for the DNS64 policy.

rule

Expression against which DNS traffic is evaluated. Written in the default syntax.

Note: * On the command line interface, if the expression includes blank spaces, the

entire expression must be enclosed in double quotation marks. * If the expression itself includes double quotation marks, you must escape the quotations by using the character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks. Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>" Example:
CLIENT.IP.SRC.IN_SUBNET(23.34.0.0/16)

action

Name of the DNS64 action to perform when the rule evaluates to TRUE. The built in actions function as follows: * A default dns64 action with prefix <default prefix> and mapped and exclude are any You can create custom actions by using the add dns action command in the CLI or the DNS64 > Actions > Create DNS64 Action dialog box in the NetScaler configuration utility.

Example

```
add dns64 policy poll
"client.ip.src.in_subnet(23.43.0.0/16)" -action
act1
```

[Top](#)

rm dns policy64

Synopsis

```
rm dns policy64 <name>
```

Description

Removes a DNS64 Policy.

Parameters

name
Name of the DNS64 policy to be removed.

[Top](#)

set dns policy64

Synopsis

```
set dns policy64 <name> [-rule <expression>] [-action <string>]
```

Description

Modifies the parameters of the specified DNS64 policy.

Parameters

name

Name of the DNS policy.

rule

Expression against which DNS traffic is evaluated. Written in the default syntax.

Note: * On the command line interface, if the expression includes blank spaces, the entire expression must be enclosed in double quotation marks. * If the expression itself includes double quotation marks, you must escape the quotations by using the character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks. Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>" Example:

CLIENT.IP.SRC.IN_SUBNET(23.34.0.0/16)

action

Name of the DNS64 action to perform when the rule evaluates to TRUE. The built in actions function as follows: * A default dns64 action with prefix <default prefix> and mapped and exclude are any You can create custom actions by using the add dns action command in the CLI or the DNS64 > Actions > Create DNS64 Action dialog box in the NetScaler configuration utility.

Example

```
set dns policy pol2 -rule
"CLIENT.IP.SRC.IN_SUBNET(1.1.1.1/24) "
```

[Top](#)

show dns policy64

Synopsis

show dns policy64 [<name>]

Description

Displays the parameters of the specified DNS64 policy or, if no policy name is specified, all configured DNS64 policies.

Parameters

name

Name of the DNS64 policy.

[Top](#)

dns zone

[[add](#) | [set](#) | [unset](#) | [rm](#) | [sign](#) | [unsign](#) | [show](#)]

add dns zone

Synopsis

```
add dns zone <zoneName> -proxyMode ( YES | NO ) [-dnssecOffload ( ENABLED |  
DISABLED ) [-nsec ( ENABLED | DISABLED )]]
```

Description

Creates a DNS zone on the NetScaler appliance. Mandatory if you want to use the appliance to implement Domain Name Security Extensions (DNSSEC) for the zone. When you add a DNS resource record, if the domain name of the record belongs to the zone, the record is automatically added to the zone.

Parameters

zoneName

Name of the zone to create.

proxyMode

Deploy the zone in proxy mode. Enable in the following scenarios: * The load balanced DNS servers are authoritative for the zone and all resource records that are part of the zone. * The load balanced DNS servers are authoritative for the zone, but the NetScaler appliance owns a subset of the resource records that belong to the zone (partial zone ownership configuration). Typically seen in global server load balancing (GSLB) configurations, in which the appliance responds authoritatively to queries for GSLB domain names but forwards queries for other domain names in the zone to the load balanced servers. In either scenario, do not create the zone's Start of Authority (SOA) and name server (NS) resource records on the appliance. Disable if the appliance is authoritative for the zone, but make sure that you have created the SOA and NS records on the appliance before you create the zone. Possible values: YES, NO Default value: ENABLED

Example

```
add dns zone foo.bar -proxyMode NO -dnssec ENABLED
```

[Top](#)

set dns zone

Synopsis

```
set dns zone <zoneName> [-proxyMode ( YES | NO )] [-dnssecOffload ( ENABLED |  
DISABLED )] [-nsec ( ENABLED | DISABLED )]
```

Description

Modifies the parameters of the specified DNS zone.

Parameters

zoneName

Name of the zone.

proxyMode

Deploy the zone in proxy mode. Enable in the following scenarios: * The load balanced DNS servers are authoritative for the zone and all resource records that are part of the zone. * The load balanced DNS servers are authoritative for the zone, but the NetScaler appliance owns a subset of the resource records that belong to the zone (partial zone ownership configuration). Typically seen in global server load balancing (GSLB) configurations, in which the appliance responds authoritatively to queries for GSLB domain names but forwards queries for other domain names in the zone to the load balanced servers. In either scenario, do not create the zone's Start of Authority (SOA) and name server (NS) resource records on the appliance. Disable if the appliance is authoritative for the zone, but make sure that you have created the SOA and NS records on the appliance before you create the zone. Possible values: YES, NO Default value: ENABLED

Example

```
set dns zone foo.bar -proxyMode NO -dnssec ENABLED
```

[Top](#)**unset dns zone****Synopsis**

```
unset dns zone <zoneName> [-proxyMode] [-dnssecOffload] [-nsec]
```

Description

Use this command to remove dns zone settings. Refer to the set dns zone command for meanings of the arguments.

[Top](#)**rm dns zone****Synopsis**

```
rm dns zone <zoneName>
```

Description

Removes a DNS zone from the NetScaler appliance.

Parameters

zoneName

Name of the zone to remove.

[Top](#)**sign dns zone****Synopsis**

```
sign dns zone <zoneName> [-keyName <string> ...]
```

Description

Signs a DNS zone with a DNS key. Before you sign a zone, make sure that you've enabled DNSSEC by setting the global DNS parameter "Enable DNSSEC extension."

Parameters

zoneName

Name of the zone.

keyName

Name of the public/private DNS key pair with which to sign the zone. You can sign a zone with up to four keys.

Example

```
sign dns zone abc.com. -keyname abc.com.zsk
abc.com.ksk
```

[Top](#)

unsign dns zone

Synopsis

```
unsign dns zone <zoneName> [-keyName <string> ...]
```

Description

Unsigns the specified DNS zone with the specified DNS key.

Parameters

zoneName

Name of the zone.

keyName

Name of the public-private DNS key pair with which to unsign the zone.

Example

```
unsign dns zone abc.com. -keyname abc.com.zsk
abc.com.ksk
```

[Top](#)

show dns zone

Synopsis

```
show dns zone [<zoneName> | -type <type>]
```

Description

Displays the parameters of the specified DNS zone, along with information about the types of resource records available for each domain name in the zone. If no zone name is specified, just the parameters are shown, for all configured zones.

Parameters

zoneName

Name of the zone. Mutually exclusive with the type parameter.

type

Type of zone to display. Mutually exclusive with the DNS Zone (zoneName) parameter. Available settings function as follows: * ADNS - Display all the zones for which the NetScaler appliance is authoritative. * PROXY - Display all the zones for which the NetScaler appliance is functioning as a proxy server. * ALL - Display all the zones configured on the appliance. Possible values: ALL, ADNS, PROXY

Example

```
show dns zone foo.bar
```

[Top](#)

dns key

[[add](#) | [create](#) | [set](#) | [unset](#) | [rm](#) | [show](#)]

add dns key

Synopsis

```
add dns key <keyName> <publickey> <privatekey> [-expires <positive_integer>
[<units>]] [-notificationPeriod <positive_integer> [<units>]] [-TTL <secs>]
```

Description

Adds a DNS key to the zone that is specified in the key file.

Parameters

keyName

Name of the public-private key pair to publish in the zone.

publickey

File name of the public key.

privatekey

File name of the private key.

expires

Time period for which to consider the key valid, after the key is used to sign a zone. Default value: 120 Minimum value: 1 Maximum value: 32767

notificationPeriod

Time at which to generate notification of key expiration, specified as number of days, hours, or minutes before expiry. Must be less than the expiry period. The notification is an SNMP trap sent to an SNMP manager. To enable the appliance to send the trap, enable the DNSKEY-EXPIRY SNMP alarm. Default value: 7 Minimum value: 1 Maximum value: 32767

TTL

Time to Live (TTL), in seconds, for the DNSKEY resource record created in the zone. TTL is the time for which the record must be cached by the DNS proxies. If the TTL is not specified, either the DNS zone's minimum TTL or the default value of 3600 is used. Default value: 3600 Maximum value: 2147483647

Example

```
add dns key secure.example.zsk -public
secure.example-rsasha1-1024.key
-private /nsconfig/dns/secure.example-
rsasha1-1024.private
```

[Top](#)

create dns key**Synopsis**

```
create dns key -zoneName <string> -keyType <keyType> -algorithm RSASHA1 -keySize
<positive_integer> -fileNamePrefix <string>
```

Description

Creates a public-private key pair to use for signing a DNS zone. The keys are created in the /nsconfig/dns/ directory on the NetScaler appliance. The private, public, and DS key files are created with names having the format <prefix>.<key/private/ds>.

Parameters**zoneName**

Name of the zone for which to create a key.

keyType

Type of key to create. Possible values: KSK, KeySigningKey, ZSK, ZoneSigningKey
Default value: NS_DNSKEY_ZSK

algorithm

Algorithm to generate for zone signing. Possible values: RSASHA1 Default value: NS_DNSKEYALGO_RSASHA1

keySize

Size of the key, in bits. Default value: 512

fileNamePrefix

Common prefix for the names of the generated public and private key files and the Delegation Signer (DS) resource record. During key generation, the .key, .private,

and .ds suffixes are appended automatically to the file name prefix to produce the names of the public key, the private key, and the DS record, respectively.

Example

```
create dns key -zone dnssec.bar -algorithm RSASHA1
-keySize 1024
```

[Top](#)

set dns key

Synopsis

```
set dns key <keyName> [-expires <positive_integer> [<units>]] [-notificationPeriod
<positive_integer> [<units>]] [-TTL <secs>]
```

Description

Modifies the specified parameters of a DNS key. Note: If you change the expiry time period of a key, the NetScaler appliance, using the modified key, automatically re-signs all the resource records in the zone, provided that the zone is currently signed with the particular key.

Parameters

keyName

Name of the public-private key pair.

expires

Time period for which to consider the key valid, after the key is used to sign a zone. Default value: 120 Minimum value: 1 Maximum value: 32767

notificationPeriod

Time at which to generate notification of key expiration, specified as number of days, hours, or minutes before expiry. Must be less than the expiry period. The notification is an SNMP trap sent to an SNMP manager. To enable the appliance to send the trap, enable the DNSKEY-EXPIRY SNMP alarm. Default value: 7 Minimum value: 1 Maximum value: 32767

TTL

Time to Live (TTL), in seconds, for the DNSKEY resource record created in the zone. TTL is the time for which the record must be cached by the DNS proxies. If the TTL is not specified, either the DNS zone's minimum TTL or the default value of 3600 is used. Default value: 3600 Maximum value: 2147483647

Example

```
add dns key secure.example.zsk -public
secure.example-rsasha1-1024.key
```



```
-private /nsconfig/dns/secure.example-  
rsasha1-1024.private
```

[Top](#)

unset dns key

Synopsis

```
unset dns key <keyName> [-expires] [-units] [-notificationPeriod] [-units] [-TTL]
```

Description

Use this command to remove dns key settings. Refer to the set dns key command for meanings of the arguments.

[Top](#)

rm dns key

Synopsis

```
rm dns key <keyName>
```

Description

Removes a DNS key.

Parameters

keyName

Name of the public-private key pair.

Example

```
rm dns key secure.example.zsk
```

[Top](#)

show dns key

Synopsis

```
show dns key [<keyName>]
```

Description

Displays the parameters of the specified DNS key. If no DNS key name is specified, all configured DNS keys are shown. Note: You cannot view the parameters of a public/private key file. You can view the parameters of a key after you have published it in a DNS zone by using either the add dns key command or the DNS > Zones > Sign/Unsign DNS Zone dialog box.

Parameters

keyName

Name of the public-private key pair.

Example

```
show dns key
```

[Top](#)

dns proxyRecords

flush dns proxyRecords

Synopsis

flush dns proxyRecords

Description

Flushes all the proxy records from the DNS cache on the NetScaler appliance.

dns records

stat dns records

Synopsis

stat dns records [<dnsRecordType>] [-detail] [-fullValues] [-ntimes <positive_integer>]
[-logFile <input_filename>] [-clearstats (basic | full)]

Description

Displays statistics for the specified DNS record or query type. If a DNS record or query type is not specified, statistics for all record and query types are shown.

Parameters

dnsRecordType

Display statistics for the specified DNS record or query type or, if a record or query type is not specified, statistics for all record types supported on the NetScaler appliance.

clearstats

Clear the statistics / counters Possible values: basic, full

dns stats

show dns stats

Synopsis

show dns stats - alias for 'stat dns'

Description

show dns stats is an alias for stat dns

dns parameter

[[set](#) | [unset](#) | [show](#)]

set dns parameter

Synopsis

set dns parameter [-retries <positive_integer>] [-minTTL <secs>] [-maxTTL <secs>] [-cacheRecords (YES | NO)] [-nameLookupPriority (WINS | DNS)] [-recursion (ENABLED | DISABLED)] [-resolutionOrder <resolutionOrder>] [-dnssec (ENABLED | DISABLED)] [-maxPipeline <positive_integer>] [-dnsRootReferral (ENABLED | DISABLED)] [-dns64Timeout <msecs>]

Description

Modifies global DNS parameters on the NetScaler appliance.

Parameters

retries

Maximum number of retry attempts when no response is received for a query sent to a name server. Applies to end resolver and forwarder configurations. Default value: 5
Minimum value: 1 Maximum value: 5

minTTL

Minimum permissible time to live (TTL) for all records cached in the DNS cache by DNS proxy, end resolver, and forwarder configurations. If the TTL of a record that is to be cached is lower than the value configured for minTTL, the TTL of the record is set to the value of minTTL before caching. When you modify this setting, the new value is applied only to those records that are cached after the modification. The TTL values of existing records are not changed. Maximum value: 604800

maxTTL

Maximum time to live (TTL) for all records cached in the DNS cache by DNS proxy, end resolver, and forwarder configurations. If the TTL of a record that is to be cached is higher than the value configured for maxTTL, the TTL of the record is set to the value of maxTTL before caching. When you modify this setting, the new value is applied only to those records that are cached after the modification. The TTL values of existing records are not changed. Default value: 604800 Minimum value: 1 Maximum value: 604800

cacheRecords

Cache resource records in the DNS cache. Applies to resource records obtained through proxy configurations only. End resolver and forwarder configurations always

cache records in the DNS cache, and you cannot disable this behavior. When you disable record caching, the appliance stops caching server responses. However, cached records are not flushed. The appliance does not serve requests from the cache until record caching is enabled again. Possible values: YES, NO Default value: YES

nameLookupPriority

Type of lookup (DNS or WINS) to attempt first. If the first-priority lookup fails, the second-priority lookup is attempted. Used only by the SSL VPN feature. Possible values: WINS, DNS Default value: NS_WINSFIRST

recursion

Function as an end resolver and recursively resolve queries for domains that are not hosted on the NetScaler appliance. Also resolve queries recursively when the external name servers configured on the appliance (for a forwarder configuration) are unavailable. When external name servers are unavailable, the appliance queries a root server and resolves the request recursively, as it does for an end resolver configuration. Possible values: ENABLED, DISABLED Default value: DISABLED

resolutionOrder

Type of DNS queries (A, AAAA, or both) to generate during the routine functioning of certain NetScaler features, such as SSL VPN, cache redirection, and the integrated cache. The queries are sent to the external name servers that are configured for the forwarder function. If you specify both query types, you can also specify the order. Available settings function as follows: * OnlyAQuery. Send queries for IPv4 address records (A records) only. * OnlyAAAAQuery. Send queries for IPv6 address records (AAAA records) instead of queries for IPv4 address records (A records). * AThenAAAAQuery. Send a query for an A record, and then send a query for an AAAA record if the query for the A record results in a NODATA response from the name server. * AAAAThenAQuery. Send a query for an AAAA record, and then send a query for an A record if the query for the AAAA record results in a NODATA response from the name server. Possible values: OnlyAQuery, OnlyAAAAQuery, AThenAAAAQuery, AAAAThenAQuery Default value: NS_FOUR

dnssec

Enable or disable the Domain Name System Security Extensions (DNSSEC) feature on the appliance. Note: Even when the DNSSEC feature is enabled, forwarder configurations (used by internal NetScaler features such as SSL VPN and Cache Redirection for name resolution) do not support the DNSSEC OK (DO) bit in the EDNS0 OPT header. Possible values: ENABLED, DISABLED Default value: ENABLED

maxPipeline

Maximum number of concurrent DNS requests to allow on a single client connection, which is identified by the <clientip:port>-<server ip:port> tuple. A value of 0 (zero) applies no limit to the number of concurrent DNS requests allowed on a single client connection. Default value: NSNATPCB_MAXPIPELINE

dnsRootReferral

Send a root referral if a client queries a domain name that is unrelated to the domains configured/cached on the NetScaler appliance. If the setting is disabled, the appliance sends a blank response instead of a root referral. Applicable to domains for which the appliance is authoritative. Disable the parameter when the appliance is

under attack from a client that is sending a flood of queries for unrelated domains.
Possible values: ENABLED, DISABLED Default value: DISABLED

dns64Timeout

While doing DNS64 resolution, this parameter specifies the time to wait before sending an A query if no response is received from backend DNS server for AAAA query. Default value: VAL_NOT_SET Maximum value: 10000

[Top](#)

unset dns parameter**Synopsis**

```
unset dns parameter [-retries] [-minTTL] [-maxTTL] [-cacheRecords] [-  
nameLookupPriority] [-recursion] [-resolutionOrder] [-dnssec] [-maxPipeline] [-  
dnsRootReferral] [-dns64Timeout]
```

Description

Use this command to remove dns parameter settings. Refer to the set dns parameter command for meanings of the arguments.

[Top](#)

show dns parameter**Synopsis**

```
show dns parameter
```

Description

Displays the global DNS parameters.

[Top](#)

dns policylabel

[[add](#) | [rm](#) | [bind](#) | [unbind](#) | [show](#) | [stat](#) | [rename](#)]

add dns policylabel**Synopsis**

```
add dns policylabel <labelName> <transform>
```

Description

Add a dns policy label.

Parameters

labelName

Name of the dns policy label.

transform

The type of transformations allowed by the policies bound to the label. Possible values: dns_req, dns_res

Example

```
add dns policylabel trans_dns dns_req
```

[Top](#)

rm dns policylabel**Synopsis**

```
rm dns policylabel <labelName>
```

Description

Remove a dns policy label.

Parameters

labelName

Name of the dns policy label.

Example

```
rm dns policylabel trans_dns
```

[Top](#)

bind dns policylabel**Synopsis**

```
bind dns policylabel <labelName> <policyName> <priority> [<gotoPriorityExpression>] [-  
invoke (<labelType> <labelName>)]
```

Description

Bind the dns policy to one of the labels.

Parameters

labelName

Name of the dns policy label.

policyName

The dns policy name.

Example

```
i)    bind dns policylabel trans_dns pol_1 1 2 -  
invoke reqvserver CURRENT  
ii)   bind rewrite policylabel trans_http_url  
pol_2 2
```

[Top](#)

unbind dns policylabel

Synopsis

unbind dns policylabel <labelName> <policyName> [-priority <positive_integer>]

Description

Unbind entities from dns label.

Parameters**labelName**

Name of the dns policy label.

policyName

The dns policy name.

priority

Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

```
unbind dns policylabel trans_dns pol_1
```

[Top](#)

show dns policylabel

Synopsis

show dns policylabel [<labelName>]

Description

Display policy label or policies bound to dns policylabel.

Parameters**labelName**

Name of the dns policy label.

Example

```
i)      show dns policylabel trans_dns
ii)     show dns policylabel
```

[Top](#)

stat dns policylabel

Synopsis

```
stat dns policylabel [<labelName>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-clearstats ( basic | full )]
```

Description

Display statistics of dns policylabel(s).

Parameters

labelName

The name of the dns policy label for which statistics will be displayed. If not given statistics are shown for all dns policylabels.

clearstats

Clear the statistics / counters Possible values: basic, full

[Top](#)

rename dns policylabel

Synopsis

```
rename dns policylabel <labelName>@ <newName>@
```

Description

Rename a dns policy label.

Parameters

labelName

The name of the dns policylabel.

newName

The new name of the dns policylabel.

Example

```
rename dns policylabel oldname newname
```

[Top](#)

dns global

[[bind](#) | [unbind](#) | [show](#)]

bind dns global

Synopsis

```
bind dns global <policyName> <priority> [-gotoPriorityExpression <string>] [-type <type>] [-invoke (<labelType> <labelName>)]
```

Description

Binds the specified DNS policy globally.

Parameters

policyName

Name of the DNS policy to bind globally.

Example

```
bind dns global pol9 9
```

[Top](#)

unbind dns global

Synopsis

```
unbind dns global <policyName>
```

Description

Unbinds the specified DNS policy from the global bind point.

Parameters

policyName

Name of the DNS policy to unbind.

Example

```
unbind dns global pol9
```

[Top](#)

show dns global

Synopsis

```
show dns global [-type <type>]
```

Description

Displays the DNS policies bound to the specified global bind point. If a global bind point is not specified, the command displays the global bind points that have policies bound to them, and the number of policies bound to each of those bind points.

Parameters

type

Type of global bind point for which to show bound policies. Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT

Example

```
show dns global
show dns global -type REQ_DEFAULT
show dns global -type RES_DEFAULT
```

[Top](#)

dns action

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add dns action

Synopsis

add dns action <actionName> <actionType> [-IPAddress <ip_addr|ipv6_addr> ... | -viewName <string> | -preferredLocList <string> ...] [-TTL <secs>]

Description

Add a dns action.

Parameters

actionName

Name of the dns action.

actionType

The type of DNS action that is being configured. Possible values: ViewName, GslbPrefLoc, Drop, Cache_Bypass, Rewrite_Response

IPAddress

List of IP address to be returned in case of rewrite_response actiontype. They can be of IPV4 or IPV6 type. In case of set command We will remove all the IP address previously present in the action and will add new once given in set dns action command.

TTL

Time to live, in seconds. Default value: 3600 Maximum value: 2147483647

viewName

The view name that must be used for the given action.

preferredLocList

The location list in priority order used for the given action.

Example

```
add dns action <actionName> <actionType> (-
IPAddress <ip_addr|ipv6_addr> ... | -viewName
<string> | -preferredLocList <string> ...) [-TTL
<secs>]
add dns action action1 Rewrite Response -
ipAddress 10.102.27.153 10.102.27.154 33::33
44::44 -TTL 4000
add dns action action1 GslbPrefLoc -
preferredLocList india.10.102.81.175.80 us.
10.102.81.176.80
add dns action action1 ViewName -viewName dnsview1
```

[Top](#)

rm dns action**Synopsis**

```
rm dns action <actionName>
```

Description

Removes a dns Action.

Parameters**actionName**

Name of the dns action.

Example

```
rm dns action action1
```

[Top](#)

set dns action**Synopsis**

```
set dns action <actionName> [-IPAddress <ip_addr|ipv6_addr> ...] [-TTL <secs>] [-
viewName <string>] [-preferredLocList <string> ...]
```

Description

Set a dns Action. Use this command to set the values for Ip address and TTL, If Ippaddress is given in set dns action command we will discard the previous set and will apply this new set of ipaddress given.

Parameters

actionName

Name of the dns action.

IPAddress

List of IP address to be returned in case of rewrite_response actiontype. They can be of IPV4 or IPV6 type. In case of set command We will remove all the IP address previously present in the action and will add new once given in set dns action command.

TTL

Time to live, in seconds. Default value: 3600 Maximum value: 2147483647

viewName

The view name that must be used for the given action.

preferredLocList

The location list in priority order used for the given action.

Example

```
set dns action <actionName> [-IPAddress <ip_addr|  
ipv6_addr> ...] [-TTL <secs>] [-viewName <string>]  
[-preferredLocList <string> ...]  
set dns action action1 -ipAddress 10.102.27.153  
10.102.27.154 33::33 44::44 -TTL 4000  
set dns action action1 -viewName dnsview2  
set dns action action1 -preferredLocList india.  
10.102.81.175.80
```

[Top](#)

unset dns action

Synopsis

```
unset dns action <actionName> -TTL
```

Description

Use this command to remove dns action settings.Refer to the set dns action command for meanings of the arguments.

[Top](#)

show dns action

Synopsis

show dns action [<actionName>]

Description

Used to display the action-related information.

Parameters

actionName

Name of the dns action.

Example

```
show dns action <Action-Name>
show dns action action1
show dns action
```

[Top](#)

dns nsecRec

show dns nsecRec

Synopsis

show dns nsecRec [<hostName> | -type <type>]

Description

Displays the NextSECure (NSEC) resource records created for the specified domain name.

Parameters

hostName

Name of the domain.

type

Type of records to display. Available settings function as follows: * ADNS - Display all authoritative address records. * PROXY - Display all proxy address records. * ALL - Display all address records. Possible values: ALL, ADNS, PROXY

Example

```
show dns nsecRec foo.bar
```

DOS Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [dos](#)
- ♦ [dos policy](#)
- ♦ [dos stats](#)

dos

stat dos

Synopsis

```
stat dos [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]
[-clearstats ( basic | full )]
```

Description

Displays DoS protection statistics.

Parameters

clearstats

Clear the statistics / counters Possible values: basic, full

dos policy

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#) | [stat](#)]

add dos policy

Synopsis

```
add dos policy <name> -qDepth <positive_integer> [-cltDetectRate <positive_integer>]
```

Description

Adds a DoS protection policy to the appliance. Note: To apply DoS protection to a service, bind the DoS policy to the service by using the bind service command.

Parameters

name

Name for the HTTP DoS protection policy. Must begin with a letter, number, or the underscore character (_). Other characters allowed, after the first character, are the hyphen (-), period (.) hash (#), space (), at (@), equals (=), and colon (:) characters.

qDepth

Queue depth. The queue size (the number of outstanding service requests on the system) before DoS protection is activated on the service to which the DoS protection policy is bound. Minimum value: 21

cltDetectRate

Client detect rate. Integer representing the percentage of traffic to which the HTTP DoS policy is to be applied after the queue depth condition is satisfied. Maximum value: 100

Example

```
add dos policy dospel -qdepth 100 -cltDetectRate 90
```

[Top](#)**rm dos policy****Synopsis**

```
rm dos policy <name>
```

Description

Removes a DoS protection policy from the appliance.

Parameters**name**

Name of the DoS protection policy to be removed.

Example

```
rm dos policy dospel
```

[Top](#)**set dos policy****Synopsis**

```
set dos policy <name> [-qDepth <positive_integer>] [-cltDetectRate <positive_integer>]
```

Description

Modifies the attributes of a DoS protection policy.

Parameters**name**

Name of the DoS protection policy to be modified.

qDepth

Queue depth. The queue size (the number of outstanding service requests on the system) before DoS protection is activated on the service to which the DoS protection policy is bound. Minimum value: 21

cltDetectRate

Client detect rate. Integer representing the percentage of traffic to which the HTTP DoS policy is to be applied after the queue depth condition is satisfied. Minimum value: 1 Maximum value: 100

Example

```
set dos policy dospel -qdepth 1000
```

[Top](#)

unset dos policy

Synopsis

unset dos policy <name> -cltDetectRate

Description

Use this command to remove dos policy settings. Refer to the set dos policy command for meanings of the arguments.

[Top](#)

show dos policy

Synopsis

show dos policy [<name>]

Description

Displays information about a DoS protection policy.

Parameters

name

Name of the DoS protection policy about which to display information. If a name is not provided, information about all DoS protection policies is shown.

Example

```
> show dos policy
    1 configured DoS policy:
1)   Policy: dospel  QDepth: 100
ClientDetectRate: 90
Done
```

[Top](#)

stat dos policy

Synopsis

```
stat dos policy [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile  
<input_filename>] [-clearstats ( basic | full )]
```

Description

Displays statistics of the DoS protection policy.

Parameters

name

The name of the DoS protection policy whose statistics must be displayed. If a name is not provided, statistics of all the DoS protection policies are displayed.

clearstats

Clear the statistics / counters Possible values: basic, full

[Top](#)

dos stats

show dos stats

Synopsis

```
show dos stats - alias for 'stat dos'
```

Description

show dos stats is an alias for stat dos Displays DoS protection statistics.

Filter Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [filter action](#)
- ♦ [filter htmlinjectionvariable](#)
- ♦ [filter policy](#)
- ♦ [filter prebodyInjection](#)
- ♦ [filter postbodyInjection](#)
- ♦ [filter htmlinjectionparameter](#)
- ♦ [filter global](#)

filter action

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add filter action

Synopsis

add filter action <name> <qual> [<serviceName>] [<value>] [<respCode>] [<page>]

Description

Creates a content filtering action. This action can be associated with a content filtering policy that is created with the add filter policy command. Note: The following content filtering actions are available by default: * RESET - Sends a TCP reset for the HTTP requests. * DROP - Drops the HTTP requests silently, without sending a TCP FIN for closing the connection.

Parameters

name

Name for the filtering action. Must begin with a letter, number, or the underscore character (_). Other characters allowed, after the first character, are the hyphen (-), period (.) hash (#), space (), at sign (@), equals (=), and colon (:) characters. Choose a name that helps identify the type of action. The name of a filter action cannot be changed after it is created. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

qual

Qualifier, which is the action to be performed. The qualifier cannot be changed after it is set. The available options function as follows: ADD - Adds the specified HTTP header. RESET - Terminates the connection, sending the appropriate termination notice to the user's browser. FORWARD - Redirects the request to the designated service. You must specify either a service name or a page, but not both. DROP - Silently deletes the request, without sending a response to the user's browser. CORRUPT - Modifies the designated HTTP header to prevent it from performing the function it was intended to perform, then sends the request/response to the server/browser. ERRORCODE. Returns the designated HTTP error code to the user's browser (for example, 404, the standard HTTP code for a non-existent Web page). Possible values: reset, add, corrupt, forward, errorcode, drop

serviceName

Service to which to forward HTTP requests. Required if the qualifier is FORWARD.

value

String containing the header_name and header_value. If the qualifier is ADD, specify <header_name>:<header_value>. If the qualifier is CORRUPT, specify only the header_name

respCode

Response code to be returned for HTTP requests (for use with the ERRORCODE qualifier). Minimum value: 1

page

HTML page to return for HTTP requests (For use with the ERRORCODE qualifier).

Example

```
add filter action bad_url_action errorcode 400
"<HTML>Bad URL.</HTML>"
add filter action forw_action FORWARD service1
add filter action add_header_action add
"HEADER:value"
```

[Top](#)**rm filter action****Synopsis**

```
rm filter action <name>
```

Description

Removes a content filtering action.

Parameters**name**

Name of the content filter action to be removed.

Example

```
rm filter action filter_action_name
```

[Top](#)**set filter action****Synopsis**

```
set filter action <name> [-serviceName <string>] [-value <string>] [-respCode
<positive_integer>] [-page <string>]
```

Description

Modifies an existing content filtering action.

Parameters**name**

Name of the content filtering action to be modified.

serviceName

Service to which to forward HTTP requests. Required if the qualifier is FORWARD.

value

String containing the header_name and header_value. If the qualifier is ADD, specify <header_name>:<header_value>. If the qualifier is CORRUPT, specify only the header_name

respCode

Response code to be returned for HTTP requests (for use with the ERRORCODE qualifier). Minimum value: 1

page

HTML page to return for HTTP requests (For use with the ERRORCODE qualifier).

Example

```
set filter action bad_url_action -respcode 400 -
page "<HTML>Bad URL.</HTML>"
set filter action forw_action -serviceName service1
set filter action add_header_action -value
"HEADER:value"
```

[Top](#)

unset filter action

Synopsis

unset filter action <name> -page

Description

Use this command to remove filter action settings. Refer to the set filter action command for meanings of the arguments.

[Top](#)

show filter action

Synopsis

show filter action [<name>]

Description

Displays information about available filtering actions.

Parameters

name

Name of the content filtering action to be displayed. If a name is not provided, information about all filter actions is shown.

Example

```
Example 1
The following shows an example of the output of
the show filter action command when no filter
actions have been defined:
1)      Name: RESET      Filter Type: reset
2)      Name: DROP       Filter Type: drop
Done
```

```

Example 2
The following command creates a filter action:
add filter action bad_url_action errorcode 400
"<HTML>Bad URL.</HTML>"
The following shows an example of the output of
the show filter action command after the previous
command has been issued:
      Name: bad_url_action      Filter Type:
errorcode
      StatusCode: 400
      Response Page: <HTML>Bad URL.</HTML>
Done

```

[Top](#)

filter htmlinjectionvariable

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add filter htmlinjectionvariable

Synopsis

add filter htmlinjectionvariable <variable> [-value <string>]

Description

Creates an HTML injection variable.

Parameters

variable

Name for the HTML injection variable to be added.

value

Value to be assigned to the new variable.

varId

ID of the system variable. Used only in builtins. Possible values: IID, UTIME, XID, PAGEID, REQRTBEG, REQRTEND, REQSTBEG, REQSTEND, RESRTBEG, RESRTEND, RESSTBEG, RESSTEND, CLTRTT, CTYPE, TRANSID, SYSVSVR, SYSSERV

Example

```

add htmlinjectionvariable EDGESIGHT_SERVER_IP -
value 1.1.1.1

```

[Top](#)

rm filter htmlinjectionvariable

Synopsis

`rm filter htmlinjectionvariable <variable>`

Description

Removes an HTML injection variable.

Parameters

variable

Name of the HTML injection variable to be removed.

Example

```
rm htmlinjectionvariable EDGESIGHT_SERVER_IP
```

[Top](#)

set filter htmlinjectionvariable

Synopsis

`set filter htmlinjectionvariable <variable> [-value <string>]`

Description

Modifies the value of an HTML injection variable.

Parameters

variable

Name of the HTML injection variable to be modified.

value

Value to be assigned to the new variable.

Example

```
set htmlinjectionvariable EDGESIGHT_SERVER_IP -  
value 2.2.2.2
```

[Top](#)

unset filter htmlinjectionvariable

Synopsis

`unset filter htmlinjectionvariable <variable> -value`

Description

Use this command to remove filter `htmlinjectionvariable` settings. Refer to the `set filter htmlinjectionvariable` command for meanings of the arguments.

[Top](#)

show filter htmlinjectionvariable

Synopsis

`show filter htmlinjectionvariable [<variable>]`

Description

Displays information about HTML injection variables.

Parameters

variable

Name of the HTML injection variable to be displayed. If a name is not provided, information about all the HTML injection variables is shown.

Example

```
show htmlinjectionvariable EDGESIGHT_SERVER_IP
```

[Top](#)

filter policy

[[add](#) | [rm](#) | [set](#) | [show](#)]

add filter policy

Synopsis

`add filter policy <name> -rule <expression> (-reqAction <string> | -resAction <string>)`

Description

Creates a content filtering policy.

Parameters

name

Name for the filtering action. Must begin with a letter, number, or the underscore character (`_`). Other characters allowed, after the first character, are the hyphen (`-`), period (`.`) pound (`#`), space (), at (`@`), equals (`=`), and colon (`:`) characters. Choose a name that helps identify the type of action. The name cannot be updated after the policy is created. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, `"my policy"` or `'my policy'`).

rule

NetScaler classic expression specifying the type of connections that match this policy.

reqAction

Name of the action to be performed on requests that match the policy. Cannot be specified if the rule includes condition to be evaluated for responses.

resAction

The action to be performed on the response. The string value can be a filter action created filter action or a built-in action.

Example

Example 1:

```
add policy expression e1 "sourceip == 66.33.22.0 -
netmask 255.255.255.0"
add policy expression e2 "URL == /admin/
account.asp"
add filter policy ip_filter -rule "e1 && e2" -
reqAction RESET
After creating above filter policy, it can be
activated by binding it globally:
bind filter global ip_filter
```

With the configured ip_filter (name of the filter policy), the NetScaler system sends a TCP reset to all HTTP requests for the /admin/account.asp URL from 66.33.22.0 Class C network. This action is applied at the HTTP request time.

Example 2:

```
To silently drop (without sending FIN) all the
HTTP requests in which the URL has root.exe or
cmd.exe, below filter policy can be configured:
add filter policy nimda_filter -rule "URL contains
root.exe || URL contains cmd.exe" -reqAction DROP
bind filter global nimda_filter
```

Example 3:

```
add filter policy url_filter -rule "url == /foo/
secure.asp && SOURCEIP != 65.186.55.0 -netmask
255.255.255.0 && SOURCEIP != 65.202.35.0 -netmask
255.255.255.0" -reqaction RESET
bind filter global url_filter
```

With the above configured filter policy named url_filter, the NetScaler system sends RESET to all HTTP requests for the URL /foo/secure.asp from all the networks except from 65.186.55.0 and 65.202.35.0 Class C networks. This action is applied at the HTTP request time.

Note: In above examples, the RESET and DROP are built-in actions in the NetScaler system.


```
"show filter action" and "show filter policy" CLI
commands show the configured filter actions and
policies in NetScaler system respectively. "show
filter global" command shows all the
globallyactive filter policies.
```

[Top](#)

rm filter policy

Synopsis

```
rm filter policy <name>
```

Description

Removes a filter policy.

Parameters

name

Name of the filter policy to be removed.

Example

```
rm filter policy filter_policy_name
The "show filter policy" command shows all filter
policies that are currently defined.
```

[Top](#)

set filter policy

Synopsis

```
set filter policy <name> [-rule <expression>] [-reqAction <string> | -resAction <string>]
```

Description

Modifies a filter policy.

Parameters

name

Name of the filter policy to be modified.

rule

NetScaler classic expression specifying the type of connections that match this policy.

reqAction

Name of the action to be performed on requests that match the policy. Cannot be specified if the rule includes condition to be evaluated for responses.

resAction

The action to be performed on the response. The string value can be a filter action created filter action or a built-in action.

Example

```
Example 1:
A filter policy to allow access of URL /foo/
secure.asp only from 65.186.55.0 network can be
created using below command:
add filter policy url_filter -rule "URL == /foo/
secure.asp && SOURCEIP != 65.186.55.0 -netmask
255.255.255.0" -reqAction RESET
This policy is activated using:
bind filter global url_filter

Later, to allow access of this url from second
network 65.202.35.0 too, above filter policy can
be changed by issuing below command:
set filter policy url_filter -rule "URL == /foo/
secure.asp && SOURCEIP != 65.186.55.0 -netmask
255.255.255.0 && SOURCEIP != 65.202.35.0 -netmask
255.255.255.0"

Changed filter policy can be viewed by using
following command:
show filter policy url_filter
    Name: url_filter  Rule: (URL == /foo/
secure.asp && (SOURCEIP != 65.186.55.0 -netmask
255.255.255.0 && SOURCEIP != 65.202.35.0 -netmask
255.255.255.0))
    Request action: RESET
    Response action:
    Hits: 0

Done
```

[Top](#)**show filter policy****Synopsis**

show filter policy [<name>]

Description

Displays information about the filter policies.

Parameters**name**

Name of the filter policy to be displayed. If a name is not provided, information about all the filter policies is shown.

Example

```

show filter policy
1)      Name: nimda_filter Rule: (URL CONTAINS
root.exe || URL CONTAINS cmd.exe)
      Request action: RESET
      Response action:
      Hits: 0
2)      Name: ip_filter Rule: (src_ips && URL == /
admin/account.asp)
      Request action: RESET
      Response action:
      Hits: 0

Done

Individual filter policy can also be viewed by
giving filter policy name as argument:
show filter policy ip_filter
      Name: ip_filter Rule: (src_ips && URL == /
admin/account.asp)
      Request action: RESET
      Response action:
      Hits: 0

Done

```

[Top](#)

filter prebodyInjection

[\[set | unset | show \]](#)

set filter prebodyInjection

Synopsis

`set filter prebodyInjection <prebody>`

Description

Specifies the file to be used for prebody injection.

Parameters

prebody

Name of file whose contents are to be inserted before the response body.

Example

```
set filter prebodyInjection ens/prebody.js
```

[Top](#)

unset filter prebodyInjection

Synopsis

unset filter prebodyInjection [-prebody]

Description

Removes the setting that specifies the file used for prebody injection..Refer to the set filter prebodyInjection command for meanings of the arguments.

Example

```
unset filter prebodyInjection
```

[Top](#)

show filter prebodyInjection

Synopsis

show filter prebodyInjection

Description

Displays the name of the file used for prebody injection.

[Top](#)

filter postbodyInjection

[[set](#) | [unset](#) | [show](#)]

set filter postbodyInjection

Synopsis

set filter postbodyInjection <postbody>

Description

Specifies the file to be used for postbody injection.

Parameters

postbody

Name of file whose contents are to be inserted after the response body.

Example

```
set filter postbodyInjection ens/postbody.js
```

[Top](#)

unset filter postbodyInjection

Synopsis

unset filter postbodyInjection [-postbody]

Description

Removes the setting that specifies the file used for postbody injection..Refer to the set filter postbodyInjection command for meanings of the arguments.

Example

```
unset filter postbodyInjection
```

[Top](#)

show filter postbodyInjection

Synopsis

show filter postbodyInjection

Description

Displays the name of the file used for postbody injection.

[Top](#)

filter htmlinjectionparameter

[[set](#) | [unset](#) | [show](#)]

set filter htmlinjectionparameter

Synopsis

set filter htmlinjectionparameter [-rate <positive_integer>] [-frequency <positive_integer>] [-strict (ENABLED | DISABLED)] [-htmlsearchlen <positive_integer>]

Description

Sets the HTML injection parameters.

Parameters

rate

For a rate of x, HTML injection is done for 1 out of x policy matches. Default value: 1
Minimum value: 1

frequency

For a frequency of x, HTML injection is done at least once per x milliseconds. Default value: 1
Minimum value: 1

strict

Searching for <html> tag. If this parameter is enabled, HTML injection does not insert the prebody or postbody content unless the <html> tag is found. Possible values: ENABLED, DISABLED Default value: ENABLED

htmlsearchlen

Number of characters, in the HTTP body, in which to search for the <html> tag if strict mode is set. Default value: 1024 Minimum value: 1

Example

```
set htmlinjectionparameter -rate 10 -frequency 1
```

[Top](#)

unset filter htmlinjectionparameter**Synopsis**

unset filter htmlinjectionparameter [-rate] [-frequency] [-strict] [-htmlsearchlen]

Description

Removes the HTML injection settings..Refer to the set filter htmlinjectionparameter command for meanings of the arguments.

Example

```
a) unset htmlinjectionparameter -rate
   b) unset htmlinjectionparameter -frequency
   c) unset htmlinjectionparameter -rate -
      frequency
```

[Top](#)

show filter htmlinjectionparameter**Synopsis**

show filter htmlinjectionparameter

Description

Displays the HTML injection parameters.

Example

```
rate      :      10
```

[Top](#)

filter global

[[bind](#) | [unbind](#) | [show](#)]

bind filter global

Synopsis

bind filter global (<policyName> [-priority <positive_integer>]) [-state (ENABLED | DISABLED)]

Description

Apply (bind) the specified filtering policy globally. Note: Filtering requires the content filtering license.

Parameters

policyName

Name of the filtering policy to be bound.

Example

```
To send RESET for all the HTTP requests which are
not get or head type, following filter policy can
be created:
add filter policy reset_invalid_req -rule "METHOD !
= GET  && METHOD != HEAD" -reqAction RESET
This filter policy can be activated globally for
NetScaler system by giving command:
bind filter global reset_invalid_req
```

```
Globally active filter policies can be seen using
command:
show filter global
1)      Policy Name: reset_invalid_req  Priority: 0
Done
```

[Top](#)

unbind filter global

Synopsis

unbind filter global <policyName>

Description

Deactivate a globally bound filter policy.

Parameters

policyName

Name of the filter policy to be unbound.

Example

```
Globally active filter policies can be seen using
command:
show filter global
1)      Policy Name: reset_invalid_req  Priority: 0
Done
This globally active filter policy can be
deactivated on NetScaler system by giving command:
unbind filter global reset_invalid_req
```

[Top](#)

show filter global

Synopsis

show filter global

Description

Displays the globally activated filter policies.

Example

```
show filter global
1)      Policy Name: url_filter Priority: 0
2)      Policy Name: reset_invalid_req  Priority: 0
Done
```

[Top](#)

GSLB Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [gslb site](#)
- ♦ [gslb service](#)
- ♦ [gslb vserver](#)
- ♦ [gslb runningConfig](#)
- ♦ [gslb domain](#)
- ♦ [gslb ldnsentries](#)
- ♦ [gslb parameter](#)
- ♦ [gslb ldnsentry](#)
- ♦ [gslb config](#)

- ◆ [gslb syncStatus](#)

gslb site

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#) | [stat](#)]

add gslb site

Synopsis

```
add gslb site <siteName> [<siteType>] <siteIPAddress> [-publicIP <ip_addr|ipv6_addr|
*>] [-metricExchange ( ENABLED | DISABLED )] [-nwMetricExchange ( ENABLED |
DISABLED )] [-sessionExchange ( ENABLED | DISABLED )] [-triggerMonitor
<triggerMonitor>] [-parentSite <string>]
```

Description

Creates a global server load balancing site.

Parameters

siteName

Name for the GSLB site. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the virtual server is created. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my gslbsite" or 'my gslbsite').

siteType

Type of site to create. If the type is not specified, the appliance automatically detects and sets the type on the basis of the IP address being assigned to the site. If the specified site IP address is owned by the appliance (for example, a MIP address or SNIP address), the site is a local site. Otherwise, it is a remote site. Possible values: REMOTE, LOCAL Default value: NS_NORMAL

siteIPAddress

IP address for the GSLB site. The GSLB site uses this IP address to communicate with other GSLB sites. For a local site, use any IP address that is owned by the appliance (for example, a SNIP or MIP address, or the IP address of the ADNS service).

publicIP

Public IP address for the local site. Required only if the appliance is deployed in a private address space and the site has a public IP address hosted on an external firewall or a NAT device.

metricExchange

Exchange metrics with other sites. Metrics are exchanged by using Metric Exchange Protocol (MEP). The appliances in the GSLB setup exchange health information once every second. If you disable metrics exchange, you can use only static load balancing methods (such as round robin, static proximity, or the hash-based methods), and if you disable metrics exchange when a dynamic load balancing method (such as least connection) is in operation, the appliance falls back to round robin. Also, if you disable metrics exchange, you must use a monitor to determine the state of GSLB

services. Otherwise, the service is marked as DOWN. Possible values: ENABLED, DISABLED Default value: ENABLED

nwMetricExchange

Exchange, with other GSLB sites, network metrics such as round-trip time (RTT), learned from communications with various local DNS (LDNS) servers used by clients. RTT information is used in the dynamic RTT load balancing method, and is exchanged every 5 seconds. Possible values: ENABLED, DISABLED Default value: ENABLED

sessionExchange

Exchange persistent session entries with other GSLB sites every five seconds. Possible values: ENABLED, DISABLED Default value: ENABLED

triggerMonitor

Specify the conditions under which the GSLB service must be monitored by a monitor, if one is bound. Available settings function as follows: * ALWAYS - Monitor the GSLB service at all times. * MEPDOWN - Monitor the GSLB service only when the exchange of metrics through the Metrics Exchange Protocol (MEP) is disabled. MEPDOWN_SVCDOWN - Monitor the service in either of the following situations: * The exchange of metrics through MEP is disabled. * The exchange of metrics through MEP is enabled but the status of the service, learned through metrics exchange, is DOWN. Possible values: ALWAYS, MEPDOWN, MEPDOWN_SVCDOWN Default value: NSGSLB_TRIGMON_ALWAYS

parentSite

Parent site of the GSLB site, in a parent-child topology.

Example

```
add site new_york LOCAL 192.168.100.12 -
publicIP 65.200.211.139
```

[Top](#)

rm gslb site

Synopsis

rm gslb site <siteName>

Description

Removes a global server load balancing (GSLB) site and all its constituent GSLB services.

Parameters

siteName

Name of the GSLB site to remove.

Example

```
rm gslb site new_york
```

[Top](#)

set gslb site

Synopsis

```
set gslb site <siteName> [-metricExchange ( ENABLED | DISABLED )] [-nwMetricExchange ( ENABLED | DISABLED )] [-sessionExchange ( ENABLED | DISABLED )] [-triggerMonitor <triggerMonitor>]
```

Description

Modifies the specified parameters of a global server load balancing (GSLB) site.

Parameters

siteName

Name of the GSLB site.

metricExchange

Exchange metrics with other sites. Metrics are exchanged by using Metric Exchange Protocol (MEP). The appliances in the GSLB setup exchange health information once every second. If you disable metrics exchange, you can use only static load balancing methods (such as round robin, static proximity, or the hash-based methods), and if you disable metrics exchange when a dynamic load balancing method (such as least connection) is in operation, the appliance falls back to round robin. Also, if you disable metrics exchange, you must use a monitor to determine the state of GSLB services. Otherwise, the service is marked as DOWN. Possible values: ENABLED, DISABLED Default value: ENABLED

nwMetricExchange

Exchange, with other GSLB sites, network metrics such as round-trip time (RTT), learned from communications with various local DNS (LDNS) servers used by clients. RTT information is used in the dynamic RTT load balancing method, and is exchanged every 5 seconds. Possible values: ENABLED, DISABLED Default value: ENABLED

sessionExchange

Exchange persistent session entries with other GSLB sites every five seconds. Possible values: ENABLED, DISABLED Default value: ENABLED

triggerMonitor

Specify the conditions under which the GSLB service must be monitored by a monitor, if one is bound. Available settings function as follows: * ALWAYS - Monitor the GSLB service at all times. * MEPDOWN - Monitor the GSLB service only when the exchange of metrics through the Metrics Exchange Protocol (MEP) is disabled. MEPDOWN_SVCDOWN - Monitor the service in either of the following situations: * The exchange of metrics through MEP is disabled. * The exchange of metrics through MEP is enabled but the status of the service, learned through metrics exchange, is DOWN.

Possible values: ALWAYS, MEPDOWN, MEPDOWN_SVCDOWN Default value:
NSGSLB_TRIGMON_ALWAYS

Example

```
set gslb site new_york - metricExchange DISABLED
```

[Top](#)

unset gslb site

Synopsis

```
unset gslb site <siteName> [-metricExchange] [-nwMetricExchange] [-sessionExchange]  
[-triggerMonitor]
```

Description

Use this command to remove gslb site settings. Refer to the set gslb site command for meanings of the arguments.

[Top](#)

show gslb site

Synopsis

```
show gslb site [<siteName>] show gslb site stats - alias for 'stat gslb site'
```

Description

Displays the parameters of all the GSLB sites configured on the appliance, or the parameters of the specified GSLB site.

Parameters

siteName

Name of the GSLB site. If you specify a site name, details of all the site's constituent services are also displayed.

Example

```
show site new_york
```

[Top](#)

stat gslb site

Synopsis

```
stat gslb site [<siteName>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile  
<input_filename>] [-clearstats ( basic | full )]
```

Description

Displays statistics for a GSLB site.

Parameters

siteName

Name of the GSLB site for which to display detailed statistics. If a name is not specified, basic information about all GSLB sites is displayed.

clearstats

Clear the statistics / counters Possible values: basic, full

[Top](#)

gslb service

[[add](#) | [rm](#) | [set](#) | [unset](#) | [bind](#) | [unbind](#) | [show](#) | [stat](#) | [rename](#)]

add gslb service

Synopsis

```
add gslb service <serviceName> [-cnameEntry <string> | <IP> | <serverName> |
<serviceType> | <port> | -publicIP <ip_addr|ipv6_addr|*> | -publicPort <port> | -
sitePersistence <sitePersistence> | -sitePrefix <string>] [-maxClient <positive_integer>]
[-healthMonitor ( YES | NO )] [-siteName <string>] [-state ( ENABLED | DISABLED )] [-cip
( ENABLED | DISABLED ) [<cipHeader>]] [-cookieTimeout <mins>] [-cltTimeout <secs>] [-
svrTimeout <secs>] [-maxBandwidth <positive_integer>] [-downStateFlush ( ENABLED |
DISABLED )] [-maxAAAUsers <positive_integer>] [-monThreshold <positive_integer>] [-
hashld <positive_integer>] [-comment <string>] [-appflowLog ( ENABLED | DISABLED )]
```

Description

Creates a global server load balancing (GSLB) service.

Parameters

serviceName

Name for the GSLB service. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the GSLB service is created. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my gslbsvc" or 'my gslbsvc').

cnameEntry

Canonical name of the GSLB service. Used in CNAME-based GSLB.

IP

IP address for the GSLB service. Should represent a load balancing, content switching, or VPN virtual server on the NetScaler appliance, or the IP address of another load balancing device.

serverName

Name of the server hosting the GSLB service.

serviceType

Type of service to create. Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, ANY, SIP_UDP, RADIUS, RDP, RTSP, MYSQL, MSSQL Default value: NSSVC_SERVICE_UNKNOWN

port

Port on which the load balancing entity represented by this GSLB service listens. Minimum value: 1

publicIP

The public IP address that a NAT device translates to the GSLB service's private IP address. Optional.

publicPort

The public port associated with the GSLB service's public IP address. The port is mapped to the service's private port number. Applicable to the local GSLB service. Optional.

maxClient

The maximum number of open connections that the service can support at any given time. A GSLB service whose connection count reaches the maximum is not considered when a GSLB decision is made, until the connection count drops below the maximum. Maximum value: 4294967294

healthMonitor

Monitor the health of the GSLB service. Possible values: YES, NO Default value: YES

siteName

Name of the GSLB site to which the service belongs.

state

Enable or disable the service. Possible values: ENABLED, DISABLED Default value: ENABLED

cip

In the request that is forwarded to the GSLB service, insert a header that stores the client's IP address. Client IP header insertion is used in connection-proxy based site persistence. Possible values: ENABLED, DISABLED Default value: DISABLED

cipHeader

Name for the HTTP header that stores the client's IP address. Used with the Client IP option. If client IP header insertion is enabled on the service and a name is not specified for the header, the NetScaler appliance uses the name specified by the cipHeader parameter in the set ns param command or, in the GUI, the Client IP Header parameter in the Configure HTTP Parameters dialog box.

sitePersistence

Use cookie-based site persistence. Applicable only to HTTP and SSL GSLB services. Possible values: ConnectionProxy, HTTPRedirect, NONE

cookieTimeout

Timeout value, in minutes, for the cookie, when cookie based site persistence is enabled. Maximum value: 1440

sitePrefix

The site's prefix string. When the service is bound to a GSLB virtual server, a GSLB site domain is generated internally for each bound service-domain pair by concatenating the site prefix of the service and the name of the domain. If the special string NONE is specified, the site-prefix string is unset. When implementing HTTP redirect site persistence, the NetScaler appliance redirects GSLB requests to GSLB services by using their site domains.

cltTimeout

Idle time, in seconds, after which a client connection is terminated. Applicable if connection proxy based site persistence is used. Maximum value: 31536000

svrTimeout

Idle time, in seconds, after which a server connection is terminated. Applicable if connection proxy based site persistence is used. Maximum value: 31536000

maxBandwidth

Integer specifying the maximum bandwidth allowed for the service. A GSLB service whose bandwidth reaches the maximum is not considered when a GSLB decision is made, until its bandwidth consumption drops below the maximum.

downStateFlush

Flush all active transactions associated with the GSLB service when its state transitions from UP to DOWN. Do not enable this option for services that must complete their transactions. Applicable if connection proxy based site persistence is used. Possible values: ENABLED, DISABLED

maxAAUsers

Maximum number of SSL VPN users that can be logged on concurrently to the VPN virtual server that is represented by this GSLB service. A GSLB service whose user count reaches the maximum is not considered when a GSLB decision is made, until the count drops below the maximum. Maximum value: 65535

monThreshold

Monitoring threshold value for the GSLB service. If the sum of the weights of the monitors that are bound to this GSLB service and are in the UP state is not equal to or greater than this threshold value, the service is marked as DOWN. Maximum value: 65535

hashId

Unique hash identifier for the GSLB service, used by hash based load balancing methods. Minimum value: 1

comment

Any comments that you might want to associate with the GSLB service.

appflowLog

Enable logging appflow flow information Possible values: ENABLED, DISABLED Default value: ENABLED

Example

```
add gslb service sj_svc 203.12.123.12 http 80 -
site san_jos
```

[Top](#)

rm gslb service

Synopsis

```
rm gslb service <serviceName>
```

Description

Removes a global server load balancing (GSLB) service configured on the appliance.

Parameters

serviceName

Name of the GSLB service.

Example

```
rm gslb service sj_svc
```

[Top](#)

set gslb service

Synopsis

```
set gslb service <serviceName> [-IPAddress <ip_addr|ipv6_addr|*>] [-publicIP <ip_addr|
ipv6_addr|*>] [-publicPort <port>] [-cip ( ENABLED | DISABLED ) [<cipHeader>]] [-
sitePersistence <sitePersistence>] [-sitePrefix <string>] [-maxClient <positive_integer>]
[-healthMonitor ( YES | NO )] [-maxBandwidth <positive_integer>] [-downStateFlush
( ENABLED | DISABLED )] [-maxAAAUUsers <positive_integer>] [-viewName <string>
<viewIP>] [-monThreshold <positive_integer>] [-weight <positive_integer>
<monitorName>] [-hashId <positive_integer>] [-comment <string>] [-appflowLog
( ENABLED | DISABLED )]
```

Description

Modifies the specified parameters of a global server load balancing (GSLB) service.

Parameters

serviceName

Name of the GSLB service.

IPAddress

The new IP address of the service.

publicIP

The public IP address that a NAT device translates to the GSLB service's private IP address. Optional.

publicPort

The public port associated with the GSLB service's public IP address. The port is mapped to the service's private port number. Applicable to the local GSLB service. Optional. Minimum value: 1

cip

In the request that is forwarded to the GSLB service, insert a header that stores the client's IP address. Client IP header insertion is used in connection-proxy based site persistence. Possible values: ENABLED, DISABLED Default value: DISABLED

sitePersistence

Use cookie-based site persistence. Applicable only to HTTP and SSL GSLB services. Possible values: ConnectionProxy, HTTPRedirect, NONE

sitePrefix

The site's prefix string. When the service is bound to a GSLB virtual server, a GSLB site domain is generated internally for each bound service-domain pair by concatenating the site prefix of the service and the name of the domain. If the special string NONE is specified, the site-prefix string is unset. When implementing HTTP redirect site persistence, the NetScaler appliance redirects GSLB requests to GSLB services by using their site domains.

maxClient

The maximum number of open connections that the service can support at any given time. A GSLB service whose connection count reaches the maximum is not considered when a GSLB decision is made, until the connection count drops below the maximum. Maximum value: 4294967294

healthMonitor

Monitor the health of the GSLB service. Possible values: YES, NO Default value: YES

maxBandwidth

Maximum bandwidth.

downStateFlush

Flush all active transactions associated with the GSLB service when its state transitions from UP to DOWN. Do not enable this option for services that must complete their transactions. Applicable if connection proxy based site persistence is used. Possible values: ENABLED, DISABLED Default value: ENABLED

maxAAUsers

Maximum number of SSL VPN users that can be logged on concurrently to the VPN virtual server that is represented by this GSLB service. A GSLB service whose user count reaches the maximum is not considered when a GSLB decision is made, until the count drops below the maximum. Maximum value: 65535

viewName

Name of the DNS view of the service. A DNS view is used in global server load balancing (GSLB) to return a predetermined IP address to a specific group of clients, which are identified by using a DNS policy.

monThreshold

Monitoring threshold value for the GSLB service. If the sum of the weights of the monitors that are bound to this GSLB service and are in the UP state is not equal to or greater than this threshold value, the service is marked as DOWN. Maximum value: 65535

weight

Weight to assign to the monitor-service binding. A larger number specifies a greater weight. Contributes to the monitoring threshold, which determines the state of the service. Minimum value: 1 Maximum value: 100

hashId

Unique hash identifier for the GSLB service, used by hash based load balancing methods. Minimum value: 1

comment

Any comments that you might want to associate with the GSLB service.

appflowLog

Enable logging appflow flow information Possible values: ENABLED, DISABLED Default value: ENABLED

Example

```
set gslb service sj_svc -sitePersistence
ConnectionProxy
```

[Top](#)

unset gslb service

Synopsis

```
unset gslb service <serviceName> [-publicIP] [-publicPort] [-cip] [-cipHeader] [-
sitePersistence] [-sitePrefix] [-maxClient] [-healthMonitor] [-maxBandwidth] [-
downStateFlush] [-maxAAUsers] [-viewIP] [-monThreshold] [-monitorName] [-hashId]
[-comment] [-appflowLog]
```

Description

Use this command to remove gslb service settings. Refer to the set gslb service command for meanings of the arguments.

[Top](#)

bind gslb service

Synopsis

```
bind gslb service <serviceName> ((-viewName <string> <viewIP>) | (-monitorName
<string>@ [-monState ( ENABLED | DISABLED )] [-weight <positive_integer>]))
```

Description

Binds a DNS view or a monitor to a global server load balancing (GSLB) service.

Parameters

serviceName

Name of the GSLB service.

viewName

Name of the DNS view of the service. A DNS view is used in global server load balancing (GSLB) to return a predetermined IP address to a specific group of clients, which are identified by using a DNS policy.

monitorName

Name of the monitor to bind to the GSLB service.

Example

```
bind gslb service -viewName privateview 1.2.3.4
```

[Top](#)

unbind gslb service

Synopsis

```
unbind gslb service <serviceName> (-viewName <string> | -monitorName <string>@)
```

Description

Unbinds a DNS view or a monitor from a global server load balancing (GSLB) service.

Parameters

serviceName

Name of the GSLB service.

viewName

Name of the DNS view of the service. A DNS view specifies the IP address that must be returned to clients accessing the service from a specific location.

monitorName

Name of the monitor to unbind.

Example

```
unbind gslb service -viewName privateview
```

[Top](#)

show gslb service

Synopsis

```
show gslb service [<serviceName>] show gslb service stats - alias for 'stat gslb service'
```

Description

Displays the parameters of all the global server load balancing (GSLB) services configured on the appliance, or the parameters of just the specified service, and statistics related to the service. To display the parameters of all the GSLB services, do not specify a service name.

Parameters

serviceName

Name of the GSLB service.

Example

```
show gslb service sj_svc
```

[Top](#)

stat gslb service

Synopsis

```
stat gslb service [<serviceName>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-clearstats ( basic | full )]
```

Description

Displays the statistical data collected for a global server load balancing (GSLB) service.

Parameters

serviceName

Name of the GSLB service.

clearstats

Clear the statistics / counters Possible values: basic, full

[Top](#)

rename gslb service

Synopsis

```
rename gslb service <serviceName>@ <newName>@
```

Description

Renames a global server load balancing (GSLB) service.

Parameters

serviceName

Existing name of the GSLB service.

newName

New name for the GSLB service.

Example

```
rename gslb service gsl_svc gslb_svc_new
```

[Top](#)

gslb vserver

[[add](#) | [rm](#) | [set](#) | [unset](#) | [bind](#) | [unbind](#) | [enable](#) | [disable](#) | [show](#) | [stat](#) | [rename](#)]

add gslb vserver

Synopsis

```
add gslb vserver <name> <serviceType> [-dnsRecordType <dnsRecordType>] [-lbMethod
<lbMethod>] [-backupLBMethod <backupLBMethod>] [-netmask <netmask>] [-
v6netmasklen <positive_integer>] [-tolerance <positive_integer>] [-persistenceType
( SOURCEIP | NONE )] [-persistenceld <positive_integer>] [-persistMask <netmask>] [-
v6persistmasklen <positive_integer>] [-timeout <mins>] [-EDR ( ENABLED | DISABLED )]
[-MIR ( ENABLED | DISABLED )] [-disablePrimaryOnDown ( ENABLED | DISABLED )] [-
dynamicWeight <dynamicWeight>] [-state ( ENABLED | DISABLED )] [-
considerEffectiveState ( NONE | STATE_ONLY )] [-comment <string>] [-soMethod
<soMethod>] [-soPersistence ( ENABLED | DISABLED )] [-soPersistenceTimeOut
<positive_integer>] [-soThreshold <positive_integer>] [-soBackupAction
<soBackupAction>] [-appflowLog ( ENABLED | DISABLED )]
```

Description

Creates a global server load balancing (GSLB) virtual server.

Parameters

name

Name for the GSLB virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the virtual server is created. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver').

serviceType

Protocol used by services bound to the virtual server. Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, ANY, SIP_UDP, RADIUS, RDP, RTSP, MYSQL, MSSQL

ipType

The IP type for this GSLB vserver. Possible values: IPV4, IPV6 Default value: NSGSLB_IPV4

dnsRecordType

DNS record type to associate with the GSLB virtual server's domain name. Possible values: A, AAAA, CNAME Default value: NSGSLB_A

lbMethod

Load balancing method for the GSLB virtual server. Possible values: ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, SOURCEIPHASH, LEASTBANDWIDTH, LEASTPACKETS, STATICPROXIMITY, RTT, CUSTOMLOAD Default value: PEMGMT_LB_LEASTCONNS

backupSessionTimeout

A non zero value enables the feature whose minimum value is 2 minutes. The feature can be disabled by setting the value to zero. The created session is in effect for a specific client per domain. Maximum value: 1440

backupLBMethod

Backup load balancing method. Becomes operational if the primary load balancing method fails or cannot be used. Valid only if the primary method is based on either round-trip time (RTT) or static proximity. Possible values: ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, SOURCEIPHASH, LEASTBANDWIDTH, LEASTPACKETS, STATICPROXIMITY, RTT, CUSTOMLOAD

netmask

IPv4 network mask for use in the SOURCEIPHASH load balancing method. Default value: 0xFFFFFFFF

v6netmasklen

Number of bits to consider, in an IPv6 source IP address, for creating the hash that is required by the SOURCEIPHASH load balancing method. Default value: 128 Minimum value: 1 Maximum value: 128

tolerance

Site selection tolerance, in milliseconds, for implementing the RTT load balancing method. If a site's RTT deviates from the lowest RTT by more than the specified tolerance, the site is not considered when the NetScaler appliance makes a GSLB decision. The appliance implements the round robin method of global server load balancing between sites whose RTT values are within the specified tolerance. If the tolerance is 0 (zero), the appliance always sends clients the IP address of the site with the lowest RTT. Maximum value: 100

persistenceType

Use source IP address based persistence for the virtual server. After the load balancing method selects a service for the first packet, the IP address received in response to the DNS query is used for subsequent requests from the same client. Possible values: SOURCEIP, NONE

persistenceId

The persistence ID for the GSLB virtual server. The ID is a positive integer that enables GSLB sites to identify the GSLB virtual server, and is required if source IP address based or spill over based persistence is enabled on the virtual server. Maximum value: 65535

persistMask

The optional IPv4 network mask applied to IPv4 addresses to establish source IP address based persistence. Default value: 0xFFFFFFFF

v6persistmasklen

Number of bits to consider in an IPv6 source IP address when creating source IP address based persistence sessions. Default value: 128 Minimum value: 1 Maximum value: 128

timeout

Idle time, in minutes, after which a persistence entry is cleared. Default value: 2 Minimum value: 2 Maximum value: 1440

EDR

Send clients an empty DNS response when the GSLB virtual server is DOWN. Possible values: ENABLED, DISABLED Default value: DISABLED

MIR

Include multiple IP addresses in the DNS responses sent to clients. Possible values: ENABLED, DISABLED Default value: DISABLED

disablePrimaryOnDown

Continue to direct traffic to the backup chain even after the primary GSLB virtual server returns to the UP state. Used when spillover is configured for the virtual server. Possible values: ENABLED, DISABLED Default value: DISABLED

dynamicWeight

Specify if the appliance should consider the service count, service weights, or ignore both when using weight-based load balancing methods. The state of the number of services bound to the virtual server help the appliance to select the service. Possible values: SERVICECOUNT, SERVICEWEIGHT, DISABLED Default value: DISABLED

state

State of the GSLB virtual server. Possible values: ENABLED, DISABLED Default value: ENABLED

considerEffectiveState

If the primary state of all bound GSLB services is DOWN, consider the effective states of all the GSLB services, obtained through the Metrics Exchange Protocol (MEP), when determining the state of the GSLB virtual server. To consider the effective state, set the parameter to STATE_ONLY. To disregard the effective state, set the parameter to NONE. The effective state of a GSLB service is the ability of the corresponding virtual server to serve traffic. The effective state of the load balancing virtual server, which is transferred to the GSLB service, is UP even if only one virtual server in the backup chain of virtual servers is in the UP state. Possible values: NONE, STATE_ONLY Default value: NS_GSLB_DONOT_CONSIDER_BKPS

comment

Any comments that you might want to associate with the GSLB virtual server.

soMethod

Type of threshold that, when exceeded, triggers spillover. Available settings function as follows: * CONNECTION - Spillover occurs when the number of client connections exceeds the threshold. * DYNAMICCONNECTION - Spillover occurs when the number of client connections at the GSLB virtual server exceeds the sum of the maximum client (Max Clients) settings for bound GSLB services. Do not specify a spillover threshold for this setting, because the threshold is implied by the Max Clients settings of the bound GSLB services. * BANDWIDTH - Spillover occurs when the bandwidth consumed

by the GSLB virtual server's incoming and outgoing traffic exceeds the threshold. * HEALTH - Spillover occurs when the percentage of weights of the GSLB services that are UP drops below the threshold. For example, if services gslbSvc1, gslbSvc2, and gslbSvc3 are bound to a virtual server, with weights 1, 2, and 3, and the spillover threshold is 50%, spillover occurs if gslbSvc1 and gslbSvc3 or gslbSvc2 and gslbSvc3 transition to DOWN. * NONE - Spillover does not occur. Possible values: CONNECTION, DYNAMICCONNECTION, BANDWIDTH, HEALTH, NONE

soPersistence

If spillover occurs, maintain source IP address based persistence for both primary and backup GSLB virtual servers. Possible values: ENABLED, DISABLED Default value: DISABLED

soPersistenceTimeout

Timeout for spillover persistence, in minutes. Default value: 2 Minimum value: 2 Maximum value: 1440

soThreshold

Threshold at which spillover occurs. Specify an integer for the CONNECTION spillover method, a bandwidth value in kilobits per second for the BANDWIDTH method (do not enter the units), or a percentage for the HEALTH method (do not enter the percentage symbol). Minimum value: 1 Maximum value: 4294967287

soBackupAction

Action to be performed if spillover is to take effect, but no backup chain to spillover is usable or exists Possible values: DROP, ACCEPT, REDIRECT

appflowLog

Enable logging appflow flow information Possible values: ENABLED, DISABLED Default value: ENABLED

Example

```
add gslb vserver gvip http
```

[Top](#)

rm gslb vserver

Synopsis

```
rm gslb vserver <name>
```

Description

Removes a global server load balancing (GSLB) virtual server configured on the appliance.

Parameters

name

Name of the GSLB virtual server to remove.

Example

```
rm gslb vserver gvip
```

[Top](#)

set gslb vserver

Synopsis

```
set gslb vserver <name> [-dnsRecordType <dnsRecordType>] [-backupVServer <string>]
[-lbMethod <lbMethod>] [-backupLBMethod <backupLBMethod>] [-netmask <netmask>]
[-v6netmasklen <positive_integer>] [-tolerance <positive_integer>] [-persistenceType
( SOURCEIP | NONE )] [-persistenceld <positive_integer>] [-persistMask <netmask>] [-
v6persistmasklen <positive_integer>] [-timeout <mins>] [-EDR ( ENABLED | DISABLED )]
[-MIR ( ENABLED | DISABLED )] [-disablePrimaryOnDown ( ENABLED | DISABLED )] [-
dynamicWeight <dynamicWeight>] [-considerEffectiveState ( NONE | STATE_ONLY )] [-
soMethod <soMethod>] [-soPersistence ( ENABLED | DISABLED )] [-soPersistenceTimeOut
<positive_integer>] [-soThreshold <positive_integer>] [-soBackupAction
<soBackupAction>] [-serviceName <string> -weight <positive_integer>] [-domainName
<string>] [-TTL <secs>] [-backupIP <ip_addr|ipv6_addr|*>] [-cookieDomain <string>] [-
cookieTimeout <mins>] [-sitedomainTTL <secs>]] [-comment <string>] [-appflowLog
( ENABLED | DISABLED )]
```

Description

Modifies the specified parameters of a global server load balancing (GSLB) virtual server.

Parameters

name

Name of the GSLB virtual server.

ipType

The IP type for this GSLB vserver. Possible values: IPV4, IPV6 Default value: NSGSLB_IPV4

dnsRecordType

DNS record type to associate with the GSLB virtual server's domain name. Possible values: A, AAAA, CNAME Default value: NSGSLB_A

backupVServer

Name of the backup GSLB virtual server to which the appliance should forward requests if the status of the primary GSLB virtual server is down or exceeds its spillover threshold.

backupSessionTimeout

A non zero value enables the feature whose minimum value is 2 minutes. The feature can be disabled by setting the value to zero. The created session is in effect for a specific client per domain. Maximum value: 1440

lbMethod

Load balancing method for the GSLB virtual server. Possible values: ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, SOURCEIPHASH, LEASTBANDWIDTH, LEASTPACKETS, STATICPROXIMITY, RTT, CUSTOMLOAD Default value: PEMGMT_LB_LEASTCONNS

netmask

IPv4 network mask for use in the SOURCEIPHASH load balancing method. Default value: 0xFFFFFFFF

v6netmasklen

Number of bits to consider, in an IPv6 source IP address, for creating the hash that is required by the SOURCEIPHASH load balancing method. Default value: 128 Minimum value: 1 Maximum value: 128

tolerance

Site selection tolerance, in milliseconds, for implementing the RTT load balancing method. If a site's RTT deviates from the lowest RTT by more than the specified tolerance, the site is not considered when the NetScaler appliance makes a GSLB decision. The appliance implements the round robin method of global server load balancing between sites whose RTT values are within the specified tolerance. If the tolerance is 0 (zero), the appliance always sends clients the IP address of the site with the lowest RTT. Maximum value: 100

persistenceType

Persistence type for the virtual server. Possible value for this parameter is SOURCEIP, which specifies persistence based on the source IP address of inbound packets. After the load balancing method selects a link for transmission of the first packet, the IP address received in response to the DNS query is used for subsequent requests from the same client. Possible values: SOURCEIP, NONE

persistenceId

The persistence ID for the GSLB virtual server. The ID is a positive integer that enables GSLB sites to identify the GSLB virtual server, and is required if source IP address based or spill over based persistence is enabled on the virtual server. Maximum value: 65535

persistMask

The optional IPv4 network mask applied to IPv4 addresses to establish source IP address based persistence. Default value: 0xFFFFFFFF

v6persistmasklen

Number of bits to consider in an IPv6 source IP address when creating source IP address based persistence sessions. Default value: 128 Minimum value: 1 Maximum value: 128

timeout

Idle time, in minutes, after which a persistence entry is cleared. Default value: 2 Minimum value: 2 Maximum value: 1440

EDR

Send clients an empty DNS response when the GSLB virtual server is DOWN. Possible values: ENABLED, DISABLED Default value: DISABLED

MIR

Include multiple IP addresses in the DNS responses sent to clients. Possible values: ENABLED, DISABLED Default value: DISABLED

disablePrimaryOnDown

Continue to direct traffic to the backup chain even after the primary GSLB virtual server returns to the UP state. Used when spillover is configured for the virtual server. Possible values: ENABLED, DISABLED Default value: DISABLED

dynamicWeight

Specify if the appliance should consider the service count, service weights, or ignore both when using weight-based load balancing methods. The state of the number of services bound to the virtual server help the appliance to select the service. Possible values: SERVICECOUNT, SERVICEWEIGHT, DISABLED Default value: DISABLED

considerEffectiveState

If the primary state of all bound GSLB services is DOWN, consider the effective states of all the GSLB services, obtained through the Metrics Exchange Protocol (MEP), when determining the state of the GSLB virtual server. To consider the effective state, set the parameter to STATE_ONLY. To disregard the effective state, set the parameter to NONE. The effective state of a GSLB service is the ability of the corresponding virtual server to serve traffic. The effective state of the load balancing virtual server, which is transferred to the GSLB service, is UP even if only one virtual server in the backup chain of virtual servers is in the UP state. Possible values: NONE, STATE_ONLY Default value: NS_GSLB_DONOT_CONSIDER_BKPS

soMethod

Type of threshold that, when exceeded, triggers spillover. Available settings function as follows: * CONNECTION - Spillover occurs when the number of client connections exceeds the threshold. * DYNAMICCONNECTION - Spillover occurs when the number of client connections at the GSLB virtual server exceeds the sum of the maximum client (Max Clients) settings for bound GSLB services. Do not specify a spillover threshold for this setting, because the threshold is implied by the Max Clients settings of the bound GSLB services. * BANDWIDTH - Spillover occurs when the bandwidth consumed by the GSLB virtual server's incoming and outgoing traffic exceeds the threshold. * HEALTH - Spillover occurs when the percentage of weights of the GSLB services that are UP drops below the threshold. For example, if services gslbSvc1, gslbSvc2, and gslbSvc3 are bound to a virtual server, with weights 1, 2, and 3, and the spillover threshold is 50%, spillover occurs if gslbSvc1 and gslbSvc3 or gslbSvc2 and gslbSvc3 transition to DOWN. * NONE - Spillover does not occur. Possible values: CONNECTION, DYNAMICCONNECTION, BANDWIDTH, HEALTH, NONE

soPersistence

If spillover occurs, maintain source IP address based persistence for both primary and backup GSLB virtual servers. Possible values: ENABLED, DISABLED Default value: DISABLED

soPersistenceTimeout

Timeout for spillover persistence, in minutes. Default value: 2 Minimum value: 2 Maximum value: 1440

soThreshold

Threshold at which spillover occurs. Specify an integer for the CONNECTION spillover method, a bandwidth value in kilobits per second for the BANDWIDTH method (do not enter the units), or a percentage for the HEALTH method (do not enter the percentage symbol). Minimum value: 1 Maximum value: 4294967287

soBackupAction

Action to be performed if spillover is to take effect, but no backup chain to spillover is usable or exists Possible values: DROP, ACCEPT, REDIRECT

serviceName

Name of the GSLB service for which to change the weight.

domainName

Domain name for which to change the time to live (TTL) and/or backup service IP address.

comment

Any comments that you might want to associate with the GSLB virtual server.

appflowLog

Enable logging appflow flow information Possible values: ENABLED, DISABLED Default value: ENABLED

Example

```
set gslb vserver gvip -persistenceType SOURCEIP
```

[Top](#)

unset gslb vserver

Synopsis

```
unset gslb vserver <name>@ [-backupVServer] [-dnsRecordType] [-lbMethod] [-  
backupLBMethod] [-netmask] [-v6netmasklen] [-tolerance] [-persistenceType] [-  
persistenceld] [-persistMask] [-v6persistmasklen] [-timeout] [-EDR] [-MIR] [-  
disablePrimaryOnDown] [-dynamicWeight] [-considerEffectiveState] [-soMethod] [-  
soPersistence] [-soPersistenceTimeOut] [-soBackupAction] [-serviceName] [-weight] [-  
comment] [-appflowLog]
```

Description

Removes the specified settings from the specified global server load balancing (GSLB) virtual server. Attributes for which a default value is available revert to their default values..Refer to the set gslb vserver command for meanings of the arguments.

Example

```
unset gslb vserver lb_vip -backupVServer
For multiple gslb vservers the command is:
unset gslb vserver lb_vip[1-3] -backupVServer
```

[Top](#)**bind gslb vserver****Synopsis**

```
bind gslb vserver <name> ((-serviceName <string> [-weight <positive_integer>]) | (-
domainName <string> [-TTL <secs>] [-backupIP <ip_addr|ipv6_addr|*>] [-cookieDomain
<string>] [-cookieTimeout <mins>] [-sitedomainTTL <secs>]) | (-policyName <string>@
[-priority <positive_integer>])) [-gotoPriorityExpression <expression>]
```

Description

Binds a domain, service, backup IP address, or cookie domain to a GSLB virtual server.

Parameters**name**

Name of the virtual server on which to perform the binding operation.

serviceName

Name of the GSLB service for which to change the weight.

domainName

Domain name for which to change the time to live (TTL) and/or backup service IP address.

policyName

Name of the policy bound to the GSLB vserver.

Example

```
bind gslb vserver gvip -domainName www.mynw.com
```

[Top](#)**unbind gslb vserver****Synopsis**

```
unbind gslb vserver <name> (-serviceName <string> | (-domainName <string> [-
backupIP] [-cookieDomain]) | -policyName <string>@)
```

Description

Unbinds the domain or service from the GSLB virtual server.

Parameters

name

Name of the GSLB virtual server.

serviceName

Name of the GSLB service for which to change the weight.

domainName

Domain name for which to change the time to live (TTL) and/or backup service IP address.

policyName

The policy that has been bound to this load balancing virtual server, using the `###bind gslb vserver###` command.

Example

```
unbind gslb vserver gvip -domainName www.mynw.com
```

[Top](#)

enable gslb vserver

Synopsis

`enable gslb vserver <name>@`

Description

Enables a global server load balancing (GSLB) virtual server that has been disabled. (A GSLB virtual server is enabled by default.)

Parameters

name

Name of the GSLB virtual server to enable.

Example

```
enable gslb vserver gslb_vip
    To enable multiple gslb vservers use the
    following command:
    enable gslb vserver gslb_vip[1-3]
```

[Top](#)

disable gslb vserver

Synopsis

`disable gslb vserver <name>@`

Description

Disables a global server load balancing (GSLB) virtual server and takes it out of service.

Parameters

name

Name of the GSLB virtual server to disable.

Example

```
disable gslb vserver gslb_vip
    To disable multiple gslb vservers use the
    following command:
    disable gslb vserver gslb_vip[1-3]
```

[Top](#)

show gslb vserver

Synopsis

show gslb vserver [<name>] show gslb vserver stats - alias for 'stat gslb vserver'

Description

Displays the parameters of all the global server load balancing (GSLB) virtual servers configured on the appliance, or the parameters of the specified GSLB virtual server.

Parameters

name

Name of the GSLB virtual server.

Example

```
show gslb vserver gvip
```

[Top](#)

stat gslb vserver

Synopsis

stat gslb vserver [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-clearstats (basic | full)]

Description

Displays statistics associated with a global server load balancing (GSLB) virtual server.

Parameters

name

Name of the GSLB virtual server for which to display statistics. If you do not specify a name, statistics are displayed for all GSLB virtual servers.

clearstats

Clear the statistics / counters Possible values: basic, full

[Top](#)

rename gslb vserver

Synopsis

```
rename gslb vserver <name>@ <newName>@
```

Description

Renames a global server load balancing (GSLB) virtual server.

Parameters

name

Existing name of the GSLB virtual server.

newName

New name for the GSLB virtual server.

Example

```
rename gslb vserver gsl_vsvr gslb_vsvr_new
```

[Top](#)

gslb runningConfig

show gslb runningConfig

Synopsis

```
show gslb runningConfig
```

Description

Displays the complete GSLB configuration running on the NetScaler appliance. In addition to the saved configuration, the running configuration includes GSLB settings that have not yet been saved to the NetScaler configuration file (ns.conf).

gslb domain

stat gslb domain

Synopsis

```
stat gslb domain [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile  
<input_filename>] [-clearstats ( basic | full )]
```

Description

Displays the statistics associated with a global server load balancing (GSLB) domain.

Parameters

name

Name of the GSLB domain for which to display statistics. If you do not specify a name, statistics are shown for all configured GSLB domains.

clearstats

Clear the statistics / counters Possible values: basic, full

gslb ldnentries

[[clear](#) | [show](#)]

clear gslb ldnentries

Synopsis

```
clear gslb ldnentries
```

Description

Clears all the local DNS (LDNS) entries created on the NetScaler appliance. LDNS entries store network metrics for RTT learned from the packets exchanged with LDNS servers.

[Top](#)

show gslb ldnentries

Synopsis

```
show gslb ldnentries
```

Description

Displays the local DNS (LDNS) entries created on the NetScaler appliance. LDNS entries store network metrics for RTT learned from the packets exchanged with LDNS servers.

Example

```
show gslb ldnentries
```

[Top](#)

gslb parameter

[[set](#) | [unset](#) | [show](#)]

set gslb parameter

Synopsis

```
set gslb parameter [-ldnsEntryTimeout <secs>] [-RTTTolerance <msecs>] [-ldnsMask  
<netmask>] [-v6ldnsmasklen <positive_integer>] [-ldnsProbeOrder <ldnsProbeOrder> ...]  
[-dropLdnsReq ( ENABLED | DISABLED )]
```

Description

Sets various global GSLB parameters.

Parameters

ldnsEntryTimeout

Time, in seconds, after which an inactive LDNS entry is removed. Default value: 180
Maximum value: 65534

RTTTolerance

Tolerance, in milliseconds, for newly learned round-trip time (RTT) values. If the difference between the old RTT value and the newly computed RTT value is less than or equal to the specified tolerance value, the LDNS entry in the network metric table is not updated with the new RTT value. Prevents the exchange of metrics when variations in RTT values are negligible. Default value: 5 Minimum value: 1 Maximum value: 100

ldnsMask

The IPv4 network mask with which to create LDNS entries. Default value: 0xFFFFFFFF

v6ldnsmasklen

Mask for creating LDNS entries for IPv6 source addresses. The mask is defined as the number of leading bits to consider, in the source IP address, when creating an LDNS entry. Default value: 128 Minimum value: 1 Maximum value: 128

ldnsProbeOrder

Order in which monitors should be initiated to calculate RTT. Possible values: PING, DNS, TCP Default value: ARRAY(0x96e0060)

dropLdnsReq

Drop LDNS requests if round-trip time (RTT) information is not available. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

```
set gslb parameter -ldnsMask 255.255.0.0
```

[Top](#)

unset gslb parameter

Synopsis

unset gslb parameter [-ldnsEntryTimeout] [-RTTTolerance] [-ldnsMask] [-v6ldnsmasklen] [-ldnsProbeOrder] [-dropLdnsReq]

Description

Use this command to remove gslb parameter settings. Refer to the set gslb parameter command for meanings of the arguments.

[Top](#)

show gslb parameter

Synopsis

show gslb parameter

Description

Displays the global GSLB parameters.

Example

```
show gslb parameter
```

[Top](#)

gslb ldnsentry

rm gslb ldnsentry

Synopsis

rm gslb ldnsentry <IPAddress>

Description

Removes the LDNS entry for the specified LDNS IP address.

Parameters

IPAddress

IP address of the LDNS server.

Example

```
rm gslb ldnsentry 10.102.27.226
```

gslb config

sync gslb config

Synopsis

```
sync gslb config [-preview | -forceSync <string> | -command <string> | -nowarn | -  
saveconfig] [-debug]
```

Description

Synchronizes the GSLB running configuration on all NetScaler appliances participating in the GSLB setup. The appliance on which this command is run is considered the master node. All GSLB sites configured on the master node and not having a parent site are synchronized with the master node.

Parameters

preview

Do not synchronize the GSLB sites, but display the commands that would be applied on the slave node upon synchronization. Mutually exclusive with the Save Configuration option.

debug

Generate verbose output when synchronizing the GSLB sites. The Debug option generates more verbose output than the sync gslb config command in which the option is not used, and is useful for analyzing synchronization issues.

forceSync

Force synchronization of the specified site even if a dependent configuration on the remote site is preventing synchronization or if one or more GSLB entities on the remote site have the same name but are of a different type. You can specify either the name of the remote site that you want to synchronize with the local site, or you can specify All Sites in the configuration utility (the string all-sites in the CLI). If you specify All Sites, all the sites in the GSLB setup are synchronized with the site on the master node. Note: If you select the Force Sync option, the synchronization starts without displaying the commands that are going to be executed.

nowarn

Suppress the warning and the confirmation prompt that are displayed before site synchronization begins. This option can be used in automation scripts that must not be interrupted by a prompt.

saveconfig

Save the configuration on all the nodes participating in the synchronization process, automatically. The master saves its configuration immediately before synchronization begins. Slave nodes save their configurations after the process of synchronization is complete. A slave node saves its configuration only if the configuration difference was successfully applied to it. Mutually exclusive with the Preview option.

command

Run the specified command on the master node and then on all the slave nodes. You cannot use this option with the force sync and preview options.

Example

```
sync gslb config
```

gslb syncStatus

show gslb syncStatus

Synopsis

show gslb syncStatus

Description

Displays the status of the last GSLB configuration synchronization.

Parameters

response
gslb sync status as text blob

HA Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [HA node](#)
- ♦ [HA sync](#)
- ♦ [HA files](#)
- ♦ [HA failover](#)

HA node

[[add](#) | [rm](#) | [set](#) | [unset](#) | [bind](#) | [unbind](#) | [show](#) | [stat](#)]

add HA node

Synopsis

add HA node <id> <IPAddress> [-inc (ENABLED | DISABLED)]

Description

Adds a peer node to an HA configuration. Each node must add the other as a peer. An algorithm determines which node becomes primary and which becomes secondary.

Parameters

id
Number that uniquely identifies the peer node. Minimum value: 1 Maximum value: 64

IPAddress

The NSIP or NSIP6 address of the node to be added for an HA configuration. This setting is neither propagated nor synchronized.

inc

This option is required if the HA nodes reside on different networks. When this mode is enabled, the following independent network entities and configurations are neither propagated nor synced to the other node: MIPs, SNIPs, VLANs, routes (except LLB routes), route monitors, RNAT rules (except any RNAT rule with a VIP as the NAT IP), and dynamic routing configurations. They are maintained independently on each node. Possible values: ENABLED, DISABLED Default value: DISABLED

[Top](#)

rm HA node

Synopsis

```
rm HA node <id>
```

Description

Removes the peer node from the HA configuration. To completely remove both the nodes from the HA configuration, you have to log on to each node and remove its peer node.

Parameters

id

Number that uniquely identifies the peer node. CLI users: To learn the ID of the peer node, run the show HA node command on the local node. Maximum value: 64

[Top](#)

set HA node

Synopsis

```
set HA node [-haStatus <haStatus>] [-haSync ( ENABLED | DISABLED )] [-haProp  
( ENABLED | DISABLED )] [-helloInterval <msecs>] [-deadInterval <secs>] [-failSafe ( ON  
| OFF )] [-maxFlips <positive_integer>] [-maxFlipTime <positive_integer>] [-syncvlan  
<positive_integer>]
```

Description

Sets the specified HA related parameters for the node. The settings are neither propagated nor synchronized to the peer node.

Parameters

id

Number that uniquely identifies the peer node. Maximum value: 64

haStatus

The HA status of the node. The HA status STAYSECONDARY is used to force the secondary device stay as secondary independent of the state of the Primary device. For example, in an existing HA setup, the Primary node has to be upgraded and this process would take few seconds. During the upgradation, it is possible that the

Primary node may suffer from a downtime for a few seconds. However, the Secondary should not take over as the Primary node. Thus, the Secondary node should remain as Secondary even if there is a failure in the Primary node. STAYPRIMARY configuration keeps the node in primary state in case if it is healthy, even if the peer node was the primary node initially. If the node with STAYPRIMARY setting (and no peer node) is added to a primary node (which has this node as the peer) then this node takes over as the new primary and the older node becomes secondary. ENABLED state means normal HA operation without any constraints/ preferences. DISABLED state disables the normal HA operation of the node. Possible values: ENABLED, STAYSECONDARY, DISABLED, STAYPRIMARY

haSync

Automatically maintain synchronization by duplicating the configuration of the primary node on the secondary node. This setting is not propagated. Automatic synchronization requires that this setting be enabled (the default) on the current secondary node. Synchronization uses TCP port 3010. Possible values: ENABLED, DISABLED Default value: ENABLED

haProp

Automatically propagate all commands from the primary to the secondary node, except the following: * All HA configuration related commands. For example, add ha node, set ha node, and bind ha node. * All Interface related commands. For example, set interface and unset interface. * All channels related commands. For example, add channel, set channel, and bind channel. The propagated command is executed on the secondary node before it is executed on the primary. If command propagation fails, or if command execution fails on the secondary, the primary node executes the command and logs an error. Command propagation uses port 3011. Note: After enabling propagation, run force synchronization on either node. Possible values: ENABLED, DISABLED Default value: ENABLED

helloInterval

Interval, in milliseconds, between heartbeat messages sent to the peer node. The heartbeat messages are UDP packets sent to port 3003 of the peer node. Default value: 200 Minimum value: 200 Maximum value: 1000

deadInterval

Number of seconds after which a peer node is marked DOWN if heartbeat messages are not received from the peer node. Default value: 3 Minimum value: 3 Maximum value: 60

failSafe

Keep one node primary if both nodes fail the health check, so that a partially available node can back up data and handle traffic. This mode is set independently on each node. Possible values: ON, OFF Default value: OFF

maxFlips

Max number of flips allowed before becoming sticky primary

maxFlipTime

Interval after which flipping of node states can again start

syncvlan

Vlan on which HA related communication is sent. This include sync, propagation , connection mirroring , LB persistency config sync, persistent session sync and session

state sync. However HA heartbeats can go all interfaces. Minimum value: 1 Maximum value: 4096

[Top](#)

unset HA node

Synopsis

unset HA node [-haStatus] [-haSync] [-haProp] [-helloInterval] [-deadInterval] [-failSafe] [-maxFlips] [-maxFlipTime] [-syncvlan]

Description

Use this command to remove HA node settings. Refer to the set HA node command for meanings of the arguments.

[Top](#)

bind HA node

Synopsis

bind HA node [<id>] (-routeMonitor <ip_addr|ipv6_addr|*> [<netmask>])

Description

Adds a route monitor to the local node. When a NetScaler appliance has only static routes for reaching a network, and you want to create a route monitor for the network, you must enable monitored static routes (MSR) for the static routes. Route Monitors are supported both in non-INC and INC modes.

Parameters

id

Number that uniquely identifies the local node. The ID of the local node is always 0. Maximum value: 64

routeMonitor

A route that you want the NetScaler appliance to monitor in its internal routing table. You can specify an IPv4 address or network, or an IPv6 address or network prefix. If you specify an IPv4 network address or IPv6 network prefix, the appliance monitors any route that matches the network or prefix.

[Top](#)

unbind HA node

Synopsis

unbind HA node [<id>] (-routeMonitor <ip_addr|ipv6_addr|*> [<netmask>])

Description

Removes a route monitor entry from the local node. The NetScaler appliance stops monitoring the route in its internal routing table.

Parameters

id

Number that uniquely identifies the local node. The ID of the local node is always 0.
Maximum value: 64

routeMonitor

The route specified in the route monitor entry that you want to remove from the NetScaler appliance. Can be an IPv4 address or network, or an IPv6 address or network prefix.

[Top](#)

show HA node

Synopsis

show HA node [<id>]

Description

Displays the HA settings of both nodes or, if you specify a node, just the specified node. You can use this command to display the master state (primary or secondary) of the nodes in a HA configuration.

Parameters

id

ID of the node whose HA settings you want to display. (The ID of the local node is always 0.) Maximum value: 64

Example

```
An example of the command's output is as follows:  
2 configured nodes:  
1) Node ID: 0 IP: 192.168.100.5 Primary node  
2) Node ID: 2 IP: 192.168.100.112 Secondary node
```

[Top](#)

stat HA node

Synopsis

stat HA node [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile
<input_filename>] [-clearstats (basic | full)]

Description

Display the statistics related to HA configuration.

Parameters

clearstats

Clear the statistics / counters Possible values: basic, full

[Top](#)

HA sync

force HA sync

Synopsis

```
force HA sync [-force [-save ( YES | NO )]]
```

Description

Forces duplication of the primary node's configuration on the secondary node. Can be executed from either node. Note: This command fails under any of the following conditions: * Synchronization is already in progress. * The secondary node is disabled. * Synchronization is disabled on either node * The secondary node is not accessible from the primary. * You run the command on a standalone appliance.

Parameters

force

Force synchronization regardless of the state of HA propagation and HA synchronization on either node.

save

After synchronization, automatically save the configuration in the secondary node configuration file (ns.conf) without prompting for confirmation. Possible values: YES, NO Default value: VAL_NOT_SET

Example

```
Can be used in following formats:
>force sync <cr>
>force sync -force <cr>
>force sync -force -save [yes|
no]<cr>
```

HA files

sync HA files

Synopsis

```
sync HA files [<Mode> ...]
```

Description

Synchronize various configuration files from the primary node to the secondary. You can run this command from either node. Files that are present on only the secondary and are specific to the secondary are not deleted. This command fails if the secondary node is disabled, the secondary node is not accessible from the primary, or you enter the command on a standalone appliance.

Parameters

Mode

Specify one of the following modes of synchronization. * all - Synchronize files related to system configuration, Access Gateway bookmarks, SSL certificates, SSL CRL lists, HTML injection scripts, and Application Firewall XML objects. * bookmarks - Synchronize all Access Gateway bookmarks. * ssl - Synchronize all certificates, keys, and CRLs for the SSL feature. * htmlinjection. Synchronize all scripts configured for the HTML injection feature. * imports. Synchronize all XML objects (for example, WSDLs, schemas, error pages) configured for the application firewall. * misc - Synchronize all license files and the rc.conf file. * all_plus_misc - Synchronize files related to system configuration, Access Gateway bookmarks, SSL certificates, SSL CRL lists, HTML injection scripts, application firewall XML objects, licenses, and the rc.conf file.

Example

```
sync files all
```

HA failover

force HA failover

Synopsis

force HA failover [-force]

Description

Forces an HA failover. Can be initiated from either node. A forced failover is not propagated or synchronized., Note: This command fails under any of the following conditions: * The secondary node is disabled or configured to remain secondary. * The primary node is configured to remain primary. * The state of the peer node is unknown. * You run the command on a standalone appliance.

Parameters

force

Force a failover without prompting for confirmation.

IPSec Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [ipsec profile](#)
- ♦ [ipsec parameter](#)
- ♦ [ipsec counters](#)

ipsec profile

[[add](#) | [show](#) | [rm](#)]

add ipsec profile

Synopsis

```
add ipsec profile <name> [-ikeVersion ( V1 | V2 )] [-encAlgo ( AES | 3DES ) ...] [-hashAlgo <hashAlgo> ...] [-lifetime <positive_integer>] (-psk | (-publickey <string> -privatekey <string> -peerPublicKey <string>)) [-livenessCheckInterval <positive_integer>] [-replayWindowSize <positive_integer>] [-ikeRetryInterval <positive_integer>] [-retransmissiontime <positive_integer>]
```

Description

Add an ipsec profile.

Parameters

name

The name of the ipsec profile

ikeVersion

IKE Protocol Version

encAlgo

Type of encryption algorithm

hashAlgo

Type of hashing algorithm

lifetime

Lifetime of SA in seconds Minimum value: 60 Maximum value: 31536000

psk

Pre shared key value

publickey

Public key file path

livenessCheckInterval

Number of seconds after which a notify payload is sent to check the liveliness of the peer. Additional retries are done as per retransmit interval setting. Zero value disables liveliness checks. Maximum value: 64999

replayWindowSize

IPSec Replay window size for the data traffic Maximum value: 16384

ikeRetryInterval

IKE retry interval for bringing up the connection Minimum value: 60 Maximum value: 3600

retransmissiontime

The interval in seconds to retry sending the IKE messages to peer, three consecutive attempts are done with doubled interval after every failure. Minimum value: 1 Maximum value: 99

[Top](#)

show ipsec profile

Synopsis

show ipsec profile [<name>]

Description

Display all of the configured ipsec peers

Parameters

name

The name of the ipsec profile

Example

```
show ipsec profile
```

[Top](#)

rm ipsec profile

Synopsis

rm ipsec profile <name>

Description

Remove an ipsec peer

Parameters

name

The name of the ipsec profile.

Example

```
rm ipsec profile
```

[Top](#)

ipsec parameter

[[set](#) | [unset](#) | [show](#)]

set ipsec parameter

Synopsis

set ipsec parameter [-ikeVersion (V1 | V2)] [-encAlgo (AES | 3DES) ...] [-hashAlgo <hashAlgo> ...] [-lifetime <positive_integer>] [-livenessCheckInterval

```
<positive_integer>] [-replayWindowSize <positive_integer>] [-ikeRetryInterval  
<positive_integer>] [-retransmissiontime <positive_integer>]
```

Description

Set global parameters for IPSEC

Parameters

ikeVersion

IKE Protocol Version Default value: KMP_IKEV2

encAlgo

Type of encryption algorithm Default value: ENC_AES

hashAlgo

Type of hashing algorithm Default value: HMAC_SHA256

lifetime

Lifetime of SA in seconds Minimum value: 60 Maximum value: 31536000

livenessCheckInterval

Number of seconds after which a notify payload is sent to check the liveness of the peer. Additional retries are done as per retransmit interval setting. Zero value disables liveness checks. Maximum value: 64999

replayWindowSize

IPSec Replay window size for the data traffic Maximum value: 16384

ikeRetryInterval

IKE retry interval for bringing up the connection Minimum value: 60 Maximum value: 3600

retransmissiontime

The interval in seconds to retry sending the IKE messages to peer, three consecutive attempts are done with doubled interval after every failure., increases for every retransmit till 6 retransmits. Minimum value: 1 Maximum value: 99

[Top](#)

unset ipsec parameter

Synopsis

```
unset ipsec parameter [-ikeVersion] [-encAlgo] [-hashAlgo] [-lifetime] [-  
livenessCheckInterval] [-replayWindowSize] [-ikeRetryInterval] [-retransmissiontime]
```

Description

Set global parameters for IPSEC. Refer to the set ipsec parameter command for meanings of the arguments.

[Top](#)

show ipsec parameter

Synopsis

```
show ipsec parameter
```

Description

Show global parameters for IPSEC

[Top](#)

ipsec counters

stat ipsec counters

Synopsis

```
stat ipsec counters [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile  
<input_filename>] [-clearstats ( basic | full )]
```

Description

Display statistics for secure tunnel sessions.

Parameters**clearstats**

Clear the statistics / counters Possible values: basic, full

Example

```
stat ipsec
```

LB Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [lb monitor](#)
- ♦ [lb route](#)
- ♦ [lb route6](#)
- ♦ [lb vserver](#)
- ♦ [lb metricTable](#)
- ♦ [lb monbindings](#)
- ♦ [lb persistentSessions](#)
- ♦ [lb group](#)
- ♦ [lb sipParameters](#)
- ♦ [lb parameter](#)

lb monitor

[[add](#) | [rm](#) | [set](#) | [unset](#) | [enable](#) | [disable](#) | [bind](#) | [unbind](#) | [show](#)]

add lb monitor

Synopsis

```
add lb monitor <monitorName> <type> [-action <action>] [-respCode <int[-int]> ...] [-
httpRequest <string>] [-rtspRequest <string>] [-customHeaders <string>] [-maxForwards
<positive_integer>] [-sipMethod <sipMethod>] [-sipURI <string>] [-sipregURI <string>] [-
send <string>] [-recv <string>] [-query <string>] [-queryType <queryType>] [-scriptName
<string>] [-scriptArgs <string>] [-dispatcherIP <ip_addr>] [-dispatcherPort <port>] [-
userName <string>] {-password } {-secondaryPassword } [-logonpointName <string>] [-
lasVersion <string>] {-radKey } [-radNASid <string>] [-radNASip <ip_addr>] [-
radAccountType <positive_integer>] [-radFramedIP <ip_addr>] [-radAPN <string>] [-
radMSISDN <string>] [-radAccountSession <string>] [-LRTM ( ENABLED | DISABLED )] [-
deviation <positive_integer> [<units>]] [-interval <integer> [<units>]] [-resptimeout
<integer> [<units>]] [-resptimeoutThresh <positive_integer>] [-retries <integer>] [-
failureRetries <integer>] [-alertRetries <integer>] [-successRetries <integer>] [-
downTime <integer> [<units>]] [-destIP <ip_addr|ipv6_addr>] [-destPort <port>] [-state
( ENABLED | DISABLED )] [-reverse ( YES | NO )] [-transparent ( YES | NO )] [-ipTunnel
( YES | NO )] [-tos ( YES | NO )] [-tosld <positive_integer>] [-secure ( YES | NO )] [-
validateCred ( YES | NO )] [-domain <string>] [-IPAddress <ip_addr|ipv6_addr|*> ...] [-
group <string>] [-fileName <string>] [-baseDN <string>] [-bindDN <string>] [-filter
<string>] [-attribute <string>] [-database <string>] [-sqlQuery <text>] [-evalRule
<expression>] [-mssqlProtocolVersion <mssqlProtocolVersion>] [-snmpOID <string>] [-
snmpCommunity <string>] [-snmpThreshold <string>] [-snmpVersion ( V1 | V2 )] [-
metricTable <string>] [-application <string>] [-sitePath <string>] [-storename <string>]
[-storefrontacctservice ( YES | NO )] [-netProfile <string>] [-originHost <string>] [-
originRealm <string>] [-hostIPAddress <ip_addr|ipv6_addr|*>] [-vendorId
<positive_integer>] [-productName <string>] [-firmwareRevision <positive_integer>] [-
authApplicationId <positive_integer> ...] [-acctApplicationId <positive_integer> ...] [-
inbandSecurityId ( NO_INBAND_SECURITY | TLS )] [-supportedVendorIds
<positive_integer> ...] [-vendorSpecificVendorId <positive_integer> [-
vendorSpecificAuthApplicationIds <positive_integer> ...] [-
vendorSpecificAcctApplicationIds <positive_integer> ...]] [-kcdAccount <string>] [-
storedb ( ENABLED | DISABLED )]
```

Description

Creates a monitor that you can bind to load balancing services. The monitor periodically sends probes to those services to test their availability.

Parameters

monitorName

Name for the monitor. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my monitor" or 'my monitor').

type

Type of monitor that you want to create. Possible values: PING, TCP, HTTP, TCP-ECV, HTTP-ECV, UDP-ECV, DNS, FTP, LDNS-PING, LDNS-TCP, LDNS-DNS, RADIUS, USER, HTTP-INLINE, SIP-UDP, LOAD, FTP-EXTENDED, SMTP, SNMP, NNTP, MYSQL, MYSQL-ECV, MSSQL-ECV, ORACLE-ECV, LDAP, POP3, CITRIX-XML-SERVICE, CITRIX-WEB-INTERFACE, DNS-TCP, RTSP, ARP, CITRIX-AG, CITRIX-AAC-LOGINPAGE, CITRIX-AAC-LAS, CITRIX-XD-DDC, ND6, CITRIX-WI-EXTENDED, DIAMETER, RADIUS_ACCOUNTING, STOREFRONT

action

Action to perform when the response to an inline monitor (a monitor of type HTTP-INLINE) indicates that the service is down. A service monitored by an inline monitor is considered DOWN if the response code is not one of the codes that have been specified for the Response Code parameter. Available settings function as follows: * NONE - Do not take any action. However, the show service command and the show lb monitor command indicate the total number of responses that were checked and the number of consecutive error responses received after the last successful probe. * LOG - Log the event in NSLOG or SYSLOG. * DOWN - Mark the service as being down, and then do not direct any traffic to the service until the configured down time has expired. Persistent connections to the service are terminated as soon as the service is marked as DOWN. Also, log the event in NSLOG or SYSLOG. Possible values: NONE, LOG, DOWN Default value: SM_DOWN

respCode

Response codes for which to mark the service as UP. For any other response code, the action performed depends on the monitor type. HTTP monitors and RADIUS monitors mark the service as DOWN, while HTTP-INLINE monitors perform the action indicated by the Action parameter.

httpRequest

HTTP request to send to the server (for example, "HEAD /file.html").

rtspRequest

RTSP request to send to the server (for example, "OPTIONS *").

customHeaders

Custom header string to include in the monitoring probes.

maxForwards

Maximum number of hops that the SIP request used for monitoring can traverse to reach the server. Applicable only to monitors of type SIP-UDP. Default value: 1
Maximum value: 255

sipMethod

SIP method to use for the query. Applicable only to monitors of type SIP-UDP. Possible values: OPTIONS, INVITE, REGISTER

sipURI

SIP URI string to send to the service (for example, sip:sip.test). Applicable only to monitors of type SIP-UDP.

sipregURI

SIP user to be registered. Applicable only if the monitor is of type SIP-UDP and the SIP Method parameter is set to REGISTER.

send

String to send to the service. Applicable to TCP-ECV, HTTP-ECV, and UDP-ECV monitors.

recv

String expected from the server for the service to be marked as UP. Applicable to TCP-ECV, HTTP-ECV, and UDP-ECV monitors.

query

Domain name to resolve as part of monitoring the DNS service (for example, example.com).

queryType

Type of DNS record for which to send monitoring queries. Set to Address for querying A records, AAAA for querying AAAA records, and Zone for querying the SOA record. Possible values: Address, Zone, AAAA

scriptName

Path and name of the script to execute. The script must be available on the NetScaler appliance, in the /nsconfig/monitors/ directory.

scriptArgs

String of arguments for the script. The string is copied verbatim into the request.

dispatcherIP

IP address of the dispatcher to which to send the probe.

dispatcherPort

Port number on which the dispatcher listens for the monitoring probe.

userName

User name with which to probe the RADIUS, NNTP, FTP, FTP-EXTENDED, MYSQL, MSSQL, POP3, CITRIX-AG, CITRIX-XD-DDC, or CITRIX-WI-EXTENDED server.

password

Password that is required for logging on to the RADIUS, NNTP, FTP, FTP-EXTENDED, MYSQL, MSSQL, POP3, CITRIX-AG, CITRIX-XD-DDC, or CITRIX-WI-EXTENDED server. Used in conjunction with the user name specified for the User Name parameter.

secondaryPassword

Secondary password that users might have to provide to log on to the Access Gateway server. Applicable to CITRIX-AG monitors.

logonpointName

Name of the logon point that is configured for the Citrix Access Gateway Advanced Access Control software. Required if you want to monitor the associated login page or Logon Agent. Applicable to CITRIX-AAC-LAS and CITRIX-AAC-LOGINPAGE monitors.

lasVersion

Version number of the Citrix Advanced Access Control Logon Agent. Required by the CITRIX-AAC-LAS monitor.

radKey

Authentication key (shared secret text string) for RADIUS clients and servers to exchange. Applicable to monitors of type RADIUS and RADIUS_ACCOUNTING.

radNASid

NAS-Identifier to send in the Access-Request packet. Applicable to monitors of type RADIUS.

radNASip

Network Access Server (NAS) IP address to use as the source IP address when monitoring a RADIUS server. Applicable to monitors of type RADIUS and RADIUS_ACCOUNTING.

radAccountType

Account Type to be used in Account Request Packet. Applicable to monitors of type RADIUS_ACCOUNTING. Default value: 1 Maximum value: 15

radFramedIP

Source ip with which the packet will go out . Applicable to monitors of type RADIUS_ACCOUNTING.

radAPN

Called Station Id to be used in Account Request Packet. Applicable to monitors of type RADIUS_ACCOUNTING.

radMSISDN

Calling Stations Id to be used in Account Request Packet. Applicable to monitors of type RADIUS_ACCOUNTING.

radAccountSession

Account Session ID to be used in Account Request Packet. Applicable to monitors of type RADIUS_ACCOUNTING.

LRTM

Calculate the least response times for bound services. If this parameter is not enabled, the appliance does not learn the response times of the bound services. Also used for LRTM load balancing. Possible values: ENABLED, DISABLED

deviation

Time value added to the learned average response time in dynamic response time monitoring (DRTM). When a deviation is specified, the appliance learns the average response time of bound services and adds the deviation to the average. The final value is then continually adjusted to accommodate response time variations over time. Specified in milliseconds, seconds, or minutes. Maximum value: 20939000

interval

Time interval between two successive probes. Must be greater than the value of Response Time-out. Default value: 5 Minimum value: 1 Maximum value: 20940000

resptimeout

Amount of time for which the appliance must wait before it marks a probe as FAILED. Must be less than the value specified for the Interval parameter. Note: For UDP-ECV monitors for which a receive string is not configured, response timeout does not apply. For UDP-ECV monitors with no receive string, probe failure is indicated by an ICMP port unreachable error received from the service. Default value: 2 Minimum value: 1 Maximum value: 20939000

resptimeoutThresh

Response time threshold, specified as a percentage of the Response Time-out parameter. If the response to a monitor probe has not arrived when the threshold is reached, the appliance generates an SNMP trap called `monRespTimeoutAboveThresh`. After the response time returns to a value below the threshold, the appliance generates a `monRespTimeoutBelowThresh` SNMP trap. For the traps to be generated, the "MONITOR-RTO-THRESHOLD" alarm must also be enabled. Maximum value: 100

retries

Maximum number of probes to send to establish the state of a service for which a monitoring probe failed. Default value: 3 Minimum value: 1 Maximum value: 127

failureRetries

Number of retries that must fail, out of the number specified for the Retries parameter, for a service to be marked as DOWN. For example, if the Retries parameter is set to 10 and the Failure Retries parameter is set to 6, out of the ten probes sent, at least six probes must fail if the service is to be marked as DOWN. The default value of 0 means that all the retries must fail if the service is to be marked as DOWN. Maximum value: 32

alertRetries

Number of consecutive probe failures after which the appliance generates an SNMP trap called `monProbeFailed`. Maximum value: 32

successRetries

Number of consecutive successful probes required to transition a service's state from DOWN to UP. Default value: 1 Minimum value: 1 Maximum value: 32

downTime

Time duration for which to wait before probing a service that has been marked as DOWN. Expressed in milliseconds, seconds, or minutes. Default value: 30 Minimum value: 1 Maximum value: 20939000

destIP

IP address of the service to which to send probes. If the parameter is set to 0, the IP address of the server to which the monitor is bound is considered the destination IP address.

destPort

TCP or UDP port to which to send the probe. If the parameter is set to 0, the port number of the service to which the monitor is bound is considered the destination port. For a monitor of type USER, however, the destination port is the port number that is included in the HTTP request sent to the dispatcher. Does not apply to monitors of type PING.

state

State of the monitor. The DISABLED setting disables not only the monitor being configured, but all monitors of the same type, until the parameter is set to ENABLED. If the monitor is bound to a service, the state of the monitor is not taken into account when the state of the service is determined. Possible values: ENABLED, DISABLED Default value: ENABLED

reverse

Mark a service as DOWN, instead of UP, when probe criteria are satisfied, and as UP instead of DOWN when probe criteria are not satisfied. Possible values: YES, NO
Default value: NO

transparent

The monitor is bound to a transparent device such as a firewall or router. The state of a transparent device depends on the responsiveness of the services behind it. If a transparent device is being monitored, a destination IP address must be specified. The probe is sent to the specified IP address by using the MAC address of the transparent device. Possible values: YES, NO Default value: NO

ipTunnel

Send the monitoring probe to the service through an IP tunnel. A destination IP address must be specified. Possible values: YES, NO Default value: NO

tos

Probe the service by encoding the destination IP address in the IP TOS (6) bits. Possible values: YES, NO

tosId

The TOS ID of the specified destination IP. Applicable only when the TOS parameter is set. Minimum value: 1 Maximum value: 63

secure

Use a secure SSL connection when monitoring a service. Applicable only to TCP based monitors. The secure option cannot be used with a CITRIX-AG monitor, because a CITRIX-AG monitor uses a secure connection by default. Possible values: YES, NO
Default value: NO

validateCred

Validate the credentials of the Xen Desktop DDC server user. Applicable to monitors of type CITRIX-XD-DDC. Possible values: YES, NO Default value: NO

domain

Domain in which the XenDesktop Desktop Delivery Controller (DDC) servers or Web Interface servers are present. Required by CITRIX-XD-DDC and CITRIX-WI-EXTENDED monitors for logging on to the DDC servers and Web Interface servers, respectively.

IPAddress

Set of IP addresses expected in the monitoring response from the DNS server, if the record type is A or AAAA. Applicable to DNS monitors.

group

Name of a newsgroup available on the NNTP service that is to be monitored. The appliance periodically generates an NNTP query for the name of the newsgroup and evaluates the response. If the newsgroup is found on the server, the service is marked as UP. If the newsgroup does not exist or if the search fails, the service is marked as DOWN. Applicable to NNTP monitors.

fileName

Name of a file on the FTP server. The appliance monitors the FTP service by periodically checking the existence of the file on the server. Applicable to FTP-EXTENDED monitors.

baseDN

The base distinguished name of the LDAP service, from where the LDAP server can begin the search for the attributes in the monitoring query. Required for LDAP service monitoring.

bindDN

The distinguished name with which an LDAP monitor can perform the Bind operation on the LDAP server. Optional. Applicable to LDAP monitors.

filter

Filter criteria for the LDAP query. Optional.

attribute

Attribute to evaluate when the LDAP server responds to the query. Success or failure of the monitoring probe depends on whether the attribute exists in the response. Optional.

database

Name of the database to probe. The name is used to connect to the database during authentication.

sqlQuery

SQL query for a MYSQL-ECV or MSSQL-ECV monitor. Sent to the database server after the server authenticates the connection.

evalRule

Default syntax expression that evaluates the database server's response to a MYSQL-ECV or MSSQL-ECV monitoring query. Must produce a Boolean result. The result determines the state of the server. If the expression returns TRUE, the probe succeeds. For example, if you want the appliance to evaluate the error message to determine the state of the server, use the rule `MYSQL.RES.ROW(10) .TEXT_ELEM(2).EQ("MySQL")`.

mssqlProtocolVersion

Version of MSSQL server that is to be monitored. Possible values: 70, 2000, 2000SP1, 2005, 2008, 2008R2, 2012 Default value: TDS_PROT_70

snmpOID

SNMP OID for SNMP monitors.

snmpCommunity

Community name for SNMP monitors.

snmpThreshold

Threshold for SNMP monitors.

snmpVersion

SNMP version to be used for SNMP monitors. Possible values: V1, V2

metricTable

Metric table to which to bind metrics.

application

Name of the application used to determine the state of the service. Applicable to monitors of type CITRIX-XML-SERVICE.

sitePath

URL of the logon page. For monitors of type CITRIX-WEB-INTERFACE, to monitor a dynamic page under the site path, terminate the site path with a slash (/).
Applicable to CITRIX-WEB-INTERFACE and CITRIX-WI-EXTENDED monitors.

storename

Store Name. For monitors of type STOREFRONT, STORENAME is an optional argument defining storefront service store name. Applicable to STOREFRONT monitors.

storefrontacctservice

Enable/Disable probing for Account Service. Applicable only to Store Front monitors.
For multi-tenancy configuration users may skip account service Possible values: YES, NO Default value: YES

hostName

Hostname in the FQDN format (Example: porche.cars.org). Applicable to STOREFRONT monitors.

netProfile

Name of the network profile.

originHost

Origin-Host value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers.

originRealm

Origin-Realm value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers.

hostIPAddress

Host-IP-Address value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. If Host-IP-Address is not specified, the appliance inserts the mapped IP (MIP) address or subnet IP (SNIP) address from which the CER request (the monitoring probe) is sent.

vendorId

Vendor-Id value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers.

productName

Product-Name value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers.

firmwareRevision

Firmware-Revision value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers.

authApplicationId

List of Auth-Application-Id attribute value pairs (AVPs) for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. A maximum of eight of these AVPs are supported in a monitoring CER message. Maximum value: 4294967295

acctApplicationId

List of Acct-Application-Id attribute value pairs (AVPs) for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. A maximum of eight of these AVPs are supported in a monitoring message. Maximum value: 4294967295

inbandSecurityId

Inband-Security-Id for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. Possible values: NO_INBAND_SECURITY, TLS

supportedVendorIds

List of Supported-Vendor-Id attribute value pairs (AVPs) for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. A maximum eight of these AVPs are supported in a monitoring message. Minimum value: 1
Maximum value: 4294967295

vendorSpecificVendorId

Vendor-Id to use in the Vendor-Specific-Application-Id grouped attribute-value pair (AVP) in the monitoring CER message. To specify Auth-Application-Id or Acct-Application-Id in Vendor-Specific-Application-Id, use vendorSpecificAuthApplicationIds or vendorSpecificAcctApplicationIds, respectively. Only one Vendor-Id is supported for all the Vendor-Specific-Application-Id AVPs in a CER monitoring message. Minimum value: 1

kcdAccount

KCD Account used by MSSQL monitor

storedb

Used in case of DB specific LB.If enalbed then we store the database list populated from monitors responses. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

```
add monitor http_mon http
```

[Top](#)

rm lb monitor

Synopsis

```
rm lb monitor <monitorName> <type> [-respCode <int[-int]> ...]
```

Description

Removes a monitor or a response code for an HTTP monitor. If you do not specify any response codes, the monitor is removed. If you provide any or all of the HTTP response codes that are configured for the monitor, only those specified response codes are removed; the monitor is not removed. Built-in monitors cannot be removed.

Parameters

monitorName

Name of the monitor.

type

Type of monitor that you want to create. Possible values: PING, TCP, HTTP, TCP-ECV, HTTP-ECV, UDP-ECV, DNS, FTP, LDNS-PING, LDNS-TCP, LDNS-DNS, RADIUS, USER, HTTP-INLINE, SIP-UDP, LOAD, FTP-EXTENDED, SMTP, SNMP, NNTP, MYSQL, MYSQL-ECV, MSSQL-ECV, ORACLE-ECV, LDAP, POP3, CITRIX-XML-SERVICE, CITRIX-WEB-INTERFACE, DNS-TCP, RTSP, ARP, CITRIX-AG, CITRIX-AAC-LOGINPAGE, CITRIX-AAC-LAS, CITRIX-XD-DDC, ND6, CITRIX-WI-EXTENDED, DIAMETER, RADIUS_ACCOUNTING, STOREFRONT

respCode

Response codes to delete from the response code list configured for the HTTP monitor.

Example

```
rm monitor http_mon http
```

[Top](#)

set lb monitor

Synopsis

```
set lb monitor <monitorName> <type> [-action <action>] [-respCode <int[-int]> ...] [-httpRequest <string>] [-rtspRequest <string>] [-customHeaders <string>] [-maxForwards <positive_integer>] [-sipMethod <sipMethod>] [-sipregURI <string>] [-sipURI <string>] [-send <string>] [-recv <string>] [-query <string>] [-queryType <queryType>] [-userName <string>] {-password } {-secondaryPassword } [-logonpointName <string>] [-lasVersion <string>] {-radKey } [-radNASid <string>] [-radNASip <ip_addr>] [-radAccountType <positive_integer>] [-radFramedIP <ip_addr>] [-radAPN <string>] [-radMSISDN <string>] [-radAccountSession <string>] [-LRTM ( ENABLED | DISABLED )] [-deviation <positive_integer> [<units>]] [-scriptName <string>] [-scriptArgs <string>] [-validateCred ( YES | NO )] [-domain <string>] [-dispatcherIP <ip_addr>] [-dispatcherPort <port>] [-interval <integer> [<units>]] [-resptimeout <integer> [<units>]] [-resptimeoutThresh <positive_integer>] [-retries <integer>] [-failureRetries <integer>] [-alertRetries <integer>] [-successRetries <integer>] [-downTime <integer> [<units>]] [-destIP <ip_addr|ipv6_addr>] [-destPort <port>] [-state ( ENABLED | DISABLED )] [-reverse ( YES | NO )] [-transparent ( YES | NO )] [-ipTunnel ( YES | NO )] [-tos ( YES | NO )] [-tosid <positive_integer>] [-secure ( YES | NO )] [-IPAddress <ip_addr|ipv6_addr|*> ...] [-group <string>] [-fileName <string>] [-baseDN <string>] [-bindDN <string>] [-filter <string>] [-attribute <string>] [-database <string>] [-sqlQuery <text>] [-evalRule <expression>] [-snmpOID <string>] [-snmpCommunity <string>] [-snmpThreshold <string>] [-snmpVersion ( V1 | V2 )] [-metricTable <string>] [-metric <string>] [-metricThreshold <positive_integer>] [-metricWeight <positive_integer>]] [-application <string>] [-sitePath <string>] [-storename <string>] [-storefrontacctservice ( YES | NO )] [-netProfile <string>] [-mssqlProtocolVersion <mssqlProtocolVersion>] [-originHost <string>] [-originRealm <string>] [-hostIPAddress <ip_addr|ipv6_addr|*>] [-vendorId
```

```
<positive_integer>] [-productName <string>] [-firmwareRevision <positive_integer>] [-
authApplicationId <positive_integer> ...] [-acctApplicationId <positive_integer> ...] [-
inbandSecurityId ( NO_INBAND_SECURITY | TLS )] [-supportedVendorIds
<positive_integer> ...] [-vendorSpecificVendorId <positive_integer> [-
vendorSpecificAuthApplicationIds <positive_integer> ...] [-
vendorSpecificAcctApplicationIds <positive_integer> ...]] [-kcdAccount <string>]
```

Description

Modifies the specified parameters of a monitor.

Parameters

monitorName

Name of the monitor.

type

Type of monitor that you want to create. Possible values: PING, TCP, HTTP, TCP-ECV, HTTP-ECV, UDP-ECV, DNS, FTP, LDNS-PING, LDNS-TCP, LDNS-DNS, RADIUS, USER, HTTP-INLINE, SIP-UDP, LOAD, FTP-EXTENDED, SMTP, SNMP, NNTP, MYSQL, MYSQL-ECV, MSSQL-ECV, ORACLE-ECV, LDAP, POP3, CITRIX-XML-SERVICE, CITRIX-WEB-INTERFACE, DNS-TCP, RTSP, ARP, CITRIX-AG, CITRIX-AAC-LOGINPAGE, CITRIX-AAC-LAS, CITRIX-XD-DDC, ND6, CITRIX-WI-EXTENDED, DIAMETER, RADIUS_ACCOUNTING, STOREFRONT

action

Action to perform when the response to an inline monitor (a monitor of type HTTP-INLINE) indicates that the service is down. A service monitored by an inline monitor is considered DOWN if the response code is not one of the codes that have been specified for the Response Code parameter. Available settings function as follows: * NONE - Do not take any action. However, the show service command and the show lb monitor command indicate the total number of responses that were checked and the number of consecutive error responses received after the last successful probe. * LOG - Log the event in NSLOG or SYSLOG. * DOWN - Mark the service as being down, and then do not direct any traffic to the service until the configured down time has expired. Persistent connections to the service are terminated as soon as the service is marked as DOWN. Also, log the event in NSLOG or SYSLOG. Possible values: NONE, LOG, DOWN Default value: SM_DOWN

respCode

Response codes for which to mark the service as UP. For any other response code, the action performed depends on the monitor type. HTTP monitors and RADIUS monitors mark the service as DOWN, while HTTP-INLINE monitors perform the action indicated by the Action parameter.

httpRequest

HTTP request to send to the server (for example, "HEAD /file.html").

rtspRequest

RTSP request to send to the server (for example, "OPTIONS *").

customHeaders

Custom header string to include in the monitoring probes.

maxForwards

Maximum number of hops that the SIP request used for monitoring can traverse to reach the server. Applicable only to monitors of type SIP-UDP. Default value: 1
Maximum value: 255

sipMethod

SIP method to use for the query. Applicable only to monitors of type SIP-UDP. Possible values: OPTIONS, INVITE, REGISTER

sipURI

SIP URI string to send to the service (for example, sip:sip.test). Applicable only to monitors of type SIP-UDP.

send

String to send to the service. Applicable to TCP-ECV, HTTP-ECV, and UDP-ECV monitors.

recv

String expected from the server for the service to be marked as UP. Applicable to TCP-ECV, HTTP-ECV, and UDP-ECV monitors.

query

Domain name to resolve as part of monitoring the DNS service (for example, example.com).

queryType

Type of DNS record for which to send monitoring queries. Set to Address for querying A records, AAAA for querying AAAA records, and Zone for querying the SOA record.
Possible values: Address, Zone, AAAA

userName

User name with which to probe the RADIUS, NNTP, FTP, FTP-EXTENDED, MYSQL, MSSQL, POP3, CITRIX-AG, CITRIX-XD-DDC, or CITRIX-WI-EXTENDED server.

password

Password that is required for logging on to the RADIUS, NNTP, FTP, FTP-EXTENDED, MYSQL, MSSQL, POP3, CITRIX-AG, CITRIX-XD-DDC, or CITRIX-WI-EXTENDED server.
Used in conjunction with the user name specified for the User Name parameter.

secondaryPassword

Secondary password that users might have to provide to log on to the Access Gateway server. Applicable to CITRIX-AG monitors.

logonpointName

Name of the logon point that is configured for the Citrix Access Gateway Advanced Access Control software. Required if you want to monitor the associated login page or Logon Agent. Applicable to CITRIX-AAC-LAS and CITRIX-AAC-LOGINPAGE monitors.

lasVersion

Version number of the Citrix Advanced Access Control Logon Agent. Required by the CITRIX-AAC-LAS monitor.

radKey

Authentication key (shared secret text string) for RADIUS clients and servers to exchange. Applicable to monitors of type RADIUS and RADIUS_ACCOUNTING.

radNASid

NAS-Identifier to send in the Access-Request packet. Applicable to monitors of type RADIUS.

radNASip

Network Access Server (NAS) IP address to use as the source IP address when monitoring a RADIUS server. Applicable to monitors of type RADIUS and RADIUS_ACCOUNTING.

radAccountType

Account Type to be used in Account Request Packet. Applicable to monitors of type RADIUS_ACCOUNTING. Default value: 1 Maximum value: 15

radFramedIP

Source ip with which the packet will go out . Applicable to monitors of type RADIUS_ACCOUNTING.

radAPN

Called Station Id to be used in Account Request Packet. Applicable to monitors of type RADIUS_ACCOUNTING.

radMSISDN

Calling Stations Id to be used in Account Request Packet. Applicable to monitors of type RADIUS_ACCOUNTING.

radAccountSession

Account Session ID to be used in Account Request Packet. Applicable to monitors of type RADIUS_ACCOUNTING.

LRTM

Calculate the least response times for bound services. If this parameter is not enabled, the appliance does not learn the response times of the bound services. Also used for LRTM load balancing. Possible values: ENABLED, DISABLED

deviation

Time value added to the learned average response time in dynamic response time monitoring (DRTM). When a deviation is specified, the appliance learns the average response time of bound services and adds the deviation to the average. The final value is then continually adjusted to accommodate response time variations over time. Specified in milliseconds, seconds, or minutes. Maximum value: 20939000

scriptName

Path and name of the script to execute. The script must be available on the NetScaler appliance, in the /nsconfig/monitors/ directory.

scriptArgs

String of arguments for the script. The string is copied verbatim into the request.

validateCred

Validate the credentials of the Xen Desktop DDC server user. Applicable to monitors of type CITRIX-XD-DDC. Possible values: YES, NO Default value: NO

domain

Domain in which the XenDesktop Desktop Delivery Controller (DDC) servers or Web Interface servers are present. Required by CITRIX-XD-DDC and CITRIX-WI-EXTENDED monitors for logging on to the DDC servers and Web Interface servers, respectively.

dispatcherIP

IP address of the dispatcher to which to send the probe.

dispatcherPort

Port number on which the dispatcher listens for the monitoring probe.

interval

Time interval between two successive probes. Must be greater than the value of Response Time-out. Default value: 5 Minimum value: 1 Maximum value: 20940000

resptimeout

Amount of time for which the appliance must wait before it marks a probe as FAILED. Must be less than the value specified for the Interval parameter. Note: For UDP-ECV monitors for which a receive string is not configured, response timeout does not apply. For UDP-ECV monitors with no receive string, probe failure is indicated by an ICMP port unreachable error received from the service. Default value: 2 Minimum value: 1 Maximum value: 20939000

resptimeoutThresh

Response time threshold, specified as a percentage of the Response Time-out parameter. If the response to a monitor probe has not arrived when the threshold is reached, the appliance generates an SNMP trap called monRespTimeoutAboveThresh. After the response time returns to a value below the threshold, the appliance generates a monRespTimeoutBelowThresh SNMP trap. For the traps to be generated, the "MONITOR-RTO-THRESHOLD" alarm must also be enabled. Maximum value: 100

retries

Maximum number of probes to send to establish the state of a service for which a monitoring probe failed. Default value: 3 Minimum value: 1 Maximum value: 127

failureRetries

Number of retries that must fail, out of the number specified for the Retries parameter, for a service to be marked as DOWN. For example, if the Retries parameter is set to 10 and the Failure Retries parameter is set to 6, out of the ten probes sent, at least six probes must fail if the service is to be marked as DOWN. The default value of 0 means that all the retries must fail if the service is to be marked as DOWN. Maximum value: 32

alertRetries

Number of consecutive probe failures after which the appliance generates an SNMP trap called monProbeFailed. Maximum value: 32

successRetries

Number of consecutive successful probes required to transition a service's state from DOWN to UP. Default value: 1 Minimum value: 1 Maximum value: 32

downTime

Time duration for which to wait before probing a service that has been marked as DOWN. Expressed in milliseconds, seconds, or minutes. Default value: 30 Minimum value: 1 Maximum value: 20939000

destIP

IP address of the service to which to send probes. If the parameter is set to 0, the IP address of the server to which the monitor is bound is considered the destination IP address.

destPort

TCP or UDP port to which to send the probe. If the parameter is set to 0, the port number of the service to which the monitor is bound is considered the destination port. For a monitor of type USER, however, the destination port is the port number that is included in the HTTP request sent to the dispatcher. Does not apply to monitors of type PING.

state

State of the monitor. The DISABLED setting disables not only the monitor being configured, but all monitors of the same type, until the parameter is set to ENABLED. If the monitor is bound to a service, the state of the monitor is not taken into account when the state of the service is determined. Possible values: ENABLED, DISABLED Default value: ENABLED

reverse

Mark a service as DOWN, instead of UP, when probe criteria are satisfied, and as UP instead of DOWN when probe criteria are not satisfied. Possible values: YES, NO Default value: NO

transparent

The monitor is bound to a transparent device such as a firewall or router. The state of a transparent device depends on the responsiveness of the services behind it. If a transparent device is being monitored, a destination IP address must be specified. The probe is sent to the specified IP address by using the MAC address of the transparent device. Possible values: YES, NO Default value: NO

ipTunnel

Send the monitoring probe to the service through an IP tunnel. A destination IP address must be specified. Possible values: YES, NO Default value: NO

tos

Probe the service by encoding the destination IP address in the IP TOS (6) bits. Possible values: YES, NO

tosId

The TOS ID of the specified destination IP. Applicable only when the TOS parameter is set. Minimum value: 1 Maximum value: 63

secure

Use a secure SSL connection when monitoring a service. Applicable only to TCP based monitors. The secure option cannot be used with a CITRIX-AG monitor, because a CITRIX-AG monitor uses a secure connection by default. Possible values: YES, NO Default value: NO

IPAddress

Set of IP addresses expected in the monitoring response from the DNS server, if the record type is A or AAAA. Applicable to DNS monitors.

group

Name of a newsgroup available on the NNTP service that is to be monitored. The appliance periodically generates an NNTP query for the name of the newsgroup and evaluates the response. If the newsgroup is found on the server, the service is marked as UP. If the newsgroup does not exist or if the search fails, the service is marked as DOWN. Applicable to NNTP monitors.

fileName

Name of a file on the FTP server. The appliance monitors the FTP service by periodically checking the existence of the file on the server. Applicable to FTP-EXTENDED monitors.

baseDN

The base distinguished name of the LDAP service, from where the LDAP server can begin the search for the attributes in the monitoring query. Required for LDAP service monitoring.

bindDN

The distinguished name with which an LDAP monitor can perform the Bind operation on the LDAP server. Optional. Applicable to LDAP monitors.

filter

Filter criteria for the LDAP query. Optional.

attribute

Attribute to evaluate when the LDAP server responds to the query. Success or failure of the monitoring probe depends on whether the attribute exists in the response. Optional.

database

Name of the database to probe. The name is used to connect to the database during authentication.

sqlQuery

SQL query for a MYSQL-ECV or MSSQL-ECV monitor. Sent to the database server after the server authenticates the connection.

evalRule

Default syntax expression that evaluates the database server's response to a MYSQL-ECV or MSSQL-ECV monitoring query. Must produce a Boolean result. The result determines the state of the server. If the expression returns TRUE, the probe succeeds. For example, if you want the appliance to evaluate the error message to determine the state of the server, use the rule `MYSQL.RES.ROW(10) .TEXT_ELEM(2).EQ("MySQL")`.

snmpOID

SNMP OID for SNMP monitors.

snmpCommunity

Community name for SNMP monitors.

snmpThreshold

Threshold for SNMP monitors.

snmpVersion

SNMP version to be used for SNMP monitors. Possible values: V1, V2

metricTable

Metric table to which to bind metrics.

metric

Metric name in the metric table, whose setting is changed. A value zero disables the metric and it will not be used for load calculation

application

Name of the application used to determine the state of the service. Applicable to monitors of type CITRIX-XML-SERVICE.

sitePath

URL of the logon page. For monitors of type CITRIX-WEB-INTERFACE, to monitor a dynamic page under the site path, terminate the site path with a slash (/). Applicable to CITRIX-WEB-INTERFACE and CITRIX-WI-EXTENDED monitors.

storename

Store Name. For monitors of type STOREFRONT, STORENAME is an optional argument defining storefront service store name. Applicable to STOREFRONT monitors.

storefrontacctservice

Enable/Disable probing for Account Service. Applicable only to Store Front monitors. For multi-tenancy configuration users my skip account service Possible values: YES, NO Default value: YES

hostName

Hostname in the FQDN format (Example: porche.cars.org). Applicable to STOREFRONT monitors.

netProfile

Name of the network profile.

mssqlProtocolVersion

Version of MSSQL server that is to be monitored. Possible values: 70, 2000, 2000SP1, 2005, 2008, 2008R2, 2012 Default value: TDS_PROT_70

originHost

Origin-Host value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers.

originRealm

Origin-Realm value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers.

hostIPAddress

Host-IP-Address value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. If Host-IP-Address is not specified, the appliance inserts the mapped IP (MIP) address or subnet IP (SNIP) address from which the CER request (the monitoring probe) is sent.

vendorId

Vendor-Id value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers.

productName

Product-Name value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers.

firmwareRevision

Firmware-Revision value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers.

authApplicationId

List of Auth-Application-Id attribute value pairs (AVPs) for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. A maximum of eight of these AVPs are supported in a monitoring CER message. Maximum value: 4294967295

acctApplicationId

List of Acct-Application-Id attribute value pairs (AVPs) for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. A maximum of eight of these AVPs are supported in a monitoring message. Maximum value: 4294967295

inbandSecurityId

Inband-Security-Id for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. Possible values: NO_INBAND_SECURITY, TLS

supportedVendorIds

List of Supported-Vendor-Id attribute value pairs (AVPs) for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. A maximum of eight of these AVPs are supported in a monitoring message. Minimum value: 1
Maximum value: 4294967295

vendorSpecificVendorId

Vendor-Id to use in the Vendor-Specific-Application-Id grouped attribute-value pair (AVP) in the monitoring CER message. To specify Auth-Application-Id or Acct-Application-Id in Vendor-Specific-Application-Id, use `vendorSpecificAuthApplicationIds` or `vendorSpecificAcctApplicationIds`, respectively. Only one Vendor-Id is supported for all the Vendor-Specific-Application-Id AVPs in a CER monitoring message. Minimum value: 1

kcdAccount

KCD Account used by MSSQL monitor

Example

```
set monitor http_mon http -respcode 100
```

[Top](#)

unset lb monitor

Synopsis

```
unset lb monitor <monitorName> <type> [-IPAddress <ip_addr|ipv6_addr|*> ...] [-scriptName] [-destPort] [-netProfile] [-action] [-respCode] [-httpRequest] [-rtspRequest] [-customHeaders] [-maxForwards] [-sipMethod] [-sipregURI] [-send] [-recv] [-query] [-queryType] [-userName] [-password] [-secondaryPassword] [-logonpointName] [-lasVersion] [-radKey] [-radNASid] [-radNASip] [-radAccountType] [-radFramedIP] [-radAPN] [-radMSISDN] [-radAccountSession] [-LRTM] [-deviation] [-scriptArgs] [-validateCred] [-domain] [-dispatcherIP] [-dispatcherPort] [-interval] [-resptimeout] [-resptimeoutThresh] [-retries] [-failureRetries] [-alertRetries] [-successRetries] [-downTime] [-destIP] [-state] [-reverse] [-transparent] [-ipTunnel] [-tos] [-tosId] [-secure] [-group] [-fileName] [-baseDN] [-bindDN] [-filter] [-attribute] [-database] [-sqlQuery] [-evalRule] [-snmpOID] [-snmpCommunity] [-snmpThreshold] [-snmpVersion] [-metricTable] [-mssqlProtocolVersion] [-originHost] [-originRealm] [-hostIPAddress] [-vendorId] [-productName] [-firmwareRevision] [-authApplicationId] [-acctApplicationId] [-inbandSecurityId] [-supportedVendorIds] [-vendorSpecificVendorId] [-vendorSpecificAuthApplicationIds] [-vendorSpecificAcctApplicationIds] [-kcdAccount]
```

Description

Removes the specified parameter settings from the specified monitor. Attributes for which a default value is available revert to their default values..Refer to the set lb monitor command for meanings of the arguments.

Example

```
set monitor dns_mon dns -ipaddress 10.102.27.230
```

[Top](#)

enable lb monitor

Synopsis

```
enable lb monitor (<serviceName>@ | <serviceGroupName>@) [<monitorName>]
```

Description

Enable the monitor that is bound to a specific service. If no monitor name is specified, all monitors bound to the service are enabled.

Parameters

serviceName

The name of the service to which the monitor is bound.

serviceGroupName

The name of the service group to which the monitor is to be bound.

monitorName

Name for the monitor. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period

(.), space, colon (:), at (@), equals (=), and hyphen (-) characters. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my monitor" or 'my monitor').

Example

```
enable monitor http_svc http_mon
    To enable monitor for multiple services use
the following command:
enable monitor http_svc[1-3] http_mon
```

[Top](#)

disable lb monitor

Synopsis

disable lb monitor (<serviceName>@ | <serviceGroupName>@) [<monitorName>]

Description

Disable the monitor for a service. If the monitor name is not specified, all monitors bound to the service are disabled.

Parameters**serviceName**

The name of the service being monitored.

serviceGroupName

The name of the service group being monitored.

monitorName

Name for the monitor. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my monitor" or 'my monitor').

Example

```
disable monitor http_svc http_mon
    To disable a monitor on multiple services use
the following command:
disable monitor http_svc[1-3] http_mon
```

[Top](#)

bind lb monitor

Synopsis

```
bind lb monitor <monitorName> [-state ( ENABLED | DISABLED )] [-weight  
<positive_integer>] [-state ( ENABLED | DISABLED )] [-weight <positive_integer>] [-  
metric <string> -metricThreshold <positive_integer> [-metricWeight  
<positive_integer>] ]
```

Description

Binds a monitor to a service or service group. Multiple monitors can be bound to a service or service group.

Parameters

monitorName

Name of the monitor.

serviceName

Name of the service or service group.

serviceName

Name of the service group.

metric

Name of the metric to be polled by the monitor.

Example

```
bind monitor http_mon http_svc  
    To bind a monitor to multiple services use the  
    following command:  
    bind monitor http_mon http_svc[1-3]
```

[Top](#)

unbind lb monitor

Synopsis

```
unbind lb monitor <monitorName> -metric <string>
```

Description

Unbinds a monitor from a service or service group.

Parameters

monitorName

Name of the monitor.

serviceName

Name of the service or service group.

serviceGroupName

Name of the service group.

metric

Name of the metric to be polled by the monitor.

Example

```
unbind monitor http_mon http_svc
    To unbind a monitor to multiple services use
    the following command:
    unbind monitor http_mon http_svc[1-3]
```

[Top](#)

show lb monitor**Synopsis**

show lb monitor [<monitorName>] [<type>] show lb monitor bindings - alias for 'show lb monbindings'

Description

Displays the parameters of all the monitors configured on the appliance, or the parameters of the specified monitor.

Parameters**monitorName**

Name of the monitor.

type

Type of monitor that you want to create. Possible values: PING, TCP, HTTP, TCP-ECV, HTTP-ECV, UDP-ECV, DNS, FTP, LDNS-PING, LDNS-TCP, LDNS-DNS, RADIUS, USER, HTTP-INLINE, SIP-UDP, LOAD, FTP-EXTENDED, SMTP, SNMP, NNTP, MYSQL, MYSQL-ECV, MSSQL-ECV, ORACLE-ECV, LDAP, POP3, CITRIX-XML-SERVICE, CITRIX-WEB-INTERFACE, DNS-TCP, RTSP, ARP, CITRIX-AG, CITRIX-AAC-LOGINPAGE, CITRIX-AAC-LAS, CITRIX-XD-DDC, ND6, CITRIX-WI-EXTENDED, DIAMETER, RADIUS_ACCOUNTING, STOREFRONT

Example

```
An example of the show monitor command output is
as follows:
8 configured monitors:
1)  Name.....:          ping  Type.....:
PING  State....ENABLED
2)  Name.....:          tcp
Type.....:      TCP  State....ENABLED
3)  Name.....:          http  Type.....:
HTTP  State....ENABLED
4)  Name.....:      tcp-ecv  Type.....:
TCP-ECV  State....ENABLED
```

```
5)  Name.....:      http-ecv  Type.....:
    HTTP-ECV    State....ENABLED
6)  Name.....:      udp-ecv   Type.....:
    UDP-ECV     State....ENABLED
7)  Name.....:              dns
    Type.....:   DNS      State....ENABLED
8)  Name.....:              ftp
    Type.....:   FTP      State....ENABLED
```

[Top](#)

lb route

[[add](#) | [rm](#) | [show](#)]

add lb route

Synopsis

add lb route <network> <netmask> <gatewayName>

Description

Bind the route VIP to the route structure.

Parameters

network

The IP address of the network to which the route belongs.

netmask

The netmask to which the route belongs.

gatewayName

The name of the route.

[Top](#)

rm lb route

Synopsis

rm lb route <network> <netmask>

Description

Remove the route VIP from the route structure.

Parameters

network

The IP address of the network to which the route VIP belongs.

netmask

The netmask of the destination network.

[Top](#)

show lb route

Synopsis

show lb route [<network> <netmask>]

Description

Display the names of the routes associated to the route structure using the `###add lb route###` command.

Parameters

network

The destination network or host.

[Top](#)

lb route6

[[add](#) | [rm](#) | [show](#)]

add lb route6

Synopsis

add lb route6 <network> [<gatewayName>]

Description

Bind the route VIP to the route structure.

Parameters

network

The destination network.

gatewayName

The name of the route.

[Top](#)

rm lb route6

Synopsis

rm lb route6 <network>

Description

Remove the route VIP from the route structure.

Parameters

network

The IP address of the network to which the route VIP belongs.

[Top](#)

show lb route6

Synopsis

show lb route6 [<network>]

Description

Display the names of the routes associated to the route structure using the `###add lb route6###` command.

Parameters

network

The destination network or host.

[Top](#)

lb vsrver

[[add](#) | [rm](#) | [set](#) | [unset](#) | [bind](#) | [unbind](#) | [enable](#) | [disable](#) | [show](#) | [stat](#) | [rename](#)]

add lb vsrver

Synopsis

```
add lb vsrver <name>@ <serviceType> [( <IPAddress>@ <port> [-range
<positive_integer>] ) | ( -IPPattern <ippat> -IPMask <ipmask> ) ] [-persistenceType
<persistenceType>] [-timeout <mins>] [-persistenceBackup ( SOURCEIP | NONE )] [-
backupPersistenceTimeout <mins>] [-lbMethod <lbMethod>] [-hashLength
<positive_integer>] [-netmask <netmask>] [-v6netmasklen <positive_integer>] [-
dataLength <positive_integer>] [-dataOffset <positive_integer>] [-cookieName
<string>] [-rule <expression>] [-Listenpolicy <expression>] [-Listenpriority
<positive_integer>] [-resRule <expression>] [-persistMask <netmask>] [-
v6persistmasklen <positive_integer>] [-pq ( ON | OFF )] [-sc ( ON | OFF )] [-rtspNat
( ON | OFF )] [-m <m>] [-tosld <positive_integer>] [-sessionless ( ENABLED | DISABLED )]
[-state ( ENABLED | DISABLED )] [-connfailover <connfailover>] [-redirectURL <URL>] [-
cacheable ( YES | NO )] [-cltTimeout <secs>] [-soMethod <soMethod>] [-soPersistence
( ENABLED | DISABLED )] [-soPersistenceTimeOut <positive_integer>] [-healthThreshold
<positive_integer>] [-soThreshold <positive_integer>] [-soBackupAction
<soBackupAction>] [-redirectPortRewrite ( ENABLED | DISABLED )] [-downStateFlush
( ENABLED | DISABLED )] [-backupVServer <string>] [-disablePrimaryOnDown ( ENABLED
| DISABLED )] [-insertVserverIPPort <insertVserverIPPort>] [-vipHeader> ] [-
AuthenticationHost <string>] [-Authentication ( ON | OFF )] [-authn401 ( ON | OFF )] [-
authnVsName <string>] [-push ( ENABLED | DISABLED )] [-pushVserver <string>] [-
pushLabel <expression>] [-pushMultiClients ( YES | NO )] [-tcpProfileName <string>] [-
httpProfileName <string>] [-dbProfileName <string>] [-comment <string>] [-l2Conn ( ON
| OFF )] [-mssqlServerVersion <mssqlServerVersion>] [-mysqlProtocolVersion
<positive_integer>] [-mysqlServerVersion <string>] [-mysqlCharacterSet
<positive_integer>] [-mysqlServerCapabilities <positive_integer>] [-appflowLog
( ENABLED | DISABLED )] [-netProfile <string>] [-icmpVsrResponse ( PASSIVE | ACTIVE )]
[-newServiceRequest <positive_integer>] [-<newServiceRequestUnit>]] [-
newServiceRequestIncrementInterval <positive_integer>] [-minAutoscaleMembers
<positive_integer>] [-maxAutoscaleMembers <positive_integer>] [-persistAVPno
```



```
<positive_integer> ...] [-skippersistency <skippersistency>] [-td <positive_integer>] [-
authnProfile <string>] [-macmodeRetainvlan ( ENABLED | DISABLED )] [-dbsLb
( ENABLED | DISABLED )] [-dns64 ( ENABLED | DISABLED )] [-bypassAAAA ( YES | NO )] [-
RecursionAvailable ( YES | NO )]
```

Description

Creates a load balancing virtual server.

Parameters

name

Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver').

serviceType

Protocol used by the service (also called the service type). Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, DTLS, NNTP, DNS, DHCPRA, ANY, SIP_UDP, DNS_TCP, RTSP, PUSH, SSL_PUSH, RADIUS, RDP, MYSQL, MSSQL, DIAMETER, SSL_DIAMETER, TFTP

IPAddress

IPv4 or IPv6 address to assign to the virtual server.

IPPattern

IP address pattern, in dotted decimal notation, for identifying packets to be accepted by the virtual server. The IP Mask parameter specifies which part of the destination IP address is matched against the pattern. Mutually exclusive with the IP Address parameter. For example, if the IP pattern assigned to the virtual server is 198.51.100.0 and the IP mask is 255.255.240.0 (a forward mask), the first 20 bits in the destination IP addresses are matched with the first 20 bits in the pattern. The virtual server accepts requests with IP addresses that range from 198.51.96.1 to 198.51.111.254. You can also use a pattern such as 0.0.2.2 and a mask such as 0.0.255.255 (a reverse mask). If a destination IP address matches more than one IP pattern, the pattern with the longest match is selected, and the associated virtual server processes the request. For example, if virtual servers vs1 and vs2 have the same IP pattern, 0.0.100.128, but different IP masks of 0.0.255.255 and 0.0.224.255, a destination IP address of 198.51.100.128 has the longest match with the IP pattern of vs1. If a destination IP address matches two or more virtual servers to the same extent, the request is processed by the virtual server whose port number matches the port number in the request.

port

Port number for the virtual server.

range

Number of IP addresses that the appliance must generate and assign to the virtual server. The virtual server then functions as a network virtual server, accepting traffic on any of the generated IP addresses. The IP addresses are generated automatically, as follows: * For a range of n, the last octet of the address specified by the IP Address parameter increments n-1 times. * If the last octet exceeds 255, it rolls over

to 0 and the third octet increments by 1. Note: The Range parameter assigns multiple IP addresses to one virtual server. To generate an array of virtual servers, each of which owns only one IP address, use brackets in the IP Address and Name parameters to specify the range. For example: add lb vserver my_vserver[1-3] HTTP 192.0.2.[1-3] 80 Default value: 1 Minimum value: 1 Maximum value: 254

persistenceType

Type of persistence for the virtual server. Available settings function as follows: * SOURCEIP - Connections from the same client IP address belong to the same persistence session. * COOKIEINSERT - Connections that have the same HTTP Cookie, inserted by a Set-Cookie directive from a server, belong to the same persistence session. * SSLSESSION - Connections that have the same SSL Session ID belong to the same persistence session. * CUSTOMSERVERID - Connections with the same server ID form part of the same session. For this persistence type, set the Server ID (CustomServerID) parameter for each service and configure the Rule parameter to identify the server ID in a request. * RULE - All connections that match a user defined rule belong to the same persistence session. * URLPASSIVE - Requests that have the same server ID in the URL query belong to the same persistence session. The server ID is the hexadecimal representation of the IP address and port of the service to which the request must be forwarded. This persistence type requires a rule to identify the server ID in the request. * DESTIP - Connections to the same destination IP address belong to the same persistence session. * SRCIPDESTIP - Connections that have the same source IP address and destination IP address belong to the same persistence session. * CALLID - Connections that have the same CALL-ID SIP header belong to the same persistence session. * RTSPSID - Connections that have the same RTSP Session ID belong to the same persistence session. Possible values: SOURCEIP, COOKIEINSERT, SSLSESSION, RULE, URLPASSIVE, CUSTOMSERVERID, DESTIP, SRCIPDESTIP, CALLID, RTSPSID, DIAMETER, NONE

timeout

Time period for which a persistence session is in effect. Default value: 2 Maximum value: 1440

persistenceBackup

Backup persistence type for the virtual server. Becomes operational if the primary persistence mechanism fails. Possible values: SOURCEIP, NONE

backupPersistenceTimeout

Time period for which backup persistence is in effect. Default value: 2 Minimum value: 2 Maximum value: 1440

lbMethod

Load balancing method. The available settings function as follows: * ROUNDROBIN - Distribute requests in rotation, regardless of the load. Weights can be assigned to services to enforce weighted round robin distribution. * LEASTCONNECTION (default) - Select the service with the fewest connections. * LEASTRESPONSETIME - Select the service with the lowest average response time. * LEASTBANDWIDTH - Select the service currently handling the least traffic. * LEASTPACKETS - Select the service currently serving the lowest number of packets per second. * CUSTOMLOAD - Base service selection on the SNMP metrics obtained by custom load monitors. * LRTM - Select the service with the lowest response time. Response times are learned through monitoring probes. This method also takes the number of active connections into account. Also available are a number of hashing methods, in which the appliance

extracts a predetermined portion of the request, creates a hash of the portion, and then checks whether any previous requests had the same hash value. If it finds a match, it forwards the request to the service that served those previous requests. Following are the hashing methods: * URLHASH - Create a hash of the request URL (or part of the URL). * DOMAINHASH - Create a hash of the domain name in the request (or part of the domain name). The domain name is taken from either the URL or the Host header. If the domain name appears in both locations, the URL is preferred. If the request does not contain a domain name, the load balancing method defaults to LEASTCONNECTION. * DESTINATIONIPHASH - Create a hash of the destination IP address in the IP header. * SOURCEIPHASH - Create a hash of the source IP address in the IP header. * TOKEN - Extract a token from the request, create a hash of the token, and then select the service to which any previous requests with the same token hash value were sent. * SRCIPDESTIPHASH - Create a hash of the string obtained by concatenating the source IP address and destination IP address in the IP header. * SRCIPSRCPORHASH - Create a hash of the source IP address and source port in the IP header. * CALLIDHASH - Create a hash of the SIP Call-ID header. Possible values: ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, URLHASH, DOMAINHASH, DESTINATIONIPHASH, SOURCEIPHASH, SRCIPDESTIPHASH, LEASTBANDWIDTH, LEASTPACKETS, TOKEN, SRCIPSRCPORHASH, LRTM, CALLIDHASH, CUSTOMLOAD, LEASTREQUEST Default value: PEMGMT_LB_LEASTCONNS

cookieName

Use this parameter to specify the cookie name for COOKIE persistence type. It specifies the name of cookie with a maximum of 32 characters. If not specified, cookie name is internally generated.

rule

Expression, or name of a named expression, against which traffic is evaluated. Written in the classic or default syntax. Note: Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>" The following requirements apply only to the NetScaler CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks. Default value: "none"

Listenpolicy

Default syntax expression identifying traffic accepted by the virtual server. Can be either an expression (for example, CLIENT.IP.DST.IN_SUBNET(192.0.2.0/24) or the name of a named expression. In the above example, the virtual server accepts all requests whose destination IP address is in the 192.0.2.0/24 subnet. Default value: "none"

Listenpriority

Integer specifying the priority of the listen policy. A higher number specifies a lower priority. If a request matches the listen policies of more than one virtual server the virtual server whose listen policy has the highest priority (the lowest priority number) accepts the request. Default value: 101 Maximum value: 101

resRule

Default syntax expression specifying which part of a server's response to use for creating rule based persistence sessions (persistence type RULE). Can be either an expression or the name of a named expression. Example:
HTTP.RES.HEADER("setcookie").VALUE(0).TYPECAST_NVLIST_T('=';';').VALUE("server1").
Default value: "none"

persistMask

Persistence mask for IP based persistence types, for IPv4 virtual servers. Default value: 0xFFFFFFFF

v6persistmasklen

Persistence mask for IP based persistence types, for IPv6 virtual servers. Default value: 128 Minimum value: 1 Maximum value: 128

pq

Use priority queuing on the virtual server. based persistence types, for IPv6 virtual servers. Possible values: ON, OFF Default value: OFF

sc

Use SureConnect on the virtual server. Possible values: ON, OFF Default value: OFF

rtspNat

Use network address translation (NAT) for RTSP data connections. Possible values: ON, OFF Default value: OFF

m

Redirection mode for load balancing. Available settings function as follows: * IP - Before forwarding a request to a server, change the destination IP address to the server's IP address. * MAC - Before forwarding a request to a server, change the destination MAC address to the server's MAC address. The destination IP address is not changed. MAC-based redirection mode is used mostly in firewall load balancing deployments. * IPTUNNEL - Perform IP-in-IP encapsulation for client IP packets. In the outer IP headers, set the destination IP address to the IP address of the server and the source IP address to the subnet IP (SNIP). The client IP packets are not modified. Applicable to both IPv4 and IPv6 packets. * TOS - Encode the virtual server's TOS ID in the TOS field of the IP header. You can use either the IPTUNNEL or the TOS option to implement Direct Server Return (DSR). Possible values: IP, MAC, IPTUNNEL, TOS Default value: NSFWD_IP

tosId

TOS ID of the virtual server. Applicable only when the load balancing redirection mode is set to TOS. Minimum value: 1 Maximum value: 63

dataLength

Length of the token to be extracted from the data segment of an incoming packet, for use in the token method of load balancing. The length of the token, specified in bytes, must not be greater than 24 KB. Applicable to virtual servers of type TCP. Minimum value: 1 Maximum value: 100

dataOffset

Offset to be considered when extracting a token from the TCP payload. Applicable to virtual servers, of type TCP, using the token method of load balancing. Must be within the first 24 KB of the TCP payload. Maximum value: 25400

sessionless

Perform load balancing on a per-packet basis, without establishing sessions. Recommended for load balancing of intrusion detection system (IDS) servers and scenarios involving direct server return (DSR), where session information is unnecessary. Possible values: ENABLED, DISABLED Default value: DISABLED

state

State of the load balancing virtual server. Possible values: ENABLED, DISABLED Default value: ENABLED

connfailover

Mode in which the connection failover feature must operate for the virtual server. After a failover, established TCP connections and UDP packet flows are kept active and resumed on the secondary appliance. Clients remain connected to the same servers. Available settings function as follows: * STATEFUL - The primary appliance shares state information with the secondary appliance, in real time, resulting in some runtime processing overhead. * STATELESS - State information is not shared, and the new primary appliance tries to re-create the packet flow on the basis of the information contained in the packets it receives. * DISABLED - Connection failover does not occur. Possible values: DISABLED, STATEFUL, STATELESS Default value: DISABLED

redirectURL

URL to which to redirect traffic if the virtual server becomes unavailable. WARNING! Make sure that the domain in the URL does not match the domain specified for a content switching policy. If it does, requests are continuously redirected to the unavailable virtual server.

cacheable

Route cacheable requests to a cache redirection virtual server. The load balancing virtual server can forward requests only to a transparent cache redirection virtual server that has an IP address and port combination of *:80, so such a cache redirection virtual server must be configured on the appliance. Possible values: YES, NO Default value: NO

cltTimeout

Idle time, in seconds, after which a client connection is terminated. Default value: VAL_NOT_SET Maximum value: 31536000

soMethod

Type of threshold that, when exceeded, triggers spillover. Available settings function as follows: * CONNECTION - Spillover occurs when the number of client connections exceeds the threshold. * DYNAMICCONNECTION - Spillover occurs when the number of client connections at the virtual server exceeds the sum of the maximum client (Max Clients) settings for bound services. Do not specify a spillover threshold for this setting, because the threshold is implied by the Max Clients settings of bound services. * BANDWIDTH - Spillover occurs when the bandwidth consumed by the virtual server's incoming and outgoing traffic exceeds the threshold. * HEALTH - Spillover occurs when the percentage of weights of the services that are UP drops below the threshold. For example, if services svc1, svc2, and svc3 are bound to a virtual server, with weights 1, 2, and 3, and the spillover threshold is 50%, spillover occurs if svc1 and svc3 or svc2 and svc3 transition to DOWN. * NONE - Spillover does

not occur. Possible values: CONNECTION, DYNAMICCONNECTION, BANDWIDTH, HEALTH, NONE

soPersistence

If spillover occurs, maintain source IP address based persistence for both primary and backup virtual servers. Possible values: ENABLED, DISABLED Default value: DISABLED

soPersistenceTimeout

Timeout for spillover persistence, in minutes. Default value: 2 Minimum value: 2 Maximum value: 1440

healthThreshold

Threshold in percent of active services below which vserver state is made down. If this threshold is 0, vserver state will be up even if one bound service is up. Maximum value: 100

soThreshold

Threshold at which spillover occurs. Specify an integer for the CONNECTION spillover method, a bandwidth value in kilobits per second for the BANDWIDTH method (do not enter the units), or a percentage for the HEALTH method (do not enter the percentage symbol). Minimum value: 1 Maximum value: 4294967287

soBackupAction

Action to be performed if spillover is to take effect, but no backup chain to spillover is usable or exists Possible values: DROP, ACCEPT, REDIRECT

redirectPortRewrite

Rewrite the port and change the protocol to ensure successful HTTP redirects from services. Possible values: ENABLED, DISABLED Default value: DISABLED

downStateFlush

Flush all active transactions associated with a virtual server whose state transitions from UP to DOWN. Do not enable this option for applications that must complete their transactions. Possible values: ENABLED, DISABLED Default value: ENABLED

backupVServer

Name of the backup virtual server to which to forward requests if the primary virtual server goes DOWN or reaches its spillover threshold.

disablePrimaryOnDown

If the primary virtual server goes down, do not allow it to return to primary status until manually enabled. Possible values: ENABLED, DISABLED Default value: DISABLED

insertVserverIPPort

Insert an HTTP header, whose value is the IP address and port number of the virtual server, before forwarding a request to the server. The format of the header is <vipHeader>: <virtual server IP address>_<port number >, where vipHeader is the name that you specify for the header. If the virtual server has an IPv6 address, the address in the header is enclosed in brackets ([and]) to separate it from the port number. If you have mapped an IPv4 address to a virtual server's IPv6 address, the value of this parameter determines which IP address is inserted in the header, as follows: * VIPADDR - Insert the IP address of the virtual server in the HTTP header regardless of whether the virtual server has an IPv4 address or an IPv6 address. A mapped IPv4 address, if configured, is ignored. * V6TOV4MAPPING - Insert the IPv4 address that is mapped to the virtual server's IPv6 address. If a mapped IPv4 address

is not configured, insert the IPv6 address. * OFF - Disable header insertion. Possible values: OFF, VIPADDR, V6TOV4MAPPING

AuthenticationHost

Fully qualified domain name (FQDN) of the authentication virtual server to which the user must be redirected for authentication. Make sure that the Authentication parameter is set to ENABLED.

Authentication

Enable or disable user authentication. Possible values: ON, OFF Default value: OFF

authn401

Enable or disable user authentication with HTTP 401 responses. Possible values: ON, OFF Default value: OFF

authnVsName

Name of an authentication virtual server with which to authenticate users.

push

Process traffic with the push virtual server that is bound to this load balancing virtual server. Possible values: ENABLED, DISABLED Default value: DISABLED

pushVserver

Name of the load balancing virtual server, of type PUSH or SSL_PUSH, to which the server pushes updates received on the load balancing virtual server that you are configuring.

pushLabel

Expression for extracting a label from the server's response. Can be either an expression or the name of a named expression. Default value: "none"

pushMultiClients

Allow multiple Web 2.0 connections from the same client to connect to the virtual server and expect updates. Possible values: YES, NO Default value: NO

tcpProfileName

Name of the TCP profile whose settings are to be applied to the virtual server.

httpProfileName

Name of the HTTP profile whose settings are to be applied to the virtual server.

dbProfileName

Name of the DB profile whose settings are to be applied to the virtual server.

comment

Any comments that you might want to associate with the virtual server.

l2Conn

Use Layer 2 parameters (channel number, MAC address, and VLAN ID) in addition to the 4-tuple (<source IP>:<source port>:<destination IP>:<destination port>) that is used to identify a connection. Allows multiple TCP and non-TCP connections with the same 4-tuple to co-exist on the NetScaler appliance. Possible values: ON, OFF

mssqlServerVersion

For a load balancing virtual server of type MSSQL, the Microsoft SQL Server version. Set this parameter if you expect some clients to run a version different from the

version of the database. This setting provides compatibility between the client-side and server-side connections by ensuring that all communication conforms to the server's version. Possible values: 70, 2000, 2000SP1, 2005, 2008, 2008R2, 2012
Default value: TDS_PROT_2008B

mysqlProtocolVersion

MySQL protocol version that the virtual server advertises to clients. Default value: NSA_MYSQL_PROTOCOL_VER_DEFAULT

mysqlServerVersion

MySQL server version string that the virtual server advertises to clients. Default value: NSA_MYSQL_SERVER_VER_DEFAULT

mysqlCharacterSet

Character set that the virtual server advertises to clients. Default value: NSA_MYSQL_CHAR_SET_DEFAULT

mysqlServerCapabilities

Server capabilities that the virtual server advertises to clients. Default value: NSA_MYSQL_SVR_CAPABILITIES_DEFAULT

appflowLog

Apply AppFlow logging to the virtual server. Possible values: ENABLED, DISABLED
Default value: ENABLED

netProfile

Name of the network profile to associate with the virtual server. If you set this parameter, the virtual server uses only the IP addresses in the network profile as source IP addresses when initiating connections with servers.

icmpVsrResponse

How the NetScaler appliance responds to ping requests received for an IP address that is common to one or more virtual servers. Available settings function as follows:
* If set to PASSIVE on all the virtual servers that share the IP address, the appliance always responds to the ping requests. * If set to ACTIVE on all the virtual servers that share the IP address, the appliance responds to the ping requests if at least one of the virtual servers is UP. Otherwise, the appliance does not respond. * If set to ACTIVE on some virtual servers and PASSIVE on the others, the appliance responds if at least one virtual server with the ACTIVE setting is UP. Otherwise, the appliance does not respond. Note: This parameter is available at the virtual server level. A similar parameter, ICMP Response, is available at the IP address level, for IPv4 addresses of type VIP. To set that parameter, use the add ip command in the CLI or the Create IP dialog box in the GUI. Possible values: PASSIVE, ACTIVE Default value: NS_VSR_PASSIVE

newServiceRequest

Number of requests, or percentage of the load on existing services, by which to increase the load on a new service at each interval in slow-start mode. A value of 0 disables slow start for new services, and any services still ramping up. They immediately receive their full share of the load. If you use the CLI, be sure to set the newServiceRequestUnit parameter to specify the unit as number of requests or percentage of load.

newServiceRequestIncrementInterval

Interval, in seconds, between successive increments in the load on a new service or a service whose state has just changed from DOWN to UP. A value of 0 (zero) specifies manual slow start. Maximum value: 3600

minAutoscaleMembers

Minimum number of members expected to be present when vserver is used in Autoscale. Maximum value: 5000

maxAutoscaleMembers

Maximum number of members expected to be present when vserver is used in Autoscale. Maximum value: 5000

persistAVPno

Persist AVP number for Diameter Persistency. In case this AVP is not defined in Base RFC 3588 and it is nested inside a Grouped AVP, define a sequence of AVP numbers (max 3) in order of parent to child. So say persist AVP number X is nested inside AVP Y which is nested in Z, then define the list as Z Y X Minimum value: 1

skippersistency

This argument decides the behavior incase the service which is selected from an existing persistence session has reached threshold. Possible values: Bypass, ReLb, None Default value: NS_DONT_SKIPPERISIST

td

Traffic Domain ID Maximum value: 4094

authnProfile

Name of the authentication profile to be used when authentication is turned on.

macmodeRetainvlan

This option is used to retain vlan information of incoming packet when macmode is enabled Possible values: ENABLED, DISABLED Default value: DISABLED

dbslb

For enabling database specific load-balacing.. Possible values: ENABLED, DISABLED Default value: DISABLED

dns64

This argument is for enabling/disabling the dns64 on lbvserver Possible values: ENABLED, DISABLED

bypassAAAA

If this option is enabled while resolving DNS64 query AAAA queries are not sent to back end dns server Possible values: YES, NO Default value: NO

RecursionAvailable

When set to YES, this option causes the DNS replies from this vserver to have the RA bit turned on. Typically one would set this option to YES, when the vserver is load balancing a set of DNS servers thatsupport recursive queries. Possible values: YES, NO Default value: NO

Example

```
add lb vserver http_vsvr http 10.102.1.10 80
    To add multiple vservers at once use the
    following command:
    add lb vs http_vsvr[1-4] http 10.102.27.
    [115-118] 80
    This command adds the vserver http_vsvr1 with
    the IP address 10.102.27.115, http_vsvr2 with
    10.102.27.116, http_vsvr3 with 10.102.27.117 and
    http_vsvr4 with 10.102.27.118
```

[Top](#)**rm lb vserver****Synopsis**

```
rm lb vserver <name>@ ...
```

Description

Removes a virtual server from the NetScaler appliance.

Parameters

name

Name of the virtual server.

Example

```
rm vserver lb_vip
    To remove multiple vservers use the following
    command:
    rm vserver lb_vip[1-3]
```

[Top](#)**set lb vserver****Synopsis**

```
set lb vserver <name>@ [-IPAddress <ip_addr|ipv6_addr|*>@] [-IPPattern <ippat>] [-
IPMask <ipmask>] [-weight <positive_integer> <serviceName>@] [-persistenceType
<persistenceType>] [-timeout <mins>] [-persistenceBackup ( SOURCEIP | NONE )] [-
backupPersistenceTimeout <mins>] [-lbMethod <lbMethod>] [-hashLength
<positive_integer>] [-netmask <netmask>] [-v6netmasklen <positive_integer>] [-rule
<expression>] [-cookieName <string>] [-resRule <expression>] [-persistMask <netmask>]
[-v6persistmasklen <positive_integer>] [-pq ( ON | OFF )] [-sc ( ON | OFF )] [-rtspNat
( ON | OFF )] [-m <m>] [-tosId <positive_integer>] [-dataLength <positive_integer>] [-
dataOffset <positive_integer>] [-sessionless ( ENABLED | DISABLED )] [-connfailover
<connfailover>] [-backupVServer <string>] [-redirectURL <URL>] [-cacheable ( YES |
```

```

NO )) [-cltTimeout <secs>] [-soMethod <soMethod>] [-soThreshold <positive_integer>] [-
soPersistence ( ENABLED | DISABLED )) [-soPersistenceTimeOut <positive_integer>] [-
healthThreshold <positive_integer>] [-soBackupAction <soBackupAction>] [-
redirectPortRewrite ( ENABLED | DISABLED )) [-downStateFlush ( ENABLED | DISABLED ))
[-insertVserverIPPort <insertVserverIPPort> [<vipHeader>] ] [-disablePrimaryOnDown
( ENABLED | DISABLED )) [-AuthenticationHost <string>] [-Authentication ( ON | OFF ))
[-authn401 ( ON | OFF )) [-authnVsName <string>] [-push ( ENABLED | DISABLED )) [-
pushVserver <string>] [-pushLabel <expression>] [-pushMultiClients ( YES | NO )) [-
Listenpolicy <expression>] [-Listenpriority <positive_integer>] [-tcpProfileName
<string>] [-httpProfileName <string>] [-dbProfileName <string>] [-comment <string>] [-
l2Conn ( ON | OFF )) [-mssqlServerVersion <mssqlServerVersion>] [-
mysqlProtocolVersion <positive_integer>] [-mysqlServerVersion <string>] [-
mysqlCharacterSet <positive_integer>] [-mysqlServerCapabilities <positive_integer>] [-
appflowLog ( ENABLED | DISABLED )) [-netProfile <string>] [-icmpVsrResponse ( PASSIVE
| ACTIVE )) [-newServiceRequest <positive_integer>] [-<newServiceRequestUnit>] [-
newServiceRequestIncrementInterval <positive_integer>] [-minAutoscaleMembers
<positive_integer>] [-maxAutoscaleMembers <positive_integer>] [-persistAVPno
<positive_integer> ...] [-skippersistency <skippersistency>] [-authnProfile <string>] [-
macmodeRetainvlan ( ENABLED | DISABLED )) [-dbsLb ( ENABLED | DISABLED )) [-dns64
( ENABLED | DISABLED )) [-bypassAAAA ( YES | NO )) [-RecursionAvailable ( YES | NO ))

```

Description

Modifies the specified parameters of a load balancing virtual server.

Parameters

name

Name of the virtual server.

IPAddress

IPv4 or IPv6 address to assign to the virtual server.

IPPattern

IP address pattern, in dotted decimal notation, for identifying packets to be accepted by the virtual server. The IP Mask parameter specifies which part of the destination IP address is matched against the pattern. Mutually exclusive with the IP Address parameter. For example, if the IP pattern assigned to the virtual server is 198.51.100.0 and the IP mask is 255.255.240.0 (a forward mask), the first 20 bits in the destination IP addresses are matched with the first 20 bits in the pattern. The virtual server accepts requests with IP addresses that range from 198.51.96.1 to 198.51.111.254. You can also use a pattern such as 0.0.2.2 and a mask such as 0.0.255.255 (a reverse mask). If a destination IP address matches more than one IP pattern, the pattern with the longest match is selected, and the associated virtual server processes the request. For example, if virtual servers vs1 and vs2 have the same IP pattern, 0.0.100.128, but different IP masks of 0.0.255.255 and 0.0.224.255, a destination IP address of 198.51.100.128 has the longest match with the IP pattern of vs1. If a destination IP address matches two or more virtual servers to the same extent, the request is processed by the virtual server whose port number matches the port number in the request.

IPMask

IP mask, in dotted decimal notation, for the IP Pattern parameter. Can have leading or trailing non-zero octets (for example, 255.255.240.0 or 0.0.255.255). Accordingly,

the mask specifies whether the first n bits or the last n bits of the destination IP address in a client request are to be matched with the corresponding bits in the IP pattern. The former is called a forward mask. The latter is called a reverse mask.

weight

Weight to assign to the specified service. Minimum value: 1 Maximum value: 100

persistenceType

Type of persistence for the virtual server. Available settings function as follows: * SOURCEIP - Connections from the same client IP address belong to the same persistence session. * COOKIEINSERT - Connections that have the same HTTP Cookie, inserted by a Set-Cookie directive from a server, belong to the same persistence session. * SSLSESSION - Connections that have the same SSL Session ID belong to the same persistence session. * CUSTOMSERVERID - Connections with the same server ID form part of the same session. For this persistence type, set the Server ID (CustomServerID) parameter for each service and configure the Rule parameter to identify the server ID in a request. * RULE - All connections that match a user defined rule belong to the same persistence session. * URLPASSIVE - Requests that have the same server ID in the URL query belong to the same persistence session. The server ID is the hexadecimal representation of the IP address and port of the service to which the request must be forwarded. This persistence type requires a rule to identify the server ID in the request. * DESTIP - Connections to the same destination IP address belong to the same persistence session. * SRCIPDESTIP - Connections that have the same source IP address and destination IP address belong to the same persistence session. * CALLID - Connections that have the same CALL-ID SIP header belong to the same persistence session. * RTSPSID - Connections that have the same RTSP Session ID belong to the same persistence session. Possible values: SOURCEIP, COOKIEINSERT, SSLSESSION, RULE, URLPASSIVE, CUSTOMSERVERID, DESTIP, SRCIPDESTIP, CALLID, RTSPSID, DIAMETER, NONE

timeout

Time period for which a persistence session is in effect. Default value: 2 Maximum value: 1440

persistenceBackup

Backup persistence type for the virtual server. Becomes operational if the primary persistence mechanism fails. Possible values: SOURCEIP, NONE

backupPersistenceTimeout

Time period for which backup persistence is in effect. Default value: 2 Minimum value: 2 Maximum value: 1440

lbMethod

Load balancing method. The available settings function as follows: * ROUNDROBIN - Distribute requests in rotation, regardless of the load. Weights can be assigned to services to enforce weighted round robin distribution. * LEASTCONNECTION (default) - Select the service with the fewest connections. * LEASTRESPONSETIME - Select the service with the lowest average response time. * LEASTBANDWIDTH - Select the service currently handling the least traffic. * LEASTPACKETS - Select the service currently serving the lowest number of packets per second. * CUSTOMLOAD - Base service selection on the SNMP metrics obtained by custom load monitors. * LRTM - Select the service with the lowest response time. Response times are learned through monitoring probes. This method also takes the number of active connections

into account. Also available are a number of hashing methods, in which the appliance extracts a predetermined portion of the request, creates a hash of the portion, and then checks whether any previous requests had the same hash value. If it finds a match, it forwards the request to the service that served those previous requests. Following are the hashing methods: * URLHASH - Create a hash of the request URL (or part of the URL). * DOMAINHASH - Create a hash of the domain name in the request (or part of the domain name). The domain name is taken from either the URL or the Host header. If the domain name appears in both locations, the URL is preferred. If the request does not contain a domain name, the load balancing method defaults to LEASTCONNECTION. * DESTINATIONIPHASH - Create a hash of the destination IP address in the IP header. * SOURCEIPHASH - Create a hash of the source IP address in the IP header. * TOKEN - Extract a token from the request, create a hash of the token, and then select the service to which any previous requests with the same token hash value were sent. * SRCIPDESTIPHASH - Create a hash of the string obtained by concatenating the source IP address and destination IP address in the IP header. * SRCIPSRCPORTHASH - Create a hash of the source IP address and source port in the IP header. * CALLIDHASH - Create a hash of the SIP Call-ID header. Possible values: ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, URLHASH, DOMAINHASH, DESTINATIONIPHASH, SOURCEIPHASH, SRCIPDESTIPHASH, LEASTBANDWIDTH, LEASTPACKETS, TOKEN, SRCIPSRCPORTHASH, LRTM, CALLIDHASH, CUSTOMLOAD, LEASTREQUEST Default value: PEMGMT_LB_LEASTCONNS

rule

Expression, or name of a named expression, against which traffic is evaluated. Written in the classic or default syntax. Note: Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>" The following requirements apply only to the NetScaler CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks. Default value: "none"

cookieName

Use this parameter to specify the cookie name for COOKIE persistence type. It specifies the name of cookie with a maximum of 32 characters. If not specified, cookie name is internally generated.

resRule

Default syntax expression specifying which part of a server's response to use for creating rule based persistence sessions (persistence type RULE). Can be either an expression or the name of a named expression. Example:
HTTP.RES.HEADER("setcookie").VALUE(0).TYPECAST_NVLIST_T('=';';').VALUE("server1").
Default value: "none"

persistMask

Persistence mask for IP based persistence types, for IPv4 virtual servers. Default value: 0xFFFFFFFF

v6persistmasklen

Persistence mask for IP based persistence types, for IPv6 virtual servers. Default value: 128 Minimum value: 1 Maximum value: 128

pq

Use priority queuing on the virtual server. based persistence types, for IPv6 virtual servers. Possible values: ON, OFF Default value: OFF

sc

Use SureConnect on the virtual server. Possible values: ON, OFF Default value: OFF

rtspNat

Use network address translation (NAT) for RTSP data connections. Possible values: ON, OFF Default value: OFF

m

Redirection mode for load balancing. Available settings function as follows: * IP - Before forwarding a request to a server, change the destination IP address to the server's IP address. * MAC - Before forwarding a request to a server, change the destination MAC address to the server's MAC address. The destination IP address is not changed. MAC-based redirection mode is used mostly in firewall load balancing deployments. * IPTUNNEL - Perform IP-in-IP encapsulation for client IP packets. In the outer IP headers, set the destination IP address to the IP address of the server and the source IP address to the subnet IP (SNIP). The client IP packets are not modified. Applicable to both IPv4 and IPv6 packets. * TOS - Encode the virtual server's TOS ID in the TOS field of the IP header. You can use either the IPTUNNEL or the TOS option to implement Direct Server Return (DSR). Possible values: IP, MAC, IPTUNNEL, TOS Default value: NSFWD_IP

tosId

TOS ID of the virtual server. Applicable only when the load balancing redirection mode is set to TOS. Minimum value: 1 Maximum value: 63

dataLength

Length of the token to be extracted from the data segment of an incoming packet, for use in the token method of load balancing. The length of the token, specified in bytes, must not be greater than 24 KB. Applicable to virtual servers of type TCP. Minimum value: 1 Maximum value: 100

dataOffset

Offset to be considered when extracting a token from the TCP payload. Applicable to virtual servers, of type TCP, using the token method of load balancing. Must be within the first 24 KB of the TCP payload. Maximum value: 25400

sessionless

Perform load balancing on a per-packet basis, without establishing sessions. Recommended for load balancing of intrusion detection system (IDS) servers and scenarios involving direct server return (DSR), where session information is unnecessary. Possible values: ENABLED, DISABLED Default value: DISABLED

connfailover

Mode in which the connection failover feature must operate for the virtual server. After a failover, established TCP connections and UDP packet flows are kept active and resumed on the secondary appliance. Clients remain connected to the same

servers. Available settings function as follows: * STATEFUL - The primary appliance shares state information with the secondary appliance, in real time, resulting in some runtime processing overhead. * STATELESS - State information is not shared, and the new primary appliance tries to re-create the packet flow on the basis of the information contained in the packets it receives. * DISABLED - Connection failover does not occur. Possible values: DISABLED, STATEFUL, STATELESS Default value: DISABLED

backupVServer

Name of the backup virtual server to which to forward requests if the primary virtual server goes DOWN or reaches its spillover threshold.

redirectURL

URL to which to redirect traffic if the virtual server becomes unavailable. WARNING! Make sure that the domain in the URL does not match the domain specified for a content switching policy. If it does, requests are continuously redirected to the unavailable virtual server.

cacheable

Route cacheable requests to a cache redirection virtual server. The load balancing virtual server can forward requests only to a transparent cache redirection virtual server that has an IP address and port combination of *:80, so such a cache redirection virtual server must be configured on the appliance. Possible values: YES, NO Default value: NO

cltTimeout

Idle time, in seconds, after which a client connection is terminated. Default value: VAL_NOT_SET Maximum value: 31536000

soMethod

Type of threshold that, when exceeded, triggers spillover. Available settings function as follows: * CONNECTION - Spillover occurs when the number of client connections exceeds the threshold. * DYNAMICCONNECTION - Spillover occurs when the number of client connections at the virtual server exceeds the sum of the maximum client (Max Clients) settings for bound services. Do not specify a spillover threshold for this setting, because the threshold is implied by the Max Clients settings of bound services. * BANDWIDTH - Spillover occurs when the bandwidth consumed by the virtual server's incoming and outgoing traffic exceeds the threshold. * HEALTH - Spillover occurs when the percentage of weights of the services that are UP drops below the threshold. For example, if services svc1, svc2, and svc3 are bound to a virtual server, with weights 1, 2, and 3, and the spillover threshold is 50%, spillover occurs if svc1 and svc3 or svc2 and svc3 transition to DOWN. * NONE - Spillover does not occur. Possible values: CONNECTION, DYNAMICCONNECTION, BANDWIDTH, HEALTH, NONE

soPersistence

If spillover occurs, maintain source IP address based persistence for both primary and backup virtual servers. Possible values: ENABLED, DISABLED Default value: DISABLED

soPersistenceTimeOut

Timeout for spillover persistence, in minutes. Default value: 2 Minimum value: 2 Maximum value: 1440

healthThreshold

Threshold in percent of active services below which vserver state is made down. If this threshold is 0, vserver state will be up even if one bound service is up. Maximum value: 100

soBackupAction

Action to be performed if spillover is to take effect, but no backup chain to spillover is usable or exists Possible values: DROP, ACCEPT, REDIRECT

redirectPortRewrite

Rewrite the port and change the protocol to ensure successful HTTP redirects from services. Possible values: ENABLED, DISABLED Default value: DISABLED

downStateFlush

Flush all active transactions associated with a virtual server whose state transitions from UP to DOWN. Do not enable this option for applications that must complete their transactions. Possible values: ENABLED, DISABLED Default value: ENABLED

insertVserverIPPort

Insert an HTTP header, whose value is the IP address and port number of the virtual server, before forwarding a request to the server. The format of the header is <vipHeader>: <virtual server IP address>_<port number >, where vipHeader is the name that you specify for the header. If the virtual server has an IPv6 address, the address in the header is enclosed in brackets ([and]) to separate it from the port number. If you have mapped an IPv4 address to a virtual server's IPv6 address, the value of this parameter determines which IP address is inserted in the header, as follows: * VIPADDR - Insert the IP address of the virtual server in the HTTP header regardless of whether the virtual server has an IPv4 address or an IPv6 address. A mapped IPv4 address, if configured, is ignored. * V6TOV4MAPPING - Insert the IPv4 address that is mapped to the virtual server's IPv6 address. If a mapped IPv4 address is not configured, insert the IPv6 address. * OFF - Disable header insertion. Possible values: OFF, VIPADDR, V6TOV4MAPPING

disablePrimaryOnDown

If the primary virtual server goes down, do not allow it to return to primary status until manually enabled. Possible values: ENABLED, DISABLED Default value: DISABLED

AuthenticationHost

Fully qualified domain name (FQDN) of the authentication virtual server to which the user must be redirected for authentication. Make sure that the Authentication parameter is set to ENABLED.

Authentication

Enable or disable user authentication. Possible values: ON, OFF Default value: OFF

authn401

Enable or disable user authentication with HTTP 401 responses. Possible values: ON, OFF Default value: OFF

authnVsName

Name of an authentication virtual server with which to authenticate users.

push

Process traffic with the push virtual server that is bound to this load balancing virtual server. Possible values: ENABLED, DISABLED Default value: DISABLED

pushVserver

Name of the load balancing virtual server, of type PUSH or SSL_PUSH, to which the server pushes updates received on the load balancing virtual server that you are configuring.

pushLabel

Expression for extracting a label from the server's response. Can be either an expression or the name of a named expression. Default value: "none"

pushMultiClients

Allow multiple Web 2.0 connections from the same client to connect to the virtual server and expect updates. Possible values: YES, NO Default value: NO

Listenpolicy

Default syntax expression identifying traffic accepted by the virtual server. Can be either an expression (for example, CLIENT.IP.DST.IN_SUBNET(192.0.2.0/24) or the name of a named expression. In the above example, the virtual server accepts all requests whose destination IP address is in the 192.0.2.0/24 subnet. Default value: "none"

Listenpriority

Integer specifying the priority of the listen policy. A higher number specifies a lower priority. If a request matches the listen policies of more than one virtual server the virtual server whose listen policy has the highest priority (the lowest priority number) accepts the request. Default value: 101 Maximum value: 101

tcpProfileName

Name of the TCP profile whose settings are to be applied to the virtual server.

httpProfileName

Name of the HTTP profile whose settings are to be applied to the virtual server.

dbProfileName

Name of the DB profile whose settings are to be applied to the virtual server.

comment

Any comments that you might want to associate with the virtual server.

l2Conn

Use Layer 2 parameters (channel number, MAC address, and VLAN ID) in addition to the 4-tuple (<source IP>:<source port>:<destination IP>:<destination port>) that is used to identify a connection. Allows multiple TCP and non-TCP connections with the same 4-tuple to co-exist on the NetScaler appliance. Possible values: ON, OFF

mssqlServerVersion

For a load balancing virtual server of type MSSQL, the Microsoft SQL Server version. Set this parameter if you expect some clients to run a version different from the version of the database. This setting provides compatibility between the client-side and server-side connections by ensuring that all communication conforms to the server's version. Possible values: 70, 2000, 2000SP1, 2005, 2008, 2008R2, 2012 Default value: TDS_PROT_2008B

mysqlProtocolVersion

MySQL protocol version that the virtual server advertises to clients. Default value: NSA_MYSQL_PROTOCOL_VER_DEFAULT

mysqlServerVersion

MySQL server version string that the virtual server advertises to clients. Default value: NSA_MYSQL_SERVER_VER_DEFAULT

mysqlCharacterSet

Character set that the virtual server advertises to clients. Default value: NSA_MYSQL_CHAR_SET_DEFAULT

mysqlServerCapabilities

Server capabilities that the virtual server advertises to clients. Default value: NSA_MYSQL_SVR_CAPABILITIES_DEFAULT

appflowLog

Apply AppFlow logging to the virtual server. Possible values: ENABLED, DISABLED
Default value: ENABLED

netProfile

Name of the network profile to associate with the virtual server. If you set this parameter, the virtual server uses only the IP addresses in the network profile as source IP addresses when initiating connections with servers.

icmpVsrResponse

How the NetScaler appliance responds to ping requests received for an IP address that is common to one or more virtual servers. Available settings function as follows:
* If set to PASSIVE on all the virtual servers that share the IP address, the appliance always responds to the ping requests. * If set to ACTIVE on all the virtual servers that share the IP address, the appliance responds to the ping requests if at least one of the virtual servers is UP. Otherwise, the appliance does not respond. * If set to ACTIVE on some virtual servers and PASSIVE on the others, the appliance responds if at least one virtual server with the ACTIVE setting is UP. Otherwise, the appliance does not respond. Note: This parameter is available at the virtual server level. A similar parameter, ICMP Response, is available at the IP address level, for IPv4 addresses of type VIP. To set that parameter, use the add ip command in the CLI or the Create IP dialog box in the GUI. Possible values: PASSIVE, ACTIVE Default value: NS_VSR_PASSIVE

newServiceRequest

Number of requests, or percentage of the load on existing services, by which to increase the load on a new service at each interval in slow-start mode. A value of 0 disables slow start for new services, and any services still ramping up. They immediately receive their full share of the load. If you use the CLI, be sure to set the newServiceRequestUnit parameter to specify the unit as number of requests or percentage of load.

newServiceRequestIncrementInterval

Interval, in seconds, between successive increments in the load on a new service or a service whose state has just changed from DOWN to UP. A value of 0 (zero) specifies manual slow start. Maximum value: 3600

minAutoscaleMembers

Minimum number of members expected to be present when vserver is used in Autoscale. Maximum value: 5000

maxAutoscaleMembers

Maximum number of members expected to be present when vserver is used in Autoscale. Maximum value: 5000

persistAVPno

Persist AVP number for Diameter Persistency. In case this AVP is not defined in Base RFC 3588 and it is nested inside a Grouped AVP, define a sequence of AVP numbers (max 3) in order of parent to child. So say persist AVP number X is nested inside AVP Y which is nested in Z, then define the list as Z Y X Minimum value: 1

skippersistency

This argument decides the behavior incase the service which is selected from an existing persistence session has reached threshold. Possible values: Bypass, ReLb, None Default value: NS_DONT_SKIPPERISIT

authnProfile

Name of the authentication profile to be used when authentication is turned on.

macmodeRetainvlan

This option is used to retain vlan information of incoming packet when macmode is enabled Possible values: ENABLED, DISABLED Default value: DISABLED

dbslb

For enabling database specific load-balacing.. Possible values: ENABLED, DISABLED Default value: DISABLED

dns64

This argument is for enabling/disabling the dns64 on lbvserver Possible values: ENABLED, DISABLED

bypassAAAA

If this option is enabled while resolving DNS64 query AAAA queries are not sent to back end dns server Possible values: YES, NO Default value: NO

RecursionAvailable

When set to YES, this option causes the DNS replies from this vserver to have the RA bit turned on. Typically one would set this option to YES, when the vserver is load balancing a set of DNS servers that support recursive queries. Possible values: YES, NO Default value: NO

Example

```
set lb vserver http_vip -lbmethod
LEASTRESPONSETIME
    To set the load balancing method for multiple
    vserver use the following command:
    set lb vserver http_vip[1-3] -lbmethod
    LEASTRESPONSETIME
```

[Top](#)

unset lb vserver

Synopsis

```
unset lb vserver <name>@ [-backupVServer] [-cltTimeout] [-redirectURL] [-authn401] [-
Authentication] [-AuthenticationHost] [-authnVsName] [-pushVserver] [-pushLabel] [-
tcpProfileName] [-httpProfileName] [-dbProfileName] [-rule] [-l2Conn] [-
mysqlProtocolVersion] [-mysqlServerVersion] [-mysqlCharacterSet] [-
mysqlServerCapabilities] [-appflowLog] [-netProfile] [-icmpVsrResponse] [-
skippersistency] [-minAutoscaleMembers] [-maxAutoscaleMembers] [-authnProfile] [-
macmodeRetainvlan] [-dbsLb] [-serviceName] [-persistenceType] [-timeout] [-
persistenceBackup] [-backupPersistenceTimeout] [-lbMethod] [-hashLength] [-netmask]
[-v6netmasklen] [-cookieName] [-resRule] [-persistMask] [-v6persistmasklen] [-pq] [-sc]
[-rtspNat] [-m] [-tosId] [-dataLength] [-dataOffset] [-sessionless] [-connfailover] [-
cacheable] [-soMethod] [-soPersistence] [-soPersistenceTimeOut] [-healthThreshold] [-
soBackupAction] [-redirectPortRewrite] [-downStateFlush] [-insertVserverIPPort] [-
vipHeader] [-disablePrimaryOnDown] [-push] [-pushMultiClients] [-Listenpolicy] [-
Listenpriority] [-comment] [-mssqlServerVersion] [-newServiceRequest] [-
newServiceRequestUnit] [-newServiceRequestIncrementInterval] [-persistAVPno] [-
RecursionAvailable]
```

Description

Removes the specified parameter settings from the virtual server..Refer to the set lb vserver command for meanings of the arguments.

Example

```
unset lb vserver lb_vip -backupVServer
    To unset the backup virtual server for
    multiple vservers use the following command:
    unset lb vserver lb_vip[1-3] -backupVServer
```

[Top](#)

bind lb vserver

Synopsis

```
bind lb vserver <name>@ ((<serviceName>@ [-weight <positive_integer>] ) |
<serviceGroupName>@ | (-policyName <string>@ [-priority <positive_integer>] [-
gotoPriorityExpression <expression>] [-type ( REQUEST | RESPONSE )] [-invoke
(<labelType> <labelName> ) ] ))
```

Description

Binds a service, service group, or policy to a virtual server.

Parameters

name

Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period

(.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver').

serviceName

Name of the service.

serviceGroupName

Name of the service group.

policyName

Name of the policy to bind to the virtual server.

Example

```
bind lb vserver http_vip http_svc
    To bind a service to multiple vservers use the
    following command:
    bind lb vs http_vip[1-3] http_svc
    To bind multiple services to a vserver use the
    following command:
    bind lb vs http_vip http_svc[1-3]
```

[Top](#)

unbind lb vserver

Synopsis

```
unbind lb vserver <name>@ (<serviceName>@ | <serviceGroupName>@ | (-policyName
<string>@ [-type ( REQUEST | RESPONSE )])) [-priority <positive_integer>]
```

Description

Unbinds a service, service group, or policy from a virtual server.

Parameters

name

Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver').

serviceName

Name of the service.

serviceGroupName

The name of the service group that is unbound.

policyName

Name of the policy to bind to the virtual server.

priority

Priority number of the policy. Minimum value: 1 Maximum value: 2147483647

Example

```
unbind lb vs server http_vip http_svc
    To unbind a service from multiple vservers use
    the following command:
    unbind lb vs http_vip[1-3] http_svc
    To unbind multiple services from a vserver
    use the following command:
    unbind lb vs http_vip http_svc[1-3]
```

[Top](#)

enable lb vserver

Synopsis

enable lb vserver <name>@

Description

Enables a virtual server.

Parameters

name

Name of the virtual server.

Example

```
enable vserver lb_vip
    To enable multiple vservers at once use the
    following command:
    enable vserver lb_vip[1-3]
```

[Top](#)

disable lb vserver

Synopsis

disable lb vserver <name>@

Description

Disables a virtual server.

Parameters

name

Name of the virtual server.

Example

```
disable vsrver lb_vip
    To disable multiple vservers at once use the
    following command:
    disable vsrver lb_vip[1-3]
```

[Top](#)

show lb vsrver

Synopsis

show lb vsrver [<name>] show lb vsrver stats - alias for 'stat lb vsrver'

Description

Displays the statistical data collected for a load balancing virtual server.

Parameters

name

Name of the virtual server. If no name is provided, statistical data of all configured virtual servers is displayed.

[Top](#)

stat lb vsrver

Synopsis

stat lb vsrver [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-clearstats (basic | full)] [-sortBy Hits [<sortOrder>]]

Description

Displays the statistical data collected for a load balancing virtual server.

Parameters

name

Name of the virtual server. If no name is provided, statistical data of all configured virtual servers is displayed.

clearstats

Clear the statistics / counters Possible values: basic, full

sortBy

use this argument to sort by specific key Possible values: Hits

[Top](#)

rename lb vserver

Synopsis

rename lb vserver <name>@ <newName>@

Description

Renames a load balancing virtual server.

Parameters

name

Existing name of the virtual server.

newName

New name for the virtual server.

Example

```
rename lb vserver http_vsvr http_vsvr_new
```

[Top](#)

lb metricTable

[[add](#) | [rm](#) | [set](#) | [bind](#) | [unbind](#) | [show](#)]

add lb metricTable

Synopsis

add lb metricTable <metricTable>

Description

Creates a metric table for load monitoring.

Parameters

metricTable

Name for the metric table. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my metricktable" or 'my metricktable').

Example

```
add metricktable newtable
```

[Top](#)

rm lb metricTable

Synopsis

rm lb metricTable <metricTable>

Description

Removes a metric table.

Parameters

metricTable

Name of the metric table.

Example

```
rm metric table netscaler
```

[Top](#)

set lb metricTable

Synopsis

set lb metricTable <metricTable> <metric> <snmpOID>

Description

Modifies the SNMP OID of a metric in a metric table.

Parameters

metricTable

Name of the metric table.

Example

```
set metrictable table met1 aliasname oidstr
```

[Top](#)

bind lb metricTable

Synopsis

bind lb metricTable <metricTable> <metric> <snmpOID>

Description

Binds a metric to a metric table. You must also specify the SNMP OID of the metric.

Parameters

metricTable
Name of the metric table.

metric
Name of the metric.

Example

```
bind metrictable tablename aliasname 1.2.3.4
```

[Top](#)

unbind lb metricTable

Synopsis

```
unbind lb metricTable <metricTable> <metric>
```

Description

Unbinds a metric from a metric table.

Parameters

metricTable
Name of the metric table.

metric
Name of the metric to unbind.

Example

```
unbind metrictable tablename aliasname
```

[Top](#)

show lb metricTable

Synopsis

```
show lb metricTable [<metricTable>]
```

Description

Displays the parameters of the specified metric table. If no metric table name is specified, a list of all configured metric tables is displayed.

Parameters

metricTable
Name of the metric table.

Example

An example of the show metricktable command output is as follows:

```
Name : ALTEON
Type : INTERNAL
Name : CISCO-CSS
Type : INTERNAL
Name : FOUNDRY
Type : INTERNAL
Name : NETSCALER
Type : INTERNAL
Name : F5
Type : INTERNAL
Name : local
Type : INTERNAL
```

[Top](#)

lb monbindings

show lb monbindings

Synopsis

show lb monbindings <monitorName>

Description

Display the services to which this monitor is bound

Parameters

monitorName

The name of the monitor.

lb persistentSessions

[[show](#) | [clear](#)]

show lb persistentSessions

Synopsis

show lb persistentSessions [<vServer>]

Description

Get all vserver persistent sessions

Parameters

vServer

The name of the virtual server.

[Top](#)

clear lb persistentSessions

Synopsis

```
clear lb persistentSessions [<vServer>] [-persistenceParameter <string>]
```

Description

Use this command to clear/flush persistent sessions

Parameters

vServer

The name of the LB vserver whose persistence sessions are to be flushed. If not specified, all persistence sessions will be flushed .

persistenceParameter

The persistence parameter whose persistence sessions are to be flushed.

[Top](#)

lb group

[[set](#) | [unset](#) | [bind](#) | [unbind](#) | [show](#) | [rename](#)]

set lb group

Synopsis

```
set lb group <name>@ [-persistenceType <persistenceType>] [-persistenceBackup  
( SOURCEIP | NONE )] [-backupPersistenceTimeout <mins>] [-persistMask <netmask>] [-  
cookieName <string>] [-v6persistmasklen <positive_integer>] [-cookieDomain <string>]  
[-timeout <mins>] [-rule <expression>]
```

Description

Configures persistence for the specified load balancing group. The persistence settings are applied to all the members of the group.

Parameters

name

Name of the load balancing virtual server group.

persistenceType

Type of persistence for the group. Available settings function as follows: * SOURCEIP - Create persistence sessions based on the client IP. * COOKIEINSERT - Create persistence sessions based on a cookie in client requests. The cookie is inserted by a Set-Cookie directive from the server, in its first response to a client. * RULE - Create persistence sessions based on a user defined rule. * NONE - Disable persistence for the group. Possible values: SOURCEIP, COOKIEINSERT, RULE, NONE

persistenceBackup

Type of backup persistence for the group. Possible values: SOURCEIP, NONE

backupPersistenceTimeout

Time period, in minutes, for which backup persistence is in effect. Default value: 2
Minimum value: 2 Maximum value: 1440

persistMask

Persistence mask to apply to source IPv4 addresses when creating source IP based persistence sessions. Default value: 0xFFFFFFFF

cookieName

Use this parameter to specify the cookie name for COOKIE persistence type. It specifies the name of cookie with a maximum of 32 characters. If not specified, cookie name is internally generated.

v6persistmasklen

Persistence mask to apply to source IPv6 addresses when creating source IP based persistence sessions. Default value: 128 Minimum value: 1 Maximum value: 128

cookieDomain

Domain attribute for the HTTP cookie.

timeout

Time period for which a persistence session is in effect. Default value: 2 Maximum value: 1440

rule

Expression, or name of a named expression, against which traffic is evaluated. Written in the classic or default syntax. Note: Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>". The following requirements apply only to the NetScaler CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks. Default value: "None"

Example

```
set lb group webgrp -persistenceType COOKIEINSERT
    To set the persistence type for multiple
    groups use the following command:
    set lb group webgrp[1-3] -persistenceType
    COOKIEINSERT
```

[Top](#)

unset lb group

Synopsis

```
unset lb group <name>@ [-persistenceType] [-persistenceBackup] [-  
backupPersistenceTimeout] [-persistMask] [-cookieName] [-v6persistmasklen] [-  
cookieDomain] [-timeout] [-rule]
```

Description

Use this command to remove lb group settings. Refer to the set lb group command for meanings of the arguments.

[Top](#)

bind lb group

Synopsis

```
bind lb group <name>@ <vServerName>@ ...
```

Description

Binds one or more virtual servers to a load balancing virtual server group. If the specified group does not exist, the NetScaler appliance first creates the group, and then binds the virtual servers to it. A virtual server group enables you to specify common persistence settings for all of its members through a single set lb group command. Only address-based virtual servers can be added to a group. Content-based virtual servers (content switching and cache redirection virtual servers) cannot be added. A virtual server can be assigned to only one group at any given time. To move a virtual server from one group to another, the virtual server must first be unbound from the group to which it belongs.

Parameters

name

Name for the load balancing virtual server group. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the virtual server is created. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my lbgroup" or 'my lbgroup').

vServerName

Name of the virtual server to bind to the group. Multiple names can be specified.

Example

```
bind lb group webgrp http_vip  
    To bind multiple vservers to a group use the  
    following command:  
    bind lb group webgrp v[1-4]  
    To bind vserver v1 to group webgrp1, v2 to  
    webgrp2 and v3 to webgrp3, use the following
```

```
command:  
  bind lb group webgrp[1-3] v[1-3]
```

[Top](#)

unbind lb group

Synopsis

unbind lb group <name> <vServerName>@ ...

Description

Unbinds one or more virtual servers from a group. When the last virtual server is unbound, the group is removed.

Parameters

name

Name of the load balancing virtual server group.

vServerName

Name of the virtual server to unbind. Multiple names can be specified.

Example

```
unbind lb group webgroup http_vip  
  To unbind multiple vservers use the following  
command:  
  unbind lb group webgroup v[1-3]
```

[Top](#)

show lb group

Synopsis

show lb group [<name>]

Description

Displays the virtual servers bound to the specified group.

Parameters

name

Name of the load balancing virtual server group.

Example

```
show lb group webgrp
```

[Top](#)

rename lb group

Synopsis

rename lb group <name>@ <newName>@

Description

Renames a load balancing virtual server group.

Parameters

name

Existing name of the load balancing virtual server group.

newName

New name for the load balancing virtual server group.

Example

```
rename lb group gv1 gv-new1
```

[Top](#)

lb sipParameters

[[set](#) | [unset](#) | [show](#)]

set lb sipParameters

Synopsis

set lb sipParameters [-rnatSrcPort <port>] [-rnatDstPort <port>] [-retryDur <integer>] [-addRportVip (ENABLED | DISABLED)] [-sip503RateThreshold <positive_integer>]

Description

Modifies the specified global SIP parameters.

Parameters

rnatSrcPort

Port number with which to match the source port in server-initiated SIP traffic. The rport parameter is added, without a value, to SIP packets that have a matching source port number, and CALL-ID based persistence is implemented for the responses received by the virtual server.

rnatDstPort

Port number with which to match the destination port in server-initiated SIP traffic. The rport parameter is added, without a value, to SIP packets that have a matching source port number, and CALL-ID based persistence is implemented for the responses received by the virtual server.

retryDur

Time, in seconds, for which a client must wait before initiating a connection after receiving a 503 Service Unavailable response from the SIP server. The time value is sent in the "Retry-After" header in the 503 response. Default value: 120 Minimum value: 1

addRportVip

Add the rport parameter to the VIA headers of SIP requests that virtual servers receive from clients or servers. Possible values: ENABLED, DISABLED Default value: ENABLED

sip503RateThreshold

Maximum number of 503 Service Unavailable responses to generate, once every 10 milliseconds, when a SIP virtual server becomes unavailable. Default value: 100

Example

```
set sip parameter
```

[Top](#)**unset lb sipParameters****Synopsis**

```
unset lb sipParameters [-rnatSrcPort] [-rnatDstPort] [-retryDur] [-addRportVip] [-sip503RateThreshold]
```

Description

Use this command to remove lb sipParameters settings. Refer to the set lb sipParameters command for meanings of the arguments.

[Top](#)**show lb sipParameters****Synopsis**

```
show lb sipParameters
```

Description

Displays the global SIP parameters.

Example

```
show sip parameter
```

[Top](#)

lb parameter

[[set](#) | [unset](#) | [show](#)]

set lb parameter

Synopsis

```
set lb parameter [-httpOnlyCookieFlag ( ENABLED | DISABLED )] [-consolidatedLConn  
( YES | NO )] [-usePortForHashLb ( YES | NO )] [-preferDirectRoute ( YES | NO )] [-  
startupRRFactor <positive_integer>] [-monitorSkipMaxClient ( ENABLED | DISABLED )] [-  
monitorConnectionClose ( RESET | FIN )] [-vServerSpecificMac ( ENABLED | DISABLED )]
```

Description

Modifies the specified global load balancing parameters.

Parameters

httpOnlyCookieFlag

Include the HttpOnly attribute in persistence cookies. The HttpOnly attribute limits the scope of a cookie to HTTP requests and helps mitigate the risk of cross-site scripting attacks. Possible values: ENABLED, DISABLED Default value: ENABLED

consolidatedLConn

To find the service with the fewest connections, the virtual server uses the consolidated connection statistics from all the packet engines. The NO setting allows consideration of only the number of connections on the packet engine that received the new connection. Possible values: YES, NO Default value: YES

usePortForHashLb

Include the port number of the service when creating a hash for hash based load balancing methods. With the NO setting, only the IP address of the service is considered when creating a hash. Possible values: YES, NO Default value: YES

preferDirectRoute

Perform route lookup for traffic received by the NetScaler appliance, and forward the traffic according to configured routes. Do not set this parameter if you want a wildcard virtual server to direct packets received by the appliance to an intermediary device, such as a firewall, even if their destination is directly connected to the appliance. Route lookup is performed after the packets have been processed and returned by the intermediary device. Possible values: YES, NO Default value: YES

startupRRFactor

Number of requests, per service, for which to apply the round robin load balancing method before switching to the configured load balancing method, thus allowing services to ramp up gradually to full load. Until the specified number of requests is distributed, the NetScaler appliance is said to be implementing the slow start mode (or startup round robin). Implemented for a virtual server when one of the following is true: * The virtual server is newly created. * One or more services are newly bound to the virtual server. * One or more services bound to the virtual server are enabled. * The load balancing method is changed. This parameter applies to all the load balancing virtual servers configured on the NetScaler appliance, except for those virtual servers for which the virtual server-level slow start parameters (New Service

Startup Request Rate and Increment Interval) are configured. If the global slow start parameter and the slow start parameters for a given virtual server are not set, the appliance implements a default slow start for the virtual server, as follows: * For a newly configured virtual server, the appliance implements slow start for the first 100 requests received by the virtual server. * For an existing virtual server, if one or more services are newly bound or newly enabled, or if the load balancing method is changed, the appliance dynamically computes the number of requests for which to implement startup round robin. It obtains this number by multiplying the request rate by the number of bound services (it includes services that are marked as DOWN). For example, if the current request rate is 20 requests/s and ten services are bound to the virtual server, the appliance performs startup round robin for 200 requests. Not applicable to a virtual server for which a hash based load balancing method is configured.

monitorSkipMaxClient

When a monitor initiates a connection to a service, do not check to determine whether the number of connections to the service has reached the limit specified by the service's Max Clients setting. Enables monitoring to continue even if the service has reached its connection limit. Possible values: ENABLED, DISABLED Default value: DISABLED

monitorConnectionClose

Close monitoring connections by sending the service a connection termination message with the specified bit set. Possible values: RESET, FIN Default value: FIN

vServerSpecificMac

Allow a MAC-mode virtual server to accept traffic returned by an intermediary device, such as a firewall, to which the traffic was previously forwarded by another MAC-mode virtual server. The second virtual server can then distribute that traffic across the destination server farm. Also useful when load balancing Branch Repeater appliances. Note: The second virtual server can also send the traffic to another set of intermediary devices, such as another set of firewalls. If necessary, you can configure multiple MAC-mode virtual servers to pass traffic successively through multiple sets of intermediary devices. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

```
set lb parameter -httponly (ENABLED|DISABLED)
```

[Top](#)

unset lb parameter

Synopsis

```
unset lb parameter [-httpOnlyCookieFlag] [-consolidatedLConn] [-usePortForHashLb] [-preferDirectRoute] [-startupRRFactor] [-monitorSkipMaxClient] [-monitorConnectionClose] [-vServerSpecificMac]
```

Description

Use this command to remove lb parameter settings. Refer to the set lb parameter command for meanings of the arguments.

[Top](#)

show lb parameter

Synopsis

show lb parameter

Description

Displays the global load balancing parameters.

Example

```
show lb parameter
```

[Top](#)

Networking Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [arp](#)
- ♦ [channel](#)
- ♦ [fis](#)
- ♦ [route](#)
- ♦ [vlan](#)
- ♦ [vriD](#)
- ♦ [vriD6](#)
- ♦ [route6](#)
- ♦ [nd6](#)
- ♦ [inat](#)
- ♦ [inatsession](#)
- ♦ [bridgegroup](#)
- ♦ [ipTunnel](#)
- ♦ [ip6Tunnel](#)
- ♦ [netbridge](#)

- ◆ [ipset](#)
- ◆ [linkset](#)
- ◆ [netProfile](#)
- ◆ [arpparam](#)
- ◆ [ci](#)
- ◆ [interface](#)
- ◆ [rnat](#)
- ◆ [bridgetable](#)
- ◆ [bridge](#)
- ◆ [lacp](#)
- ◆ [rnatparam](#)
- ◆ [rnatip](#)
- ◆ [vrIDParam](#)
- ◆ [nd6RAvariables](#)
- ◆ [onLinkIPv6Prefix](#)
- ◆ [ipv6](#)
- ◆ [ipTunnelParam](#)
- ◆ [ip6TunnelParam](#)
- ◆ [L2Param](#)
- ◆ [L3Param](#)
- ◆ [forwardingSession](#)
- ◆ [ptp](#)
- ◆ [rnat6](#)
- ◆ [inatparam](#)
- ◆ [nat64](#)
- ◆ [rsskeytype](#)
- ◆ [tunnelip](#)
- ◆ [tunnelip6](#)
- ◆ [L4Param](#)
- ◆ [vpath](#)
- ◆ [vPathParam](#)

arp

[[add](#) | [rm](#) | [send](#) | [show](#)]

add arp

Synopsis

```
add arp -IPAddress <ip_addr> [-td <positive_integer>] -mac <mac_addr> -ifnum  
<interface_name> [-ownerNode <positive_integer>]
```

Description

Adds a static ARP entry to the ARP table of the NetScaler appliance.

Parameters

IPAddress

IP address of the network device that you want to add to the ARP table.

td

Traffic Domain Id. Maximum value: 4094

mac

MAC address of the network device.

ifnum

Interface through which the network device is accessible. Specify the interface in (slot/port) notation. For example, 1/3.

ownerNode

The owner node for the Arp entry. Default value: VAL_NOT_SET Maximum value: 31

Example

```
add arp -ip 10.100.0.48 -mac 00:a0:cc:5f:76:3a -  
ifnum 1/1
```

[Top](#)

rm arp

Synopsis

```
rm arp (<IPAddress> | -all) [-td <positive_integer>] [-ownerNode <positive_integer>]
```

Description

Removes a specified static ARP entry or all static ARP entries from the NetScaler appliance's ARP table.

Parameters

IPAddress

IP address of the network device in the ARP entry that you want to remove from the ARP table.

td

Traffic Domain Id. Maximum value: 4094

all

Remove all ARP entries from the ARP table of the NetScaler appliance.

ownerNode

The owner node for the Arp entry. Default value: VAL_NOT_SET Maximum value: 31

[Top](#)

send arp**Synopsis**

```
send arp ((-IPAddress <ip_addr> [-td <positive_integer>]) | -all)
```

Description

Sends Gratuitous Address Resolution Protocol (GARP) messages for the specified NetScaler owned IP addresses.

Parameters**IPAddress**

NetScaler owned IP address for which the NetScaler appliance sends Gratuitous Address Resolution Protocol (GARP) messages.

all

Send GARP messages for all NetScaler owned IP addresses on which the ARP option is enabled. In a secondary node of an high availability configuration, this option sends GARP messages for the node's NSIP address only.

Example

```
send arp 10.10.10.10
```

[Top](#)

show arp**Synopsis**

```
show arp [<IPAddress> [-td <positive_integer>] [-ownerNode <positive_integer>]]
```

Description

Display all the entries in the system's ARP table.

Parameters**IPAddress**

The IP address corresponding to an ARP entry.

ownerNode

The cluster node which owns the ARP entry. Default value: VAL_NOT_SET Maximum value: 31

Example

The output of the `sh arp` command is as follows:
5 configured arps:

	IP	MAC	Inface
TD	VLAN	Origin	TTL
	-----	-----	-----
1)	10.250.11.1	00:04:76:dc:f1:b9	1/2
2	2	dynamic	700
2)	10.11.0.254	00:30:19:c1:7e:f4	1/1
3	1	dynamic	500
3)	10.11.0.41	00:d0:a8:00:7c:e4	0/1
4	1	dynamic	500
4)	10.11.222.2	00:ee:ff:22:00:01	0/1
5	1	dynamic	500
5)	10.11.201.12	00:30:48:31:23:49	0/1
6	1	dynamic	500

[Top](#)

channel

[[add](#) | [rm](#) | [set](#) | [unset](#) | [bind](#) | [unbind](#) | [show](#)]

add channel

Synopsis

```
add channel <id> [-ifnum <interface_name> ...] [-state ( ENABLED | DISABLED )] [-lmac <mac_addr>] [-speed <speed>] [-flowControl <flowControl>] [-haMonitor ( ON | OFF )] [-tagall ( ON | OFF )] [-ifAlias <string>] [-throughput <positive_integer>] [-bandwidthHigh <positive_integer> [-bandwidthNormal <positive_integer>]]
```

Description

Creates a link aggregate channel on the NetScaler appliance or on a cluster configuration. Link aggregation combines data coming from multiple ports into a single high-speed link. Configuring link aggregation increases the capacity and availability of the communication channel between the NetScaler appliance and other connected devices. When a network interface is bound to a channel, the channel parameters have precedence over the network interface parameters. That is, the network interface parameters are ignored. A network interface can be bound only to one channel.

Parameters

id

ID for the LA channel or cluster LA channel to be created. Specify an LA channel in LA/x notation or cluster LA channel in CLA/x notation, where x can range from 1 to 4. Cannot be changed after the LA channel is created.

ifnum

Interfaces to be bound to the LA channel of a NetScaler appliance or to the LA channel of a cluster configuration. For an LA channel of a NetScaler appliance, specify an interface in C/U notation (for example, 1/3). For an LA channel of a cluster configuration, specify an interface in N/C/U notation (for example, 2/1/3), where C can take one of the following values: * 0 - Indicates a management interface. * 1 - Indicates a 1 Gbps port. * 10 - Indicates a 10 Gbps port. U is a unique integer for representing an interface in a particular port group. N is the ID of the node to which an interface belongs in a cluster configuration. Use spaces to separate multiple entries.

state

Enable or disable the LA channel. Possible values: ENABLED, DISABLED Default value: NSA_DVC_ENABLE

Mode

The initial mode for the LA channel. Possible values: MANUAL, AUTO

connDistr

The 'connection' distribution mode for the LA channel. Possible values: DISABLED, ENABLED

macdistr

The 'MAC' distribution mode for the LA channel. Possible values: SOURCE, DESTINATION, BOTH

lamac

MAC address for LA channels on VPX Platforms namely VPX on SDX,Xen,ESX.

speed

Ethernet speed of the channel, in Mbps. If the speed of any bound interface is greater than or equal to the value set for this parameter, the state of the interface is UP. Otherwise, the state is INACTIVE. Bound Interfaces whose state is INACTIVE do not process any traffic. Possible values: AUTO, 10, 100, 1000, 10000 Default value: NSA_DVC_SPEED_AUTO

flowControl

Flow control for the LA channel. Possible values: OFF, RX, TX, RXTX Default value: NSA_DVC_FC_OFF

haMonitor

In a High Availability (HA) configuration, monitor the LA channel for failure events. Failure of any LA channel that has HA MON enabled triggers HA failover. Possible values: ON, OFF Default value: NSA_DVC_MONITOR_ON

tagall

Adds a four-byte 802.1q tag to every packet sent on this channel. The ON setting applies tags for all VLANs that are bound to this channel. OFF applies the tag for all

VLANs other than the native VLAN. Possible values: ON, OFF Default value: NSA_DVC_VTRUNK_OFF

trunk

This is deprecated by tagall Possible values: ON, OFF Default value: OFF

ifAlias

Alias name for the LA channel. Used only to enhance readability. To perform any operations, you have to specify the LA channel ID. Default value: " "

throughput

Low threshold value for the throughput of the LA channel, in Mbps. In an HA configuration, failover is triggered if the LA channel has HA MON enabled and the throughput is below the specified threshold. Maximum value: 80000

bandwidthHigh

High threshold value for the bandwidth usage of the LA channel, in Mbps. The NetScaler appliance generates an SNMP trap message when the bandwidth usage of the LA channel is greater than or equal to the specified high threshold value. Maximum value: 80000

[Top](#)

rm channel

Synopsis

rm channel <id>

Description

Removes an LA channel from the NetScaler appliance or a cluster LA channel from a cluster configuration. Important: When a LA channel is removed, the network interfaces bound to it induce network loops that decrease network performance. You must disable the network interfaces before you remove the channel.

Parameters

id

ID of the LA channel or cluster LA channel that you want to remove. Specify an LA channel in LA/x notation or a cluster LA channel in CLA/x notation, where x can range from 1 to 4.

[Top](#)

set channel

Synopsis

set channel <id> [-state (ENABLED | DISABLED)] [-lamac <mac_addr>] [-speed <speed>] [-flowControl <flowControl>] [-haMonitor (ON | OFF)] [-tagall (ON | OFF)] [-ifAlias <string>] [-throughput <positive_integer>] [-lrMinThroughput <positive_integer>] [-bandwidthHigh <positive_integer>] [-bandwidthNormal <positive_integer>]]

Description

Modifies the specified parameters of an LA channel.

Parameters

id

ID of the LA channel or the cluster LA channel whose parameters you want to modify. Specify an LA channel in LA/x notation or a cluster LA channel in CLA/x notation, where x can range from 1 to 4. Required for identifying the LA channel and cannot be modified.

state

Enable or disable the LA channel. Possible values: ENABLED, DISABLED Default value: NSA_DVC_ENABLE

Mode

The mode for the LA channel. Possible values: MANUAL, AUTO

connDistr

The 'connection' distribution mode for the LA channel. Possible values: DISABLED, ENABLED

macdistr

The 'MAC' distribution mode for the LA channel. Possible values: SOURCE, DESTINATION, BOTH

lamac

Allows User to set MAC address for LA channels on Hypervised platforms.

speed

The speed for the LA channel. Possible values: AUTO, 10, 100, 1000, 10000 Default value: NSA_DVC_SPEED_AUTO

flowControl

Required flow control for the LA channel. Possible values: OFF, RX, TX, RXTX Default value: NSA_DVC_FC_OFF

haMonitor

The state of HA monitoring for the LA channel. Possible values: ON, OFF Default value: NSA_DVC_MONITOR_ON

tagall

The appliance adds a four-byte 802.1q tag to every packet sent on this channel. ON applies tags for all the VLANs that are bound to this channel. OFF, applies the tag for all VLANs other than the native VLAN. Possible values: ON, OFF Default value: NSA_DVC_VTRUNK_OFF

trunk

This is deprecated by tagall. Possible values: ON, OFF Default value: OFF

ifAlias

The alias name for the interface. Default value: " "

throughput

Low threshold value for the throughput of the LA channel, in Mbps. In an HA configuration, failover is triggered if the LA channel has HA MON enabled and the throughput is below the specified threshold. Maximum value: 80000

lrMinThroughput

Minimum required throughput for a channel where we require Link Redundancy. When throughput falls below the threshold, the subset of interfaces which can give maximum throughput will become active. When configured in HA pair, this will work along with the throughput parameter set. If lrMinThroughput can be achieved Link Failover will be attempted before Node Failover. Maximum value: 80000

bandwidthHigh

High threshold value for the bandwidth usage of the LA channel, in Mbps. The NetScaler appliance generates an SNMP trap message when the bandwidth usage of the LA channel is greater than or equal to the specified high threshold value. Maximum value: 80000

[Top](#)

unset channel**Synopsis**

```
unset channel <id> [-state] [-speed] [-flowControl] [-haMonitor] [-tagall] [-ifAlias] [-throughput] [-lrMinThroughput] [-bandwidthHigh] [-bandwidthNormal]
```

Description

Use this command to remove channel settings. Refer to the set channel command for meanings of the arguments.

[Top](#)

bind channel**Synopsis**

```
bind channel <id> <ifnum> ...
```

Description

Binds the specified interfaces to a channel.

Parameters**id**

ID of the LA channel or the cluster LA channel to which you want to bind interfaces. Specify an LA channel in LA/x notation or a cluster LA channel in CLA/x notation, where x can range from 1 to 4.

ifnum

Interfaces to be bound to the LA channel of a NetScaler appliance or to the LA channel of a cluster configuration. For an LA channel of a NetScaler appliance, specify an interface in C/U notation (for example, 1/3). For an LA channel of a cluster configuration, specify an interface in N/C/U notation (for example, 2/1/3), where C can take one of the following values: * 0 - Indicates a management

interface. * 1 - Indicates a 1 Gbps port. * 10 - Indicates a 10 Gbps port. U is a unique integer for representing an interface in a particular port group. N is the ID of the node to which an interface belongs in a cluster configuration. Use spaces to separate multiple entries.

[Top](#)

unbind channel

Synopsis

```
unbind channel <id> <ifnum> ...
```

Description

Unbinds the specified interfaces from an LA channel.

Parameters

id

ID of the LA channel or cluster LA channel from which you want to unbind interfaces. Specify an LA channel in LA/x notation or a cluster LA channel in CLA/x notation, where x can range from 1 to 4.

ifnum

Interfaces to be unbound from the LA channel of a NetScaler appliance or from the LA channel of a cluster configuration. For an LA channel of a NetScaler appliance, specify an interface in C/U notation (for example, 1/3). For an LA channel of a cluster configuration, specify an interface in N/C/U notation (for example, 2/1/3), where C can take one of the following values: * 0 - Indicates a management interface. * 1 - Indicates a 1 Gbps port. * 10 - Indicates a 10 Gbps port. U is a unique integer for representing an interface in a particular port group. N is the ID of the node to which an interface belongs in a cluster configuration. Use spaces to separate multiple entries.

[Top](#)

show channel

Synopsis

```
show channel [<id>]
```

Description

Displays the settings of all LA channels or of the specified channel. To display the settings of all channels, run the command without any parameters. To display the settings of a particular channel, specify the ID of the channel.

Parameters

id

ID of an LA channel or LA channel in cluster configuration whose details you want the NetScaler appliance to display. Specify an LA channel in LA/x notation or a cluster LA channel in CLA/x notation, where x can range from 1 to 4. Minimum value: 1

[Top](#)

fis

[[add](#) | [rm](#) | [bind](#) | [unbind](#) | [show](#)]

add fis

Synopsis

add fis <name>

Description

Adds a failover interface set (FIS) to the NetScaler appliance. A FIS is a logical group of interfaces. In an HA configuration, using a FIS is a way to prevent failover by grouping interfaces so that, when one interface fails, other functioning interfaces are still available.

Parameters

name

Name for the FIS to be created. Leading character must be a number or letter. Other characters allowed, after the first character, are @ _ - . (period) : (colon) # and space ().

[Top](#)

rm fis

Synopsis

rm fis <name>

Description

Removes an FIS from the NetScaler appliance. When an FIS is removed, its interfaces are marked as critical interfaces.

Parameters

name

Name of the FIS that you want to remove from the NetScaler appliance.

[Top](#)

bind fis

Synopsis

bind fis <name> <ifnum> ...

Description

Binds the specified interfaces to a FIS.

Parameters

name

The name of the FIS to which you want to bind interfaces.

ifnum

Interface to be bound to the FIS, specified in slot/port notation (for example, 1/3).

[Top](#)**unbind fis****Synopsis**

unbind fis <name> <ifnum> ...

Description

Unbinds the specified interfaces from a FIS. An unbound interface becomes a critical interface if it is enabled and HA MON is on.

Parameters**name**

Name of the FIS from which to unbind interfaces.

ifnum

Interfaces to unbind from the FIS, specified in slot/port notation (for example, 1/3).
Use spaces to separate multiple entries.

[Top](#)**show fis****Synopsis**

show fis [<name>]

Description

Displays the configured FISs.

Parameters**name**

The name of the FIS configured on the appliance.

Example

```
>show fis
1)      FIS: fis1
        Member Interfaces : 1/1

Done
```

[Top](#)**route**

[[add](#) | [clear](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add route

Synopsis

```
add route <network> <netmask> <gateway> [-td <positive_integer>] [-distance  
<positive_integer>] [-cost <positive_integer>] [-weight <positive_integer>] [-advertise  
( DISABLED | ENABLED )] [-protocol <protocol> ...] [-msr ( ENABLED | DISABLED ) [-  
monitor <string>]]
```

Description

Adds an IPv4 static route to the routing table of the NetScaler appliance.

Parameters

network

IPv4 network address for which to add a route entry in the routing table of the NetScaler appliance.

netmask

The subnet mask associated with the network address.

gateway

IP address of the gateway for this route. Can be either the IP address of the gateway, or can be null to specify a null interface route.

cost

Positive integer used by the routing algorithms to determine preference for using this route. The lower the cost, the higher the preference. Maximum value: 65535

td

Traffic Domain Id. Maximum value: 4094

distance

Administrative distance of this route, which determines the preference of this route over other routes, with same destination, from different routing protocols. A lower value is preferred. Default value: STATIC_ROUTE_DEFAULT_DISTANCE Maximum value: 255

weight

Positive integer used by the routing algorithms to determine preference for this route over others of equal cost. The lower the weight, the higher the preference. Default value: ROUTE_DEFAULT_WEIGHT Minimum value: 1 Maximum value: 65535

advertise

Advertise this route. Possible values: DISABLED, ENABLED

protocol

Routing protocol used for advertising this route. Default value: ADV_ROUTE_FLAGS

msr

Monitor this route using a monitor of type ARP or PING. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

```
add route 10.10.10.0 255.255.255.0 10.10.10.1
```

[Top](#)**clear route****Synopsis**

clear route <routeType>

Description

Removes routes of the specified type(protocol) from the routing table of the NetScaler appliance.

Parameters**routeType**

Protocol used by routes that you want to remove from the routing table of the NetScaler appliance.

[Top](#)**rm route****Synopsis**

rm route <network> <netmask> <gateway> [-td <positive_integer>]

Description

Removes a static route from the NetScaler appliance. Note: You cannot use this command to remove routes that are part of a VLAN configuration. Use the rmvlan or clear vlan command instead.

Parameters**network**

Network address specified in the route entry that you want to remove from the routing table of the NetScaler appliance.

netmask

Subnet mask associated with the network address.

gateway

IP address of the gateway for this route.

td

The Traffic Domain Id of the route to be removed. Maximum value: 4094

[Top](#)

set route

Synopsis

```
set route <network> <netmask> <gateway> [-td <positive_integer>] [-distance  
<positive_integer>] [-cost <positive_integer>] [-weight <positive_integer>] [-advertise  
( DISABLED | ENABLED )] [-protocol <protocol> ...] [-msr ( ENABLED | DISABLED ) [-  
monitor <string>]]
```

Description

Modifies parameters of an IPv4 static route.

Parameters

network

Network address in the route entry that you want to modify.

netmask

Subnet mask associated with the network address.

gateway

IP address of the gateway for this route. Can be either the IP address of the gateway, or can be null to specify a null interface route.

td

Traffic Domain Id. Maximum value: 4094

distance

Administrative distance of this route, which determines the preference of this route over other routes, with same destination, from different routing protocols. A lower value is preferred. Default value: STATIC_ROUTE_DEFAULT_DISTANCE Maximum value: 255

cost

The cost of a route is used to compare routes of the same type. The route having the lowest cost is the most preferred route. Possible values: 0 through 65535. Default: 0. Maximum value: 65535

weight

Positive integer used by the routing algorithms to determine preference for this route over others of equal cost. The lower the weight, the higher the preference. Default value: ROUTE_DEFAULT_WEIGHT Minimum value: 1 Maximum value: 65535

advertise

Advertise this route. Possible values: DISABLED, ENABLED

protocol

Routing protocol used for advertising this route. Default value: ADV_ROUTE_FLAGS

msr

Monitor this route using a monitor of type ARP or PING. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

```
set route 10.10.10.0 255.255.255.0 10.10.10.1 -  
advertise enable
```

[Top](#)**unset route****Synopsis**

```
unset route <network> <netmask> <gateway> [-td <positive_integer>] [-advertise] [-  
distance] [-cost] [-weight] [-protocol] [-msr] [-monitor]
```

Description

Unset the attributes of a route that were added by the add/set route command..Refer to the set route command for meanings of the arguments.

Example

```
unset route 10.10.10.0 255.255.255.0 10.10.10.1 -  
advertise enable
```

[Top](#)**show route****Synopsis**

```
show route [<network> <netmask> [<gateway>] [-td <positive_integer>]] [<routeType>]  
[-detail]
```

Description

Display the configured routing information.

Parameters**network**

The destination network or host.

routeType

The type of routes to be shown.

detail

Display a detailed view.

Example

```
An example of the output of the show route command  
is as follows:
```

```
3 configured routes:
```

	Network OwnedIP	Type	Netmask	Gateway/
	-----		-----	
1)	0.0.0.0		0.0.0.0	
	10.11.0.254		STATIC	
2)	127.0.0.0		255.0.0.0	
	127.0.0.1		PERMANENT	
3)	10.251.0.0		255.255.0.0	
	10.251.0.254		NAT	

[Top](#)

vlan

[[add](#) | [rm](#) | [set](#) | [unset](#) | [bind](#) | [unbind](#) | [show](#) | [stat](#)]

add vlan

Synopsis

```
add vlan <id> [-aliasName <string>] [-ipv6DynamicRouting ( ENABLED | DISABLED )]
```

Description

Adds a VLAN to the NetScaler appliance. The new VLAN is not active unless interfaces are bound to it.

Parameters

id

ID of the VLAN whose parameters you want to modify. Minimum value: 1 Maximum value: 4094

aliasName

A name for the VLAN. Must begin with a letter, a number, or the underscore symbol, and can consist of from 1 to 31 letters, numbers, and the hyphen (-), period (.) pound (#), space (), at sign (@), equals (=), colon (:), and underscore (_) characters. You should choose a name that helps identify the VLAN. However, you cannot perform any VLAN operation by specifying this name instead of the VLAN ID.

ipv6DynamicRouting

Enable all IPv6 dynamic routing protocols on this VLAN. Note: For the ENABLED setting to work, you must configure IPv6 dynamic routing protocols from the VTYSH command line. Possible values: ENABLED, DISABLED Default value: DISABLED

[Top](#)

rm vlan

Synopsis

```
rm vlan <id>
```

Description

Removes a VLAN from the NetScaler appliance. When the VLAN is removed, its interfaces are bound to VLAN 1. Note: VLAN 1 cannot be removed by any command.

Parameters

id

Integer that uniquely identifies the VLAN to be removed from the NetScaler appliance. When the VLAN is removed, its interfaces become members of VLAN 1. Minimum value: 2 Maximum value: 4094

[Top](#)

set vlan

Synopsis

```
set vlan <id> [-aliasName <string>] [-ipv6DynamicRouting ( ENABLED | DISABLED )]
```

Description

Modifies parameters of a VLAN on the NetScaler appliance.

Parameters

id

ID of the VLAN whose parameters you want to modify. Minimum value: 1 Maximum value: 4094

aliasName

A name for the VLAN. Must begin with a letter, a number, or the underscore symbol, and can consist of from 1 to 31 letters, numbers, and the hyphen (-), period (.) pound (#), space (), at sign (@), equals (=), colon (:), and underscore (_) characters. You should choose a name that helps identify the VLAN. However, you cannot perform any VLAN operation by specifying this name instead of the VLAN ID.

ipv6DynamicRouting

Enable all IPv6 dynamic routing protocols on this bridge group. Note: For the ENABLED setting to work, you must configure IPv6 dynamic routing protocols from the VTYSH command line. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

```
set vlan 2 -dynamicRouting ENABLED
```

[Top](#)

unset vlan

Synopsis

```
unset vlan <id> [-aliasName] [-ipv6DynamicRouting]
```

Description

Use this command to remove vlan settings. Refer to the set vlan command for meanings of the arguments.

[Top](#)

bind vlan

Synopsis

```
bind vlan <id> [-ifnum <interface_name> ... [-tagged]] [-IPAddress <ip_addr|ipv6_addr|
*> [<netmask>] [-td <positive_integer>]]
```

Description

Binds the specified interfaces or IP addresses to a VLAN. An interface can be bound to a VLAN as a tagged or an untagged member. Adding an interface as an untagged member removes it from its current native VLAN and adds it to the new VLAN. If an interface is added as a tagged member to a VLAN, it still remains a member of its native VLAN.

Parameters

id

Specifies the virtual LAN ID. Minimum value: 1 Maximum value: 4094

ifnum

Interface to be bound to the VLAN, specified in slot/port notation (for example, 1/3). Minimum value: 1

IPAddress

Network address to be associated with the VLAN. Should exist on the appliance before you associate it with the VLAN. To enable IP forwarding among VLANs, the specified address can be used as the default gateway by the hosts in the network.

[Top](#)

unbind vlan

Synopsis

```
unbind vlan <id> [-ifnum <interface_name> ... [-tagged]] [-IPAddress <ip_addr|
ipv6_addr|*> [<netmask>] [-td <positive_integer>]]
```

Description

Unbinds the specified interfaces or IP addresses from a VLAN. If any of the interfaces are untagged members of the VLAN, they are automatically bound to VLAN 1.

Parameters

id

The virtual LAN (VLAN) id. Minimum value: 1 Maximum value: 4094

ifnum

Interface to unbind from the VLAN, specified in slot/port notation (for example, 1/3). Minimum value: 1

IPAddress

The IP Address associated with the VLAN configuration.

[Top](#)

show vlan**Synopsis**

show vlan [*<id>*] show vlan stats - alias for 'stat vlan'

Description

Displays the settings of all VLANs configured on the NetScaler appliance, or of the specified VLAN. To display the settings of all the VLANs, run the command without any parameters. To display the settings of a particular VLAN, specify the ID of the VLAN.

Parameters**id**

Integer that uniquely identifies the VLAN for which the details are to be displayed.
Minimum value: 1 Maximum value: 4094

Example

An example of the output of the show vlan command is as follows:

```
1)      VLAN ID: 5      VLAN Alias Name:
        Interfaces : 1/7
        IPs :
        10.102.169.36      Mask: 255.255.255.0

2)      VLAN ID: 3      VLAN Alias Name:
        Interfaces : 1/5(T)
        Channels : LA/2

Done

* (T) - Tagged
```

[Top](#)

stat vlan**Synopsis**

stat vlan [*<id>*] [-detail] [-fullValues] [-ntimes *<positive_integer>*] [-logFile *<input_filename>*] [-clearstats (basic | full)]

Description

Display statistics for VLAN(s).

Parameters

id

An integer specifying the VLAN identification number (VID). Possible values: 1 through 4094. Minimum value: 1 Maximum value: 4094

clearstats

Clear the statistics / counters Possible values: basic, full

Example

```
stat vlan 1
```

[Top](#)

vrID

[[add](#) | [rm](#) | [set](#) | [unset](#) | [bind](#) | [unbind](#) | [show](#)]

add vrID

Synopsis

add vrID <id> [-priority <positive_integer>] [-preemption (ENABLED | DISABLED)] [-sharing (ENABLED | DISABLED)] [-tracking <tracking>]

Description

Adds a VMAC address to the NetScaler appliance. A Virtual MAC address (VMAC) is a floating entity, shared by the nodes in an HA configuration.

Parameters

id

Integer that uniquely identifies the VMAC address. The generic VMAC address is in the form of 00:00:5e:00:01:<VRID>. For example, if you add a VRID with a value of 60 and bind it to an interface, the resulting VMAC address is 00:00:5e:00:01:3c, where 3c is the hexadecimal representation of 60. Minimum value: 1 Maximum value: 255

priority

Base priority (BP), in an active-active mode configuration, which ordinarily determines the master VIP address. Default value: 255 Minimum value: 1 Maximum value: 255

preemption

In an active-active mode configuration, make a backup VIP address the master if its priority becomes higher than that of a master VIP address bound to this VMAC address. If you disable pre-emption while a backup VIP address is the master, the backup VIP address remains master until the original master VIP's priority becomes higher than that of the current master. Possible values: ENABLED, DISABLED Default value: ENABLED

sharing

In an active-active mode configuration, enable the backup VIP address to process any traffic instead of dropping it. Possible values: ENABLED, DISABLED Default value: DISABLED

tracking

The effective priority (EP) value, relative to the base priority (BP) value in an active-active mode configuration. When EP is set to a value other than None, it is EP, not BP, which determines the master VIP address. Available settings function as follows: * NONE - No tracking. EP = BP * ALL - If the status of all virtual servers is UP, EP = BP. Otherwise, EP = 0. * ONE - If the status of at least one virtual server is UP, EP = BP. Otherwise, EP = 0. * PROGRESSIVE - If the status of all virtual servers is UP, EP = BP. If the status of all virtual servers is DOWN, EP = 0. Otherwise EP = BP (1 - K/N), where N is the total number of virtual servers associated with the VIP address and K is the number of virtual servers for which the status is DOWN. Default: NONE. Possible values: NONE, ONE, ALL, PROGRESSIVE Default value: TRACK_NONE

Example

```
add vrID 1
```

[Top](#)

rm vrID**Synopsis**

```
rm vrID (<id> | -all)
```

Description

Removes a specified VMAC entry or all VMAC entries from the NetScaler appliance.

Parameters**id**

Integer value that uniquely identifies the VMAC address. Minimum value: 1 Maximum value: 255

all

Remove all the configured VMAC addresses from the NetScaler appliance.

[Top](#)

set vrID**Synopsis**

```
set vrID <id> [-priority <positive_integer>] [-preemption ( ENABLED | DISABLED )] [-sharing ( ENABLED | DISABLED )] [-tracking <tracking>]
```

Description

Modifies parameters related to a VMAC address on the NetScaler appliance.

Parameters

id

Integer value that uniquely identifies the VMAC address. The generic VMAC address is in the form of 00:00:5e:00:01:<VRID>. For example, if you add a VRID with a value of 60 and bind it to an interface, the resulting VMAC address is 00:00:5e:00:01:3c, where 3c is the hexadecimal representation of 60. Minimum value: 1 Maximum value: 255

priority

Base priority (BP), in an active-active mode configuration, which ordinarily determines the master VIP address. Default value: 255 Minimum value: 1 Maximum value: 255

preemption

In an active-active mode configuration, make a backup VIP address the master if its priority becomes higher than that of a master VIP address bound to this VMAC address. If you disable pre-emption while a backup VIP address is the master, the backup VIP address remains master until the original master VIP's priority becomes higher than that of the current master. Possible values: ENABLED, DISABLED Default value: ENABLED

sharing

In an active-active mode configuration, enable the backup VIP address to process any traffic instead of dropping it. Possible values: ENABLED, DISABLED Default value: DISABLED

tracking

The effective priority (EP) value, relative to the base priority (BP) value in an active-active mode configuration. When EP is set to a value other than None, it is EP, not BP, which determines the master VIP address. Available settings function as follows: * NONE - No tracking. EP = BP * ALL - If the status of all virtual servers is UP, EP = BP. Otherwise, EP = 0. * ONE - If the status of at least one virtual server is UP, EP = BP. Otherwise, EP = 0. * PROGRESSIVE - If the status of all virtual servers is UP, EP = BP. If the status of all virtual servers is DOWN, EP = 0. Otherwise EP = BP (1 - K/N), where N is the total number of virtual servers associated with the VIP address and K is the number of virtual servers for which the status is DOWN. Default: NONE. Possible values: NONE, ONE, ALL, PROGRESSIVE Default value: TRACK_NONE

Example

```
set vrID 1 -priority 100
```

[Top](#)

unset vrID

Synopsis

```
unset vrID <id> [-priority] [-preemption] [-sharing] [-tracking]
```

Description

Use this command to remove vrID settings. Refer to the set vrID command for meanings of the arguments.

[Top](#)

bind vrID

Synopsis

```
bind vrID <id> -ifnum <interface_name> ...
```

Description

Binds the specified interfaces to a VMAC configuration.

Parameters

id

Integer that uniquely identifies the VMAC address. The generic VMAC address is in the form of 00:00:5e:00:01:<VRID>. For example, if you add a VRID with a value of 60 and bind it to an interface, the resulting VMAC address is 00:00:5e:00:01:3c, where 3c is the hexadecimal representation of 60. Minimum value: 1 Maximum value: 255

ifnum

Interfaces to bind to the VMAC, specified in (slot/port) notation (for example, 1/2). Use spaces to separate multiple entries.

Example

```
add vrID 1
```

[Top](#)

unbind vrID

Synopsis

```
unbind vrID <id> -ifnum <interface_name> ...
```

Description

Unbinds specified interfaces from a VMAC configuration.

Parameters

id

Integer value that uniquely identifies the VMAC address. The generic VMAC address is in the form of 00:00:5e:00:01:<VRID>. For example, if you add a VRID with a value of 60 and bind it to an interface, the resulting VMAC address is 00:00:5e:00:01:3c, where 3c is the hexadecimal representation of 60. Minimum value: 1 Maximum value: 255

ifnum

Interfaces to unbind from the VMAC, specified in (slot/port) notation (for example, 1/2). Use spaces to separate multiple entries.

[Top](#)

show vrid

Synopsis

show vrid [<id>]

Description

Displays the settings of all VRIDs configured on the NetScaler appliance, or of the specified VRID. To display the settings of all the VRIDs, run the command without any parameters. To display the settings of a particular VRID, specify the VRID.

Parameters

id

Integer value that uniquely identifies the VMAC address. Minimum value: 1 Maximum value: 255

Example

```
show vrid
```

[Top](#)

vrid6

[[add](#) | [rm](#) | [bind](#) | [unbind](#) | [show](#)]

add vrid6

Synopsis

add vrid6 <id>

Description

Adds a VMAC6 address to the NetScaler appliance. A Virtual MAC address (VMAC6) is a floating entity, shared by the nodes in an HA configuration.

Parameters

id

Integer value that uniquely identifies a VMAC6 address. Minimum value: 1 Maximum value: 255

Example

```
add vrID6 1
```

[Top](#)**rm vrID6****Synopsis**

```
rm vrID6 (<id> | -all)
```

Description

Removes a specified VMAC6 entry or all VMAC6 entries from the NetScaler appliance.

Parameters**id**

Integer value that uniquely identifies a VMAC6 address. Minimum value: 1 Maximum value: 255

all

Remove all configured VMAC6 addresses from the NetScaler appliance.

[Top](#)**bind vrID6****Synopsis**

```
bind vrID6 <id> -ifnum <interface_name> ...
```

Description

Binds the specified interfaces to a VMAC6 configuration.

Parameters**id**

Integer value that uniquely identifies a VMAC6 address. Minimum value: 1 Maximum value: 255

ifnum

Interfaces to bind to the VMAC6, specified in (slot/port) notation (for example, 1/2). Use spaces to separate multiple entries.

Example

```
add vrID6 1
```

[Top](#)

unbind vrid6

Synopsis

unbind vrid6 <id> -ifnum <interface_name> ...

Description

Unbinds the specified interfaces from a VMAC6 configuration.

Parameters

id

Integer value that uniquely identifies a VMAC6 address. Minimum value: 1 Maximum value: 255

ifnum

Interfaces to unbind from the VMAC6, specified in (slot/port) notation (for example, 1/2). Use spaces to separate multiple entries.

[Top](#)

show vrid6

Synopsis

show vrid6 [<id>]

Description

Displays the settings of all VRID6s configured on the NetScaler appliance, or of the specified VRID6. To display the settings of all the VRID6s, run the command without any parameters. To display the settings of a particular VRID6, specify the VRID6.

Parameters

id

Integer value that uniquely identifies a VMAC6 address. Minimum value: 1 Maximum value: 255

Example

```
show vrid6
```

[Top](#)

route6

[[add](#) | [clear](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add route6

Synopsis

```
add route6 <network> [<gateway>] [-vlan <positive_integer>] [-weight  
<positive_integer>] [-distance <positive_integer>] [-cost <positive_integer>] [-advertise  
( DISABLED | ENABLED )] [-msr ( ENABLED | DISABLED )] [-monitor <string>]] [-td  
<positive_integer>]
```

Description

Adds an IPv6 static route to the routing table of the NetScaler appliance.

Parameters

network

IPv6 network address for which to add a route entry to the routing table of the NetScaler appliance.

gateway

The gateway for this route. The value for this parameter is either an IPv6 address or null.

vlan

Integer value that uniquely identifies a VLAN through which the NetScaler appliance forwards the packets for this route. Maximum value: 4094

weight

Positive integer used by the routing algorithms to determine preference for this route over others of equal cost. The lower the weight, the higher the preference. Default value: 1 Minimum value: 1 Maximum value: 65535

distance

Administrative distance of this route from the appliance. Default value: 1 Minimum value: 1 Maximum value: 254

cost

Positive integer used by the routing algorithms to determine preference for this route. The lower the cost, the higher the preference. Default value: 1 Maximum value: 65535

advertise

Advertise this route. Possible values: DISABLED, ENABLED

msr

Monitor this route with a monitor of type ND6 or PING. Possible values: ENABLED, DISABLED Default value: DISABLED

td

Traffic Domain Id for IPv6 network. Maximum value: 4094

Example

```
add route6 ::/0 2004::1 add route6 ::/0 FE80::67 -  
vlan 5
```

[Top](#)

clear route6

Synopsis

clear route6 <routeType>

Description

Removes IPv6 routes of the specified type (protocol) from the routing table of the NetScaler appliance.

Parameters

routeType

Type of IPv6 routes to remove from the routing table of the NetScaler appliance.

[Top](#)

rm route6

Synopsis

rm route6 <network> [<gateway>] [-vlan <positive_integer>] [-td <positive_integer>]

Description

Removes a static IPv6 route from the NetScaler appliance.

Parameters

network

The network of the route to be removed.

gateway

The gateway address of the route to be removed.

vlan

Integer that uniquely identifies the VLAN defined for this route. Maximum value: 4094

td

Traffic Domain Id for IPv6 network. Maximum value: 4094

Example

```
rm route6 ::/0 2004::1  
rm route6 ::/0 FE80::67 -vlan 5
```


[Top](#)

set route6

Synopsis

```
set route6 <network> [<gateway>] [-vlan <positive_integer>] [-weight  
<positive_integer>] [-distance <positive_integer>] [-cost <positive_integer>] [-advertise  
( DISABLED | ENABLED )] [-msr ( ENABLED | DISABLED )] [-monitor <string>]] [-td  
<positive_integer>]
```

Description

Modifies parameters of an IPv6 static route.

Parameters

network

IPv6 network address of the route entry to be modified.

gateway

The gateway for the route's destination network.

vlan

Integer value that uniquely identifies a VLAN through which the NetScaler appliance forwards the packets for this route. Maximum value: 4094

weight

Positive integer used by the routing algorithms to determine preference for this route over others of equal cost. The lower the weight, the higher the preference. Default value: 1 Minimum value: 1 Maximum value: 65535

distance

Administrative distance of this route from the appliance. Default value: 1 Minimum value: 1 Maximum value: 254

cost

Positive integer used by the routing algorithms to determine preference for this route. The lower the cost, the higher the preference. Default value: 1 Maximum value: 65535

advertise

Advertise this route. Possible values: DISABLED, ENABLED

msr

Monitor this route with a monitor of type ND6 or PING. Possible values: ENABLED, DISABLED Default value: DISABLED

td

Traffic Domain Id for IPv6 network. Maximum value: 4094

Example

```
set route6 1::1/100 2000::1 -advertise enable
```

[Top](#)

unset route6

Synopsis

```
unset route6 <network> [<gateway>] [-vlan <positive_integer>] [-td <positive_integer>]
[-weight] [-distance] [-cost] [-advertise] [-msr] [-monitor]
```

Description

Unset the attributes of a route that were added by the add/set route command..Refer to the set route6 command for meanings of the arguments.

Example

```
unset route6 2000::1/100 3000::1 -advertise enable
```

[Top](#)

show route6

Synopsis

```
show route6 [<network> [<gateway>] [-vlan <positive_integer>] [-td
<positive_integer>]] [<routeType>] [-detail]
```

Description

Displays configuration and state information of all IPv6 routes in the NetScaler appliance's routing table, or of the specified IPv6 route.

Parameters

network

IPv6 network address of the route entry for which to display details.

routeType

The type of IPv6 routes to be to be displayed.

detail

To get a detailed view.

Example

```
Following is an example of the output of the show
route6 command:
```

```
Flags: Static(S), Dynamic(D), Active(A)
-----
Network          Gateway(vlan)    Flags
-----          -
```

0::0/0	2001::1	S (A)
0::0/0	FE80::90 (4)	D (A)

[Top](#)

nd6

[[add](#) | [clear](#) | [rm](#) | [show](#)]

add nd6

Synopsis

add nd6 <neighbor> <mac> <ifnum> [-vlan <integer>] [-td <positive_integer>]

Description

Adds a static entry to the ND6 table of the NetScaler appliance.

Parameters

- neighbor**
Link-local IPv6 address of the adjacent network device to add to the ND6 table.
- mac**
MAC address of the adjacent network device.
- ifnum**
Interface through which the adjacent network device is available, specified in slot/port notation (for example, 1/3). Use spaces to separate multiple entries.
- vlan**
Integer value that uniquely identifies the VLAN on which the adjacent network device exists. Minimum value: 1 Maximum value: 4094
- td**
Traffic Domain Id. Maximum value: 4094

Example

```
add nd6 2001::1 00:04:23:be:3c:06 5 1/1
```

[Top](#)

clear nd6

Synopsis

clear nd6

Description

Removes all IPv6 neighbour discovery entries from the NetScaler appliance.

[Top](#)

rm nd6

Synopsis

```
rm nd6 <neighbor> [-vlan <integer>] [-td <positive_integer>]
```

Description

Remove a static IPv6 neighbor discovery entry from the NetScaler appliance's ND6 table.

Parameters

neighbor

Link-local IPv6 address of the adjacent network device that you want to remove from the ND6 table.

vlan

Integer value that uniquely identifies the VLAN for the ND6 entry you want to remove. Minimum value: 1 Maximum value: 4094

td

Traffic Domain Id. Maximum value: 4094

Example

```
rm nd6 2001::1 5 1/1
```

[Top](#)

show nd6

Synopsis

```
show nd6 [<neighbor> [-td <positive_integer>]]
```

Description

Display the neighbor discovery information.

Parameters

neighbor

Link-local IPv6 address of the adjacent network device to add to the ND6 table.

Example

Following is an example of the output for the show nd6 command:

Neighbor Interface)	MAC-Address (Vlan, State	TIME (hh:mm:ss)


```

2001::1          00:04:23:be:3c:06 (5,
1/1)            REACHABLE 00:00:24
FE80::123:1      00:04:23:be:3c:07 (4,
1/2)            STALE   00:03:34

```

[Top](#)

inat

[[add](#) | [rm](#) | [set](#) | [unset](#) | [stat](#) | [show](#)]

add inat

Synopsis

```

add inat <name>@ <publicIP>@ <privateIP>@ [-tcpproxy ( ENABLED | DISABLED )] [-ftp
( ENABLED | DISABLED )] [-tftp ( ENABLED | DISABLED )] [-usip ( ON | OFF )] [-usnip
( ON | OFF )] [-proxyIP <ip_addr|ipv6_addr>] [-mode STATELESS] [-td
<positive_integer>]

```

Description

Adds an INAT rule to the NetScaler appliance. When a packet generated by a client matches the conditions specified in the INAT rule, the appliance translates the packet's public destination IP address to a private destination IP address and forwards the packet to the server at that address.

Parameters

name

Name for the Inbound NAT (INAT) entry. Leading character must be a number or letter. Other characters allowed, after the first character, are @ _ . (period) : (colon) # and space ().

publicIP

Public IP address of packets received on the NetScaler appliance. Can be a NetScaler-owned VIP or VIP6 address.

privateIP

IP address of the server to which the packet is sent by the NetScaler. Can be an IPv4 or IPv6 address.

tcpproxy

Enable TCP proxy, which enables the NetScaler appliance to optimize the RNAT TCP traffic by using Layer 4 features. Possible values: ENABLED, DISABLED Default value: DISABLED

ftp

Enable the FTP protocol on the server for transferring files between the client and the server. Possible values: ENABLED, DISABLED Default value: DISABLED

tftp

To enable/disable TFTP (Default DISABLED). Possible values: ENABLED, DISABLED Default value: DISABLED

usip

Enable the NetScaler appliance to retain the source IP address of packets before sending the packets to the server. Possible values: ON, OFF Default value: OFF

usnip

Enable the NetScaler appliance to use a SNIP address as the source IP address of packets before sending the packets to the server. Possible values: ON, OFF Default value: ON

proxyIP

Unique IP address used as the source IP address in packets sent to the server. Must be a MIP or SNIP address.

mode

Stateless translation. Possible values: STATELESS

td

Traffic Domain Id. Maximum value: 4094

Example

```
add nat mynat 1.2.3.4 192.168.1.100
```

[Top](#)

rm inat

Synopsis

rm inat <name>@

Description

Remove the specified Inbound NAT configuration.

Parameters

name

Name of the Inbound NAT entry to be removed from the NetScaler appliance.

Example

```
rm nat mynat.
```

[Top](#)

set inat

Synopsis

set inat <name>@ [-privateIP <ip_addr|ipv6_addr>@] [-tcpproxy (ENABLED | DISABLED)] [-ftp (ENABLED | DISABLED)] [-tftp (ENABLED | DISABLED)] [-usip (ON | OFF)] [-usnip (ON | OFF)] [-proxyIP <ip_addr|ipv6_addr>] [-mode STATELESS]

Description

Modifies parameters of an INAT rule.

Parameters

name

The name of the Inbound NAT (INAT) entry that you want to modify.

privateIP

IP address of the server to which the packet is sent by the NetScaler. Can be an IPv4 or IPv6 address.

tcpproxy

Enable TCP proxy, which enables the NetScaler appliance to optimize the RNAT TCP traffic by using Layer 4 features. Possible values: ENABLED, DISABLED Default value: DISABLED

ftp

Enable the FTP protocol on the server for transferring files between the client and the server. Possible values: ENABLED, DISABLED Default value: DISABLED

tftp

To enable/disable TFTP (Default DISABLED). Possible values: ENABLED, DISABLED Default value: DISABLED

usip

Enable the NetScaler appliance to retain the source IP address of packets before sending the packets to the server. Possible values: ON, OFF Default value: OFF

usnip

Enable the NetScaler appliance to use a SNIP address as the source IP address of packets before sending the packets to the server. Possible values: ON, OFF Default value: ON

proxyIP

A unique IP address used as the source IP address in packets sent to the server. Must be a MIP or SNIP address.

mode

Stateless translation. Possible values: STATELESS

Example

```
set nat mynat -tcpproxy ENABLED
```

[Top](#)

unset inat

Synopsis

```
unset inat <name>@ [-tcpproxy] [-ftp] [-tftp] [-usip] [-usnip] [-proxyIP] [-mode]
```

Description

Use this command to remove inat settings. Refer to the set inat command for meanings of the arguments.

[Top](#)

stat inat

Synopsis

```
stat inat [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile  
<input_filename>] [-clearstats ( basic | full )]
```

Description

Display statistics for inat sessions.

Parameters

name

The INAT.

clearstats

Clear the statistics / counters Possible values: basic, full

Example

```
stat inat
```

[Top](#)

show inat

Synopsis

```
show inat [<name>]
```

Description

show all configured inbound NAT.

Parameters

name

Name for the Inbound NAT (INAT) entry. Leading character must be a number or letter. Other characters allowed, after the first character, are @ _ - . (period) : (colon) # and space ().

Example

```
show nat
```

[Top](#)

inatsession

stat inatsession

Synopsis

```
stat inatsession <name> [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile
<input_filename>] [-clearstats ( basic | full )]
```

Description

Display statistics for stateful inat sessions.

Parameters

name

INAT name

clearstats

Clear the statistics / counters Possible values: basic, full

Example

```
stat inatsession inat_1
```

bridgegroup

[[add](#) | [rm](#) | [set](#) | [unset](#) | [bind](#) | [unbind](#) | [show](#)]

add bridgegroup

Synopsis

```
add bridgegroup <id> [-ipv6DynamicRouting ( ENABLED | DISABLED )]
```

Description

Create a Bridge group.

Parameters

id

An integer that uniquely identifies the bridge group. Minimum value: 1. Maximum value: 1000. Minimum value: 1 Maximum value: 1000

ipv6DynamicRouting

Enable all IPv6 dynamic routing protocols on this VLAN. Possible values: ENABLED, DISABLED Default: DISABLED. Note: For the ENABLED setting to work, you must configure IPv6 dynamic routing protocols from the VTYSH command line. For more information about configuring IPv6 dynamic routing protocols on the NetScaler appliance, see the 'Dynamic Routing' chapter of the Citrix NetScaler Networking Guide. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

```
add bridgegroup bg1
```

[Top](#)

rm bridgegroup

Synopsis

```
rm bridgegroup <id>
```

Description

Remove the bridge group created by the add bridge group command.

Parameters**id**

An integer that uniquely identifies the bridge group that you want to remove from the NetScaler appliance. Minimum value: 1 Maximum value: 1000

[Top](#)

set bridgegroup

Synopsis

```
set bridgegroup <id> -ipv6DynamicRouting ( ENABLED | DISABLED )
```

Description

Set Bridge group parameters.

Parameters**id**

An integer value that uniquely identifies the bridge group. Minimum value: 1. Maximum value: 1000. Minimum value: 1 Maximum value: 1000

ipv6DynamicRouting

Enable all IPv6 dynamic routing protocols on this bridge group. For this setting to work, you must configure IPv6 dynamic routing protocols from the VTYSH command line. For more information about configuring IPv6 dynamic routing protocols on the NetScaler appliance, see the Dynamic Routing chapter of the Citrix NetScaler Networking Guide. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

```
set bridgegroup bg1 -dynamicRouting ENABLED
```

[Top](#)

unset bridgegroup

Synopsis

unset bridgegroup <id> -ipv6DynamicRouting

Description

Use this command to remove bridgegroup settings. Refer to the set bridgegroup command for meanings of the arguments.

[Top](#)

bind bridgegroup

Synopsis

bind bridgegroup <id> [-vlan <positive_integer>] [-IPAddress <ip_addr|ipv6_addr|*> [<netmask>] [-td <positive_integer>]]

Description

Bind a vlan or an ip address to a bridgegroup.

Parameters

id

The integer that uniquely identifies the bridge group. Minimum value: 1 Maximum value: 1000

vlan

An integer that uniquely identifies the VLAN that you want to bind to this bridge group. Minimum value: 2 Maximum value: 4094

IPAddress

A network address or addresses to be associated with the bridge group. You must add entries for these network addresses in the routing table before running this command.

Example

```
bind bridgegroup bg1 -vlan 2
```

[Top](#)

unbind bridgegroup

Synopsis

unbind bridgegroup <id> [-vlan <positive_integer>] [-IPAddress <ip_addr|ipv6_addr|*> [<netmask>] [-td <positive_integer>]]

Description

Unbinds the specified VLANs or IP addresses from a bridge group.

Parameters

id

Integer that uniquely identifies the bridge group. Minimum value: 1 Maximum value: 1000

vlan

ID of the VLAN to unbind from this bridge group. Minimum value: 2 Maximum value: 4094

IPAddress

Network address associated with the bridge group.

[Top](#)

show bridgegroup

Synopsis

show bridgegroup [<id>]

Description

Display the configured bridge group. If a name is specified, only that particular bridge group information is displayed. Otherwise, all configured bridge groups are displayed.

Parameters

id

The name of the bridge group. Minimum value: 1 Maximum value: 1000

Example

```
An example of the output of the show bridge group
command is as follows:
2 configured Bridge Group:
1)      Bridge Group: 1
        Member vlans : 2 3 4
        IP: 10.102.33.27 MASK: 255.255.255.0
2)      Bridge Group: 2
        Member vlans : 5 6
```

[Top](#)

ipTunnel

[[add](#) | [rm](#) | [show](#)]

add ipTunnel

Synopsis

add ipTunnel <name> <remote> <remoteSubnetMask> <local> [-protocol <protocol>] [-ipsecProfileName <string>]

Description

Creates an IPv4 tunnel. An IP tunnel is a communication channel, using encapsulation technologies, between two networks that do not have a routing path. Every IP packet that is shared between the two networks is encapsulated within another packet and then sent through the tunnel.

Parameters

name

Name for the IP tunnel. Leading character must be a number or letter. Other characters allowed, after the first character, are @ _ - . (period) : (colon) # and space ().

remote

Public IPv4 address, of the remote device, used to set up the tunnel. For this parameter, you can alternatively specify a network address if you specify IPIP (IP over IP) for the Protocol parameter.

remoteSubnetMask

Subnet mask of the remote IP address of the tunnel.

local

Type of NetScaler owned public IPv4 address, configured on the local NetScaler appliance and used to set up the tunnel.

protocol

The IP tunneling protocol. Possible values: IPIP, GRE, IPSEC Default value: TNL_IPIP

ipsecProfileName

Name of IPSec profile to be associated. Default value: "ns_ipsec_default_profile"

Example

```
add iptunnel tunnel1 10.100.20.0 255.255.255.0 *
```

[Top](#)

rm ipTunnel

Synopsis

```
rm ipTunnel <name>
```

Description

Removes an IP tunnel configuration from the NetScaler appliance.

Parameters

name

Name of the IP Tunnel.

Example

```
rm iptunnel tunnel1
```

[Top](#)

show ipTunnel**Synopsis**

```
show ipTunnel [(<remote> <remoteSubnetMask>) | <name>]
```

Description

Display the configured IP tunnels.

Parameters**remote**

Public IPv4 address, of the remote device, used to set up the tunnel. For this parameter, you can alternatively specify a network address if you specify IPIP (IP over IP) for the Protocol parameter.

name

Name for the IP tunnel. Leading character must be a number or letter. Other characters allowed, after the first character, are @ _ - . (period) : (colon) # and space ().

Example

```
1) Name.....: t1
   Remote.....: 10.102.33.0   Mask.....:
255.255.255.0
   Local.....: *
   Encap.....: 0.0.0.0
   Protocol.....: IPIP
   Type.....: C

2) Name.....: tunnel1
   Remote.....: 10.100.20.0   Mask.....:
255.255.255.0
   Local.....: *
   Encap.....: 0.0.0.0
   Protocol.....: IPIP
   Type.....: C

3) Name.....:
   Remote.....: 10.102.33.190   Mask.....:
255.255.255.255
   Local.....: *
   Encap.....: 10.102.33.85
```

Protocol.....:	IPIP
Type.....:	I

[Top](#)

ip6Tunnel

[\[add | rm | show \]](#)

add ip6Tunnel

Synopsis

add ip6Tunnel <name> <remote> <local>

Description

Creates an IPv6 tunnel. An IP tunnel is a communication channel, using encapsulation technologies, between two networks that do not have a routing path. Every IP packet that is shared between the two networks is encapsulated within another packet and then sent through the tunnel.

Parameters

name

Name for the IPv6 Tunnel. Cannot be changed after the service group is created. Must begin with a number or letter, and can consist of letters, numbers, and the @ _ - . (period) : (colon) # and space () characters.

remote

An IPv6 address of the remote NetScaler appliance used to set up the tunnel.

local

An IPv6 address of the local NetScaler appliance used to set up the tunnel.

Example

```
add ip6tunnel tun6 9901::200/64 *
```

[Top](#)

rm ip6Tunnel

Synopsis

rm ip6Tunnel <name>

Description

Removes an IPv6 tunnel from the NetScaler appliance.

Parameters

name

Name of the IPv6 tunnel to be removed.

Example

```
rm ip6tunnel tun6
```

[Top](#)

show ip6Tunnel

Synopsis

show ip6Tunnel [<name> | <remote>]

Description

Displays the settings of all IPv6 tunnels configured on the NetScaler appliance, or of the specified IPv6 tunnel.

Parameters

name

Name of the IPv6 tunnel whose details you want to display.

remote

The IPv6 address at which the remote NetScaler appliance connects to the tunnel.

Example

```
1) Name.....: tun61
   Remote.....: 9901::200/64
   Local.....: *
   Encap.....: ::0/128
   Type.....: C

2) Name.....: tun62
   Remote.....: 9903::400/84
   Local.....: 9903::100
   Encap.....: ::0/128
   Type.....: C

3) Name.....:
   Remote.....: 9902::300/90
   Local.....: *
   Encap.....: 9902::100
   Type.....: I
```

[Top](#)

netbridge

[[add](#) | [rm](#) | [show](#) | [bind](#) | [unbind](#)]

add netbridge

Synopsis

add netbridge <name>

Description

Add a network bridge.

Parameters

name

The name of the network bridge.

Example

```
add netbridge bridge1
```

[Top](#)

rm netbridge

Synopsis

rm netbridge <name>

Description

Remove a network bridge.

Parameters

name

The name of the network bridge.

Example

```
remove netbridge bridge1
```

[Top](#)

show netbridge

Synopsis

show netbridge [<name>]

Description

Show configured network bridges.

Parameters

name

The name of the network bridge.

[Top](#)

bind netbridge

Synopsis

```
bind netbridge <name> [-tunnel <string> ...] [-vlan <positive_integer> ...] [-IPAddress  
<ip_addr|ipv6_addr|*> [<netmask>]]
```

Description

Bind a network bridge to its attributes.

Parameters

name

The name of the network bridge.

tunnel

The name of the tunnel that needs to be a part of this network bridge.

vlan

The VLAN that needs to be extended. Minimum value: 1 Maximum value: 4094

IPAddress

The subnet that needs to be extended.

Example

```
bind netbridge bridge1 -tunnel tun0
```

[Top](#)

unbind netbridge

Synopsis

```
unbind netbridge <name> [-tunnel <string> ...] [-vlan <positive_integer> ...] [-IPAddress  
<ip_addr|ipv6_addr|*> [<netmask>]]
```

Description

Unbind a network bridge from its attributes.

Parameters

name

The name of the network bridge.

tunnel

The name of the tunnel that is part of this network bridge.

vlan

The vlan that is part of this network bridge. Minimum value: 1 Maximum value: 4094

IPAddress

The subnet that is part of this network bridge.

Example

```
unbind netbridge bridge1 -tunnel tun0
```

[Top](#)

ipset

[[add](#) | [rm](#) | [bind](#) | [unbind](#) | [show](#)]

add ipset

Synopsis

```
add ipset <name> [-td <positive_integer>]
```

Description

Creates an IP set to which you can bind subnet IP (SNIP) or mapped IP (MIP) addresses that have been configured on the NetScaler appliance.

Parameters

name

Name for the IP set. Must begin with a letter, number, or the underscore character (_), and can consist of letters, numbers, and the hyphen (-), period (.) pound (#), space (), at sign (@), equals (=), colon (:), and underscore characters. Cannot be changed after the IP set is created. Choose a name that helps identify the IP set.

td

Traffic Domain Id. Maximum value: 4094

Example

```
add ipset pool1
```

[Top](#)

rm ipset

Synopsis

```
rm ipset <name> ...
```

Description

Removes an IP set from the NetScaler appliance.

Parameters

name

Name of the IP set to be removed.

Example

```
rm ipset pool1
```

[Top](#)

bind ipset

Synopsis

bind ipset <name> <IPAddress>@ ...

Description

Binds specified IP addresses to an IP set.

Parameters

name

Name of the IP set to which to bind IP addresses.

IPAddress

SNIP or MIP addresses, configured on the NetScaler appliance, to be bound to the IP set. (If using the CLI, use spaces to separate multiple addresses.)

Example

```
bind ipset ipset_1 10.102.1.10
```

[Top](#)

unbind ipset

Synopsis

unbind ipset <name> <IPAddress>@ ...

Description

Unbinds the associated IP addresses from an IP set.

Parameters

name

Name of the IP set from which to unbind IP addresses.

IPAddress

IP addresses to be unbound from the IP set. (If using the CLI, use spaces to separate multiple addresses.)

Example

```
unbind ipset ipset_1 10.102.1.10
```

[Top](#)

show ipset

Synopsis

```
show ipset [<name>]
```

Description

Displays the settings of all IP sets configured on the NetScaler appliance, or of the specified IP set.

Parameters

name

Name of the IP set whose details you want to display.

Example

```
show network ipset
```

[Top](#)

linkset

[[add](#) | [rm](#) | [bind](#) | [unbind](#) | [show](#)]

add linkset

Synopsis

```
add linkset <id>
```

Description

Adds a linkset to the NetScaler cluster.

Parameters

id

Unique identifier for the linkset. Must be of the form LS/x, where x can be an integer from 1 to 32.

Example

```
add linkset LS/1
```

[Top](#)

rm linkset

Synopsis

rm linkset <id>

Description

Removes a linkset from the cluster.

Parameters

id

ID of the linkset to be removed.

Example

```
rm linkset LS/1
```

[Top](#)

bind linkset

Synopsis

bind linkset <id> -ifnum <interface_name> ...

Description

Binds interfaces to the linkset.

Parameters

id

ID of the linkset to which to bind the interfaces.

ifnum

The interfaces to be bound to the linkset.

Example

```
bind linkset LS/1 -ifnum 1/1/1
```

[Top](#)

unbind linkset

Synopsis

unbind linkset <id> -ifnum <interface_name> ...

Description

Unbinds interfaces from the linkset.

Parameters

id

ID of the linkset from which to unbind the interfaces.

ifnum

Interfaces to be unbound from the linkset.

Example

```
unbind linkset LS/1 -ifnum 1/1/1
```

[Top](#)

show linkset

Synopsis

show linkset [<id>]

Description

Displays information about all linksets, or displays information about the specified linkset.

Parameters

id

ID of the linkset for which to display information. If an ID is not provided, the display includes information about all linksets that are available in the cluster.

Example

```
show linkset
```

[Top](#)

netProfile

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add netProfile

Synopsis

add netProfile <name> [-td <positive_integer>] [-srcIP <string>]

Description

Creates a net profile. A net profile (or network profile) contains an IP address or an IP set. During communication with physical servers or peers, the NetScaler appliance uses the addresses specified in the profile as the source IP address.

Parameters

name

Name for the net profile. Must begin with a letter, number, or the underscore character (_), and can consist of letters, numbers, and the hyphen (-), period (.) pound (#), space (), at sign (@), equals (=), colon (:), and underscore characters. Cannot be changed after the profile is created. Choose a name that helps identify the net profile.

td

Traffic Domain Id. Maximum value: 4094

srcIP

IP address or the name of an IP set.

Example

```
add netProfile prof1 -srcip 10.102.1.10
```

[Top](#)

rm netProfile

Synopsis

rm netProfile <name> ...

Description

Removes a net profile from the NetScaler appliance.

Parameters

name

Name of the net profile to be removed.

Example

```
rm netProfile prof1
```

[Top](#)

set netProfile

Synopsis

set netProfile <name> [-srcIP <string>]

Description

Modifies the srcIP parameter of a net profile.

Parameters

name

Name of the net profile whose parameter you want to modify.

srcIP

IP address or the name of an IP set.

Example

```
set netProfile prof_1 -srcIP 10.102.1.10
```

[Top](#)

unset netProfile

Synopsis

unset netProfile <name> [-srcIP]

Description

Removes the srcIP attribute of a net profile..Refer to the set netProfile command for meanings of the arguments.

Example

```
unset netProfile prof1 -srcIP
```

[Top](#)

show netProfile

Synopsis

show netProfile [<name>]

Description

Displays the settings of all net profiles configured on the NetScaler appliance, or of the specified net profile.

Parameters

name

Name of the net profile whose details you want to display.

Example

```
show netProfile
```

[Top](#)

arpparam

[[set](#) | [unset](#) | [show](#)]

set arpparam

Synopsis

set arpparam [-timeout <positive_integer>] [-spoofValidation (ENABLED | DISABLED)]

Description

Sets a global time-out value for dynamic ARP entries.

Parameters

timeout

Time-out value (aging time) for the dynamically learned ARP entries, in seconds. The new value applies only to ARP entries that are dynamically learned after the new value is set. Previously existing ARP entries expire after the previously configured aging time. Default value: 1200 Minimum value: 5 Maximum value: 1200

spoofValidation

enable/disable arp spoofing validation Possible values: ENABLED, DISABLED Default value: DISABLED

Example

```
set arpparam -timeout 200 -spoofvalidate ENABLE
```

[Top](#)

unset arpparam

Synopsis

unset arpparam [-timeout] [-spoofValidation]

Description

Use this command to remove arpparam settings. Refer to the set arpparam command for meanings of the arguments.

[Top](#)

show arpparam

Synopsis

show arpparam

Description

Display the global setting of dynamically learned ARP entries.

Example

```
show arpparam
```

[Top](#)

ci

show ci

Synopsis

show ci

Description

Displays all the critical interfaces of the NetScaler appliance. In a High Availability configuration, an interface that has HA MON enabled and is not bound to any FIS, is a critical interface. Failure of any critical interface triggers HA failover.

Example

```
>show ci
Critical Interfaces: LO/1 1/2
```

interface

[[clear](#) | [set](#) | [unset](#) | [enable](#) | [disable](#) | [reset](#) | [show](#) | [stat](#)]

clear interface

Synopsis

clear interface <id>@

Description

Resets the statistical counters of the specified interface.

Parameters

id

Interface number, in C/U format, where C can take one of the following values: * 0 - Indicates a management interface. * 1 - Indicates a 1 Gbps port. * 10 - Indicates a 10 Gbps port. * LA - Indicates a link aggregation port. * LO - Indicates a loop back port. U is a unique integer for representing an interface in a particular port group.

[Top](#)

set interface

Synopsis

```
set interface <id>@ [-speed <speed>] [-duplex <duplex>] [-flowControl <flowControl>]
[-autoneg ( DISABLED | ENABLED )] [-haMonitor ( ON | OFF )] [-tagall ( ON | OFF )] [-
lacpMode <lacpMode>] [-lacpKey <positive_integer>] [-lagtype ( NODE | CLUSTER )] [-
lacpPriority <positive_integer>] [-lacpTimeout ( LONG | SHORT )] [-ifAlias <string>] [-
throughput <positive_integer>] [-bandwidthHigh <positive_integer> [-bandwidthNormal
<positive_integer>]]
```

Description

Modifies the parameters of an interface.

Parameters

id

ID of the Interface whose parameters you want to modify. For a NetScaler appliance, specify the interface in C/U notation (for example, 1/3). For a cluster configuration, specify the interface in N/C/U notation (for example, 2/1/3). where C can take one of the following values: * 0 - Indicates a management interface. * 1 - Indicates a 1 Gbps port. * 10 - Indicates a 10 Gbps port. U is a unique integer for representing an interface in a particular port group. N is the ID of the node to which an interface belongs in a cluster configuration. Use spaces to separate multiple entries.

speed

Ethernet speed of the interface, in Mbps. Notes: * If you set the speed as AUTO, the NetScaler appliance attempts to auto-negotiate or auto-sense the link speed of the interface when it is UP. You must enable auto negotiation on the interface. * If you set a speed other than AUTO, you must specify the same speed for the peer network device. Mismatched speed and duplex settings between the peer devices of a link lead to link errors, packet loss, and other errors. Some interfaces do not support certain speeds. If you specify an unsupported speed, an error message appears. Possible values: AUTO, 10, 100, 1000, 10000 Default value: NSA_DVC_SPEED_AUTO

duplex

The duplex mode for the interface. Notes: * If you set the duplex mode to AUTO, the NetScaler appliance attempts to auto-negotiate the duplex mode of the interface when it is UP. You must enable auto negotiation on the interface. If you set a duplex mode other than AUTO, you must specify the same duplex mode for the peer network

device. Mismatched speed and duplex settings between the peer devices of a link lead to link errors, packet loss, and other errors. Possible values: AUTO, HALF, FULL
Default value: NSA_DVC_DUPLEX_AUTO

flowControl

802.3x flow control setting for the interface. The 802.3x specification does not define flow control for 10 Mbps and 100 Mbps speeds, but if a Gigabit Ethernet interface operates at those speeds, the flow control settings can be applied. The flow control setting that is finally applied to an interface depends on auto-negotiation. With the ON option, the peer negotiates the flow control, but the appliance then forces two-way flow control for the interface. Possible values: OFF, RX, TX, RXTX Default value: NSA_DVC_FC_OFF

autoneg

Auto-negotiation state of the interface. With the ENABLED setting, the NetScaler appliance auto-negotiates the speed and duplex settings with the peer network device on the link. The NetScaler appliance auto-negotiates the settings of only those parameters (speed or duplex mode) for which the value is set as AUTO. Possible values: DISABLED, ENABLED Default value: NSA_DVC_AUTONEG_ON

haMonitor

In a High Availability (HA) configuration, monitor the interface for failure events. In an HA configuration, an interface that has HA MON enabled and is not bound to any Failover Interface Set (FIS), is a critical interface. Failure or disabling of any critical interface triggers HA failover. Possible values: ON, OFF Default value: NSA_DVC_MONITOR_ON

tagall

Add a four-byte 802.1q tag to every packet sent on this interface. The ON setting applies the tag for this interface's native VLAN. OFF applies the tag for all VLANs other than the native VLAN. Possible values: ON, OFF Default value: NSA_DVC_VTRUNK_OFF

trunk

This argument is deprecated by tagall. Possible values: ON, OFF Default value: NSA_DVC_VTRUNK_OFF

lacpMode

Bind the interface to a LA channel created by the Link Aggregation control protocol (LACP). Available settings function as follows: * Active - The LA channel port of the NetScaler appliance generates LACPDU messages on a regular basis, regardless of any need expressed by its peer device to receive them. * Passive - The LA channel port of the NetScaler appliance does not transmit LACPDU messages unless the peer device port is in the active mode. That is, the port does not speak unless spoken to. * Disabled - Unbinds the interface from the LA channel. If this is the only interface in the LA channel, the LA channel is removed. Possible values: DISABLED, ACTIVE, PASSIVE Default value: NSA_LACP_DISABLE

lacpKey

Integer identifying the LACP LA channel to which the interface is to be bound. For an LA channel of the NetScaler appliance, this digit specifies the variable x of an LA channel in LA/x notation, where x can range from 1 to 4. For example, if you specify 3 as the LACP key for an LA channel, the interface is bound to the LA channel LA/3.

For an LA channel of a cluster configuration, this digit specifies the variable y of a cluster LA channel in CLA/(y-4) notation, where y can range from 5 to 8. For example, if you specify 6 as the LACP key for a cluster LA channel, the interface is bound to the cluster LA channel CLA/2. Minimum value: 1 Maximum value: 8

lagtype

Type of entity (NetScaler appliance or cluster configuration) for which to create the channel. Possible values: NODE, CLUSTER Default value: NSA_LAG_NODE

lacpPriority

LACP port priority, expressed as an integer. The lower the number, the higher the priority. The NetScaler appliance limits the number of interfaces in an LA channel to eight. If LACP is enabled on more than eight interfaces, the appliance selects eight interfaces, in descending order of port priority, to form a channel. Default value: 32768 Minimum value: 1 Maximum value: 65535

lacpTimeout

Interval at which the NetScaler appliance sends LACPDU messages to the peer device on the LA channel. Available settings function as follows: LONG - 30 seconds. SHORT - 1 second. Possible values: LONG, SHORT Default value: NSA_LACP_TIMEOUT_LONG

ifAlias

Alias name for the interface. Used only to enhance readability. To perform any operations, you have to specify the interface ID. Default value: ""

throughput

Low threshold value for the throughput of the interface, in Mbps. In an HA configuration, failover is triggered if the interface has HA MON enabled and the throughput is below the specified the threshold. Maximum value: 80000

bandwidthHigh

High threshold value for the bandwidth usage of the interface, in Mbps. The NetScaler appliance generates an SNMP trap message when the bandwidth usage of the interface is greater than or equal to the specified high threshold value. Maximum value: 80000

[Top](#)

unset interface

Synopsis

```
unset interface <id>@ [-speed] [-duplex] [-flowControl] [-autoneg] [-haMonitor] [-tagall] [-lacpMode] [-lacpKey] [-lacpPriority] [-lacpTimeout] [-ifAlias] [-throughput] [-bandwidthHigh] [-bandwidthNormal]
```

Description

Use this command to remove interface settings. Refer to the set interface command for meanings of the arguments.

[Top](#)

enable interface

Synopsis

enable interface <id>@

Description

Enables the interface. If the link is active, it can transmit and receive packets. Note: To view the status of an interface, use the show interface command.

Parameters

id

Interface number, in C/U format, where C can take one of the following values: * 0 - Indicates a management interface. * 1 - Indicates a 1 Gbps port. * 10 - Indicates a 10 Gbps port. * LA - Indicates a link aggregation port. * LO - Indicates a loop back port. U is a unique integer for representing an interface in a particular port group.

[Top](#)

disable interface

Synopsis

disable interface <id>@

Description

Disables the interface from transmitting and receiving packets. The link remains active and the peer network device is unaware that the interface has been disabled. In a High Availability configuration, an interface that has HA MON enabled and is not bound to any Failover Interface Set (FIS), is a critical interface. Disabling or failure of any critical interface triggers HA failover. Note: To view the status of an interface, use the show interface command.

Parameters

id

Interface number, in C/U format, where C can take one of the following values: * 0 - Indicates a management interface. * 1 - Indicates a 1 Gbps port. * 10 - Indicates a 10 Gbps port. * LA - Indicates a link aggregation port. * LO - Indicates a loop back port. U is a unique integer for representing an interface in a particular port group.

[Top](#)

reset interface

Synopsis

reset interface <id>@

Description

Restarts the interface but leaves the administrative state ENABLED or DISABLED and configuration unchanged. The link pertaining to the interface is reestablished with the existing settings.

Parameters

id

Interface number, in C/U format, where C can take one of the following values: * 0 - Indicates a management interface. * 1 - Indicates a 1 Gbps port. * 10 - Indicates a 10 Gbps port. * LA - Indicates a link aggregation port. * LO - Indicates a loop back port. U is a unique integer for representing an interface in a particular port group.

[Top](#)

show interface

Synopsis

show interface [<id>@] show interface stats - alias for 'stat interface'

Description

Displays the settings of all interfaces or of the specified interface on the NetScaler appliance. To display the settings of all interfaces, run the command without any parameters. To display the settings of a particular interface, specify the ID of the interface.

Parameters

id

Interface number, in C/U format, where C can take one of the following values: * 0 - Indicates a management interface. * 1 - Indicates a 1 Gbps port. * 10 - Indicates a 10 Gbps port. * LA - Indicates a link aggregation port. * LO - Indicates a loop back port. U is a unique integer for representing an interface in a particular port group.

Example

The output for the show interface command is as follows:

```
1)      Interface 0/1 (Gig Ethernet 10/100/1000
MBits) #4
      flags=0x4021 <ENABLED, UP, UP, autoneg,
HAMON, 802.1q>
      MTU=1514, native vlan=1,
MAC=00:30:48:67:9a:9a, uptime 1039h54m28s
      Requested: media AUTO, speed AUTO, duplex
AUTO, fctl OFF,
              throughput 0

2)      Interface 1/1 (Gig Ethernet, copper SFP) #3
      flags=0x4021 <ENABLED, UP, UP, autoneg,
HAMON, BACKPLANE, 802.1q>
      MTU=1514, native vlan=1, MAC=00:e0:ed:
12:e8:b7, uptime 1039h54m28s
      Requested: media AUTO, speed AUTO, duplex
AUTO, fctl OFF,
              throughput 0
```



```

3)      Interface 1/2 (Gig Ethernet, copper SFP) #2
        flags=0x4001 <ENABLED, DOWN, down,
autoneg, HAMON, 802.1q>
        MTU=1514, native vlan=1, MAC=00:e0:ed:
12:e8:b6, downtime 1039h54m28s
        Requested: media AUTO, speed AUTO, duplex
AUTO, fctl OFF,
        throughput 0

4)      Interface 1/3 (Gig Ethernet, copper SFP) #1
        flags=0x4001 <disabled, DOWN, down,
autoneg, HAMON, 802.1q>
        MTU=1514, native vlan=1, MAC=00:e0:ed:
12:e8:b5, downtime 1039h54m33s
        Requested: media AUTO, speed AUTO, duplex
AUTO, fctl OFF,
        throughput 0

5)      Interface 1/4 (Gig Ethernet, copper SFP) #0
        flags=0x4001 <disabled, UP, down, autoneg,
HAMON, 802.1q>
        MTU=1514, native vlan=1, MAC=00:e0:ed:
12:e8:b4, downtime 1039h54m28s
        Requested: media AUTO, speed AUTO, duplex
AUTO, fctl OFF,
        throughput 0

Done
>

```

The output for the show interface 0/1 command is as follows:

```

        Interface 0/1 (Gig Ethernet 10/100/1000
Mbits) #4
        flags=0xc020 <ENABLED, UP, UP, autoneg,
HAMON, 802.1q>
        MTU=1514, native vlan=1,
MAC=00:30:48:67:9a:9a, uptime 0h00m40s
        Requested: media AUTO, speed AUTO, duplex
AUTO, fctl RXTX,
        throughput 0
        Actual: media UTP, speed 1000, duplex
FULL, fctl RXTX, throughput 1000

        RX: Pkts(27) Bytes(2034) Errs(0) Drops(27)
Stalls(0)
        TX: Pkts(3) Bytes(170) Errs(0) Drops(22)
Stalls(0)
        NIC: InDisc(0) OutDisc(0) Fctls(0)
Stalls(0) Hangs(0) Muted(0)
        Bandwidth thresholds are not set.

Done
>

```

[Top](#)

stat interface

Synopsis

```
stat interface [<id>@] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile  
<input_filename>] [-clearstats ( basic | full )]
```

Description

Displays the statistics of all interfaces or of the specified interface on the NetScaler appliance. To display the statistics of all interfaces, run the command without any parameters. To display the statistics of a particular interface, specify the ID of the interface.

Parameters

id

Interface number, in C/U format, where C can take one of the following values: * 0 - Indicates a management interface. * 1 - Indicates a 1 Gbps port. * 10 - Indicates a 10 Gbps port. * LA - Indicates a link aggregation port. * LO - Indicates a loop back port. U is a unique integer for representing an interface in a particular port group.

clearstats

Clear the statistics / counters Possible values: basic, full

[Top](#)

rnat

[[clear](#) | [set](#) | [unset](#) | [stat](#) | [show](#)]

clear rnat

Synopsis

```
clear rnat ((<network> [<netmask>]) | (<aclname> [-redirectPort])) [-natIP <ip_addr|  
*>@ ...] [-td <positive_integer>]
```

Description

Removes an RNAT rule from the NetScaler appliance.

Parameters

network

The network address defined for the RNAT entry.

netmask

The subnet mask for the network address.

aclname

An extended ACL defined for the RNAT entry.

redirectPort

The port number to which the packets are redirected.

natIP

The NAT IP address defined for the RNAT entry.

td

Traffic Domain Id. Maximum value: 4094

[Top](#)

set rnat**Synopsis**

```
set rnat (((<network> [<netmask>] [-natIP <ip_addr|*>@ ...]) | (<aclname> [-redirectPort <port>] [-natIP <ip_addr|*>@ ...])) [-td <positive_integer>]
```

Description

Modifies parameters of an RNAT rule.

Parameters**network**

IPv4 network address on whose traffic you want the NetScaler appliance to do RNAT processing.

aclname

Name of any configured extended ACL whose action is ALLOW. The condition specified in the extended ACL rule is used as the condition for the RNAT6 rule.

[Top](#)

unset rnat**Synopsis**

```
unset rnat (((<network> [<netmask>]) | (<aclname> [-redirectPort])) [-td <positive_integer>] [-natIP <ip_addr|*>@ ...]
```

Description

Use this command to modify the parameters of configured Reverse NAT on the system..Refer to the set rnat command for meanings of the arguments.

[Top](#)

stat rnat**Synopsis**

```
stat rnat [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-clearstats ( basic | full )]
```

Description

Display statistics for rnat sessions.

Parameters

clearstats

Clear the statistics / counters Possible values: basic, full

Example

```
stat rnat
```

[Top](#)

show rnat

Synopsis

show rnat

Description

Display the Reverse NAT configuration.

[Top](#)

bridgetable

[[set](#) | [unset](#) | [show](#) | [clear](#)]

set bridgetable

Synopsis

set bridgetable -bridgeAge <positive_integer>

Description

Sets global parameters of bridge table entries.

Parameters

bridgeAge

Time-out value for the bridge table entries, in seconds. The new value applies only to the entries that are dynamically learned after the new value is set. Previously existing bridge table entries expire after the previously configured time-out value. Default value: 300 Minimum value: 60 Maximum value: 300

Example

```
set bridgetable -bridgeAge 200
```

[Top](#)

unset bridgetable

Synopsis

unset bridgetable -bridgeAge

Description

Use this command to remove bridgetable settings. Refer to the set bridgetable command for meanings of the arguments.

[Top](#)

show bridgetable

Synopsis

show bridgetable

Description

Displays the bridge table entries and the configured time-out values for these entries.

Example

```
show bridgetable
```

[Top](#)

clear bridgetable

Synopsis

clear bridgetable [-vlan <positive_integer>] [-ifnum <interface_name>]

Description

Remove entries from bridge table

Parameters

vlan

VLAN whose entries are to be removed.

ifnum

INTERFACE whose entries are to be removed.

[Top](#)

bridge

stat bridge

Synopsis

```
stat bridge [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile  
<input_filename>] [-clearstats ( basic | full )]
```

Description

Display bridging statistics.

Parameters

clearstats

Clear the statistics / counters Possible values: basic, full

lACP

[[set](#) | [show](#)]

set lacp

Synopsis

```
set lacp -sysPriority <positive_integer> [-ownerNode <positive_integer>]
```

Description

Sets the Link Aggregation Control Protocol (LACP) system priority.

Parameters

sysPriority

Priority number that determines which peer device of an LACP LA channel can have control over the LA channel. This parameter is globally applied to all LACP channels on the NetScaler appliance. The lower the number, the higher the priority. Default value: 32768 Minimum value: 1 Maximum value: 65535

ownerNode

The owner node in a cluster for which we want to set the lacp priority. Owner node can vary from 0 to 31. Ownernode value of 254 is used for Cluster. Default value: 255

[Top](#)

show lacp

Synopsis

```
show lacp [-ownerNode <positive_integer>]
```

Description

Displays the settings of all channels created by the link aggregation control protocol (LACP) on the NetScaler appliance.

Parameters

ownerNode

The owner node in a cluster for which we want to set the lacp priority. Owner node can vary from 0 to 31. Ownernode value of 254 is used for Cluster. Default value: 255

[Top](#)

rnatparam

[[set](#) | [unset](#) | [show](#)]

set rnatparam

Synopsis

set rnatparam -tcpproxy (ENABLED | DISABLED)

Description

Sets global parameters of RNAT rules on the NetScaler appliance.

Parameters

tcpproxy

Enable TCP proxy, which enables the NetScaler appliance to optimize the RNAT TCP traffic by using Layer 4 features. Possible values: ENABLED, DISABLED Default value: ENABLED

Example

```
set rnat parameter -tcpproxy ENABLED
```

[Top](#)

unset rnatparam

Synopsis

unset rnatparam -tcpproxy

Description

Use this command to remove rnatparam settings. Refer to the set rnatparam command for meanings of the arguments.

[Top](#)

show rnatparam

Synopsis

show rnatparam

Description

Show the rnat parameter.

Example

```
show rnat parameter
```

[Top](#)

rnatip

stat rnatip

Synopsis

```
stat rnatip [<rnatip>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile  
<input_filename>] [-clearstats ( basic | full )]
```

Description

Display statistics for RNAT sessions.

Parameters

rnatip

Specifies the NAT IP address of the configured RNAT entry for which you want to see the statistics. If you do not specify an IP address, this displays the statistics for all the configured RNAT entries.

clearstats

Clear the statistics / counters Possible values: basic, full

Example

```
stat rnatip 1.1.1.1
```

vrIDParam

[[set](#) | [unset](#) | [show](#)]

set vrIDParam

Synopsis

```
set vrIDParam -sendToMaster ( ENABLED | DISABLED )
```

Description

Sets global parameters of VMACs on the NetScaler appliance.

Parameters

sendToMaster

Forward packets to the master node, in an active-active mode configuration, if the virtual server is in the backup state and sharing is disabled. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

```
set vrIDParam -sendToMaster ENABLED
```

[Top](#)

unset vrIDParam

Synopsis

```
unset vrIDParam -sendToMaster
```

Description

Use this command to remove vrIDParam settings. Refer to the set vrIDParam command for meanings of the arguments.

[Top](#)

show vrIDParam

Synopsis

```
show vrIDParam
```

Description

Displays the VRID global settings on the NetScaler appliance.

[Top](#)

nd6RAvariables

[[set](#) | [unset](#) | [show](#) | [bind](#) | [unbind](#)]

set nd6RAvariables

Synopsis

```
set nd6RAvariables -vlan <positive_integer> [-ceaseRouterAdv ( YES | NO )] [-sendRouterAdv ( YES | NO )] [-srcLinkLayerAddrOption ( YES | NO )] [-onlyUnicastRtAdvResponse ( YES | NO )] [-managedAddrConfig ( YES | NO )] [-otherAddrConfig ( YES | NO )] [-currHopLimit <positive_integer>] [-maxRtAdvInterval <positive_integer>] [-minRtAdvInterval <positive_integer>] [-linkMTU <positive_integer>] [-reachableTime <positive_integer>] [-retransTime <positive_integer>] [-defaultLifeTime <integer>]
```

Description

Set vlan specific Router Advertisement parameters in NetScaler.

Parameters

vlan

The VLAN number. Maximum value: 4094

ceaseRouterAdv

Cease router advertisements on this vlan. Possible values: YES, NO Default value: NO

sendRouterAdv

whether the router sends periodic RAs and responds to Router Solicitations. Possible values: YES, NO Default value: NO

srcLinkLayerAddrOption

Include source link layer address option in RA messages. Possible values: YES, NO Default value: YES

onlyUnicastRtAdvResponse

Send only Unicast Router Advertisements in respond to Router Solicitations. Possible values: YES, NO Default value: NO

managedAddrConfig

Value to be placed in the Managed address configuration flag field. Possible values: YES, NO Default value: NO

otherAddrConfig

Value to be placed in the Other configuration flag field. Possible values: YES, NO Default value: NO

currHopLimit

Current Hop limit. Default value: 64 Maximum value: 255

maxRtAdvInterval

Maximum time allowed between unsolicited multicast RAs, in seconds. Default value: 600 Minimum value: 4 Maximum value: 1800

minRtAdvInterval

Minimum time interval between RA messages, in seconds. Default value: 198 Minimum value: 3 Maximum value: 1350

linkMTU

The Link MTU. Maximum value: 1500

reachableTime

Reachable time, in milliseconds. Maximum value: 3600000

retransTime

Retransmission time, in milliseconds.

defaultLifeTime

Default life time, in seconds. Default value: 1800 Maximum value: 9000

Example

```
set nd6RAvariables -vlan 2 -maxRtAdvInterval 600
```

[Top](#)**unset nd6RAvariables****Synopsis**

```
unset nd6RAvariables -vlan <positive_integer> [-ceaseRouterAdv] [-sendRouterAdv] [-srcLinkLayerAddrOption] [-onlyUnicastRtAdvResponse] [-managedAddrConfig] [-otherAddrConfig] [-currHopLimit] [-maxRtAdvInterval] [-minRtAdvInterval] [-linkMTU] [-reachableTime] [-retransTime] [-defaultLifeTime]
```

Description

Use this command to remove nd6RAvariables settings. Refer to the set nd6RAvariables command for meanings of the arguments.

[Top](#)**show nd6RAvariables****Synopsis**

```
show nd6RAvariables [-vlan <positive_integer>]
```

Description

Display Router Advertisement configuration variables.

Parameters

vlan
The VLAN number. Maximum value: 4094

[Top](#)**bind nd6RAvariables****Synopsis**

```
bind nd6RAvariables -vlan <positive_integer> -ipv6Prefix <ipv6_addr|*>
```

Description

Bind on-link global prefixes to Router Advertisements variables.

Parameters

vlan
The VLAN number. Maximum value: 4094

ipv6Prefix
Onlink prefixes for RA messages.

Example

```
bind nd6RAvariables -vlan 2 -ipv6Prefix 8000::/64
```

[Top](#)

unbind nd6RAvariables

Synopsis

```
unbind nd6RAvariables -vlan <positive_integer> -ipv6Prefix <ipv6_addr|*>
```

Description

Unbind prefix from Router Advertisement parameters in NetScaler

Parameters

vlan

The VLAN number. Maximum value: 4094

ipv6Prefix

Onlink prefixes for RA messages.

Example

```
unbind nd6RAvariables -vlan 2 -ipv6Prefix 8000::/64
```

[Top](#)

onLinkIPv6Prefix

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add onLinkIPv6Prefix

Synopsis

```
add onLinkIPv6Prefix <ipv6Prefix> [-onlinkPrefix ( YES | NO )] [-autonomusPrefix ( YES | NO )] [-depricatePrefix ( YES | NO )] [-decrementPrefixLifeTimes ( YES | NO )] [-prefixValideLifeTime <positive_integer>] [-prefixPreferredLifeTime <positive_integer>]
```

Description

add a new on-link global prefix.

Parameters

ipv6Prefix

Onlink prefixes for RA messages.

onlinkPrefix

RA Prefix onlink flag. Possible values: YES, NO Default value: YES

autonomusPrefix

RA Prefix Autonomus flag. Possible values: YES, NO Default value: YES

depricatePrefix

Depricate the prefix. Possible values: YES, NO Default value: NO

decrementPrefixLifeTimes

RA Prefix Autonomus flag. Possible values: YES, NO Default value: NO

prefixValideLifeTime

Valide life time of the prefix, in seconds. Default value: 2592000

prefixPreferredLifeTime

Preferred life time of the prefix, in seconds. Default value: 604800

Example

```
add onLinkIPv6Prefix 8000::/64
```

[Top](#)

rm onLinkIPv6Prefix**Synopsis**

```
rm onLinkIPv6Prefix <ipv6Prefix>
```

Description

remove an existing on-link global prefix.

Parameters**ipv6Prefix**

Onlink prefixes for RA messages.

Example

```
rm onLinkIPv6Prefix 8000::/64
```

[Top](#)

set onLinkIPv6Prefix**Synopsis**

```
set onLinkIPv6Prefix <ipv6Prefix> [-onlinkPrefix ( YES | NO )] [-autonomusPrefix ( YES | NO )] [-depricatePrefix ( YES | NO )] [-decrementPrefixLifeTimes ( YES | NO )] [-prefixValideLifeTime <positive_integer>] [-prefixPreferredLifeTime <positive_integer>]
```

Description

set on-link global prefix's configuration variables.

Parameters

ipv6Prefix

Onlink prefixes for RA messages.

onlinkPrefix

RA Prefix onlink flag. Possible values: YES, NO Default value: YES

autonomusPrefix

RA Prefix Autonomus flag. Possible values: YES, NO Default value: YES

depricatePrefix

Depricate the prefix. Possible values: YES, NO Default value: NO

decrementPrefixLifeTimes

RA Prefix Autonomus flag. Possible values: YES, NO Default value: NO

prefixValideLifeTime

Valide life time of the prefix, in seconds. Default value: 2592000

prefixPreferredLifeTime

Preferred life time of the prefix, in seconds. Default value: 604800

Example

```
set onLinkIPv6Prefix 8000::/64 -  
prefixValideLifeTime 2592000
```

[Top](#)

unset onLinkIPv6Prefix

Synopsis

```
unset onLinkIPv6Prefix <ipv6Prefix> [-onlinkPrefix] [-autonomusPrefix] [-  
depricatePrefix] [-decrementPrefixLifeTimes] [-prefixValideLifeTime] [-  
prefixPreferredLifeTime]
```

Description

Use this command to remove onLinkIPv6Prefix settings.Refer to the set onLinkIPv6Prefix command for meanings of the arguments.

[Top](#)

show onLinkIPv6Prefix

Synopsis

```
show onLinkIPv6Prefix [<ipv6Prefix>]
```

Description

displays on-link global prefixes.

Parameters

ipv6Prefix

Onlink prefixes for RA messages.

[Top](#)

ipv6

[[set](#) | [unset](#) | [show](#)]

set ipv6

Synopsis

```
set ipv6 [-rlearning ( ENABLED | DISABLED )] [-routerRedirection ( ENABLED |
DISABLED )] [-ndBasereachTime <positive_integer>] [-ndRetransmissionTime
<positive_integer>] [-natprefix <ipv6_addr|*>] [-doDAD ( ENABLED | DISABLED )]
```

Description

Sets the IPv6-related parameters: RA Learning and IPv6 NAT Prefix.

Parameters

rlearning

Enable the NetScaler appliance to learn about various routes from Router Advertisement (RA) and Router Solicitation (RS) messages sent by the routers. Possible values: ENABLED, DISABLED Default value: DISABLED

routerRedirection

Enable the NetScaler appliance to do Router Redirection. Possible values: ENABLED, DISABLED Default value: DISABLED

ndBasereachTime

ND6 base reachable time (ms) Default value: 30000

ndRetransmissionTime

ND6 retransmission time (ms) Default value: 1000

natprefix

Prefix used for translating packets from private IPv6 servers to IPv4 packets. This prefix has a length of 96 bits (128-32 = 96). The IPv6 servers embed the destination IP address of the IPv4 servers or hosts in the last 32 bits of the destination IP address field of the IPv6 packets. The first 96 bits of the destination IP address field are set as the IPv6 NAT prefix. IPv6 packets addressed to this prefix have to be routed to the NetScaler appliance to ensure that the IPv6-IPv4 translation is done by the appliance.

doDAD

Enable the NetScaler appliance to do Duplicate Address Detection(DAD) for all the IPv6 addresses configured on NS, regardless of whether they are obtained through stateless autoconfiguration .DHCPv6, or manual configuration. RFC4862-sec 5.4. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

```
set ipv6 -natprefix 2000::/96
```

[Top](#)

unset ipv6

Synopsis

```
unset ipv6 [-ralearning] [-routerRedirection] [-ndBasereachTime] [-ndRetransmissionTime] [-natprefix] [-doDAD]
```

Description

Use this command to remove ipv6 settings. Refer to the set ipv6 command for meanings of the arguments.

[Top](#)

show ipv6

Synopsis

```
show ipv6
```

Description

Display IPv6 settings

Example

```
show ipv6
```

[Top](#)

ipTunnelParam

[[set](#) | [unset](#) | [show](#)]

set ipTunnelParam

Synopsis

```
set ipTunnelParam [-srcIP <ip_addr>] [-dropFrag ( YES | NO )] [-dropFragCpuThreshold <positive_integer>] [-srcIPRoundRobin ( YES | NO )]
```

Description

Sets global parameters of IPv4 tunnels on the NetScaler appliance.

Parameters

srcIP

Common source-IP address for all tunnels. For a specific tunnel, this global setting is overridden if you have specified another source IP address. Must be a MIP or SNIP address.

dropFrag

Drop any IP packet that requires fragmentation before it is sent through the tunnel. Possible values: YES, NO Default value: NO

dropFragCpuThreshold

Threshold value, as a percentage of CPU usage, at which to drop packets that require fragmentation to use the IP tunnel. Applies only if dropFragparameter is set to NO. The default value, 0, specifies that this parameter is not set. Minimum value: 1 Maximum value: 100

srcIPRoundRobin

Use a different source IP address for each new session through a particular IP tunnel, as determined by round robin selection of one of the SNIP addresses. This setting is ignored if a common global source IP address has been specified for all the IP tunnels. This setting does not apply to a tunnel for which a source IP address has been specified. Possible values: YES, NO Default value: NO

Example

```
set ipTunnelParam -srcIP 10.100.20.48 -dropFrag
YES -dropFragCpuThreshold 95
```

[Top](#)

unset ipTunnelParam

Synopsis

```
unset ipTunnelParam [-srcIP] [-dropFrag] [-dropFragCpuThreshold] [-srcIPRoundRobin]
```

Description

Use this command to remove ipTunnelParam settings. Refer to the set ipTunnelParam command for meanings of the arguments.

[Top](#)

show ipTunnelParam

Synopsis

```
show ipTunnelParam
```

Description

Display the IP Tunnel global settings on the NetScaler

Example

```
Tunnel Source IP: 10.100.20.48
Drop if Fragmentation Needed: YES
CPU usage threshold to avoid fragmentation: 95
```

[Top](#)

ip6TunnelParam

[[set](#) | [unset](#) | [show](#)]

set ip6TunnelParam

Synopsis

```
set ip6TunnelParam [-srcIP <ipv6_addr|null>] [-dropFrag ( YES | NO )] [-
dropFragCpuThreshold <positive_integer>] [-srcIPRoundRobin ( YES | NO )]
```

Description

Sets global parameters of IPv6 tunnels on the NetScaler appliance.

Parameters

srcIP

Common source IPv6 address for all IPv6 tunnels. Must be a SNIP6 or VIP6 address.

dropFrag

Drop any packet that requires fragmentation. Possible values: YES, NO Default value: NO

dropFragCpuThreshold

Threshold value, as a percentage of CPU usage, at which to drop packets that require fragmentation. Applies only if dropFragparameter is set to NO. Minimum value: 1
Maximum value: 100

srcIPRoundRobin

Use a different source IPv6 address for each new session through a particular IPv6 tunnel, as determined by round robin selection of one of the SNIP6 addresses. This setting is ignored if a common global source IPv6 address has been specified for all the IPv6 tunnels. This setting does not apply to a tunnel for which a source IPv6 address has been specified. Possible values: YES, NO Default value: NO

Example

```
set ip6TunnelParam -srcIP 9901::100 -dropFrag YES -
dropFragCpuThreshold 95
```

[Top](#)

unset ip6TunnelParam

Synopsis

```
unset ip6TunnelParam [-srcIP] [-dropFrag] [-dropFragCpuThreshold] [-srcIPRoundRobin]
```

Description

Resets the specified global parameters of IPv6 tunnels to their default settings. Refer to the set ip6TunnelParam command for parameter descriptions..Refer to the set ip6TunnelParam command for meanings of the arguments.

Example

```
unset ip6TunnelParam -srcIP -dropFrag -
dropFragCpuThreshold
```

[Top](#)

show ip6TunnelParam

Synopsis

```
show ip6TunnelParam
```

Description

Displays the global settings of IPv6 tunnels on the NetScaler appliance.

Example

```
Tunnel Source IP: 9901::100
Drop if Fragmentation Needed: YES
CPU usage threshold to avoid fragmentation: 95
```

[Top](#)

L2Param

[[set](#) | [unset](#) | [show](#)]

set L2Param

Synopsis

```
set L2Param [-mbfPeermacUpdate <positive_integer>] [-maxBridgeCollision
<positive_integer>] [-bdggrpProxyArp ( ENABLED | DISABLED )] [-bdgSetting ( ENABLED |
DISABLED )] [-garpOnVridIntf ( ENABLED | DISABLED )] [-macModeFwdMyPkt
( ENABLED | DISABLED )] [-useMyMAC ( ENABLED | DISABLED )] [-proxyArp ( ENABLED |
DISABLED )] [-garpReply ( ENABLED | DISABLED )] [-mbfInstLearning ( ENABLED |
DISABLED )] [-rstIntfOnHaFo ( ENABLED | DISABLED )] [-skipProxyingBsdTraffic
( ENABLED | DISABLED )] [-returnToEthernetSender ( ENABLED | DISABLED )]
```

Description

Set Layer 2 related global settings on the NetScaler

Parameters

mbfPeermacUpdate

When mbf_instant_learning is enabled, learn any changes in peer's MAC after this time interval, which is in 10ms ticks. Default value: 10

maxBridgeCollision

Maximum bridge collision for loop detection Default value: 20

bdggrpProxyArp

Set/reset proxy ARP in bridge group deployment Possible values: ENABLED, DISABLED
Default value: ENABLED

bdgSetting

Bridging settings for C2C behavior Possible values: ENABLED, DISABLED Default value: DISABLED

garpOnVridIntf

Send GARP messages on VRID-configured interfaces upon failover Possible values: ENABLED, DISABLED Default value: ENABLED

macModeFwdMyPkt

MAC mode vserver forward packets destined to VIPs. Possible values: ENABLED, DISABLED Default value: DISABLED

useMyMAC

Set/reset cfg_use_my_mac Possible values: ENABLED, DISABLED Default value: DISABLED

proxyArp

Set/reset cfg_proxy_arp_dr Possible values: ENABLED, DISABLED Default value: ENABLED

garpReply

Set/reset REPLY form of GARP Possible values: ENABLED, DISABLED Default value: DISABLED

mbfInstLearning

Enable instant learning of MAC changes in MBF mode. Possible values: ENABLED, DISABLED Default value: DISABLED

rstIntfOnHaFo

Enable the reset interface upon HA failover. Possible values: ENABLED, DISABLED
Default value: DISABLED

skipProxyingBsdTraffic

Enable the proxying of FreeBSD traffic. Possible values: ENABLED, DISABLED Default value: DISABLED

returnToEthernetSender

Return to ethernet sender. Possible values: ENABLED, DISABLED Default value: DISABLED

[Top](#)

unset L2Param

Synopsis

```
unset L2Param [-mbfPeermacUpdate] [-maxBridgeCollision] [-bdggrpProxyArp] [-bdgSetting] [-garpOnVridIntf] [-macModeFwdMyPkt] [-useMyMAC] [-proxyArp] [-garpReply] [-mbfInstLearning] [-rstIntfOnHaFo] [-skipProxyingBsdTraffic] [-returnToEthernetSender]
```

Description

Use this command to remove L2Param settings. Refer to the set L2Param command for meanings of the arguments.

[Top](#)

show L2Param

Synopsis

```
show L2Param
```

Description

Displays the settings of global Layer 2 parameters on the NetScaler appliance.

[Top](#)

L3Param

[[set](#) | [unset](#) | [show](#)]

set L3Param

Synopsis

```
set L3Param [-srcnat ( ENABLED | DISABLED )] [-icmpGenRateThreshold <positive_integer>] [-overrideRnat ( ENABLED | DISABLED )] [-dropDFFlag ( ENABLED | DISABLED )] [-mipRoundRobin ( ENABLED | DISABLED )] [-externalLoopBack ( ENABLED | DISABLED )] [-tnlPmtuWoConn ( ENABLED | DISABLED )] [-usipServerStrayPkt ( ENABLED | DISABLED )] [-forwardICMPFragments ( ENABLED | DISABLED )] [-dropIPFragments ( ENABLED | DISABLED )] [-AclLogTime <positive_integer>]
```

Description

Set Layer 3 related global settings on the NetScaler

Parameters

srcnat

Perform NAT if only the source is in the private network Possible values: ENABLED, DISABLED Default value: ENABLED

icmpGenRateThreshold

NS generated ICMP pkts per 10ms rate threshold Default value: 100

overrideRnat

USNIP/USIP settings override RNAT settings for configured service/virtual server traffic.. Possible values: ENABLED, DISABLED Default value: DISABLED

dropDFFlag

Enable dropping the IP DF flag. Possible values: ENABLED, DISABLED Default value: DISABLED

mipRoundRobin

Enable round robin usage of mapped IPs. Possible values: ENABLED, DISABLED Default value: ENABLED

externalLoopBack

Enable external loopback. Possible values: ENABLED, DISABLED Default value: DISABLED

tnIPmtuWoConn

Enable external loopback. Possible values: ENABLED, DISABLED Default value: ENABLED

usipServerStrayPkt

Enable detection of stray server side pkts in USIP mode. Possible values: ENABLED, DISABLED Default value: DISABLED

forwardICMPFragments

Enable forwarding of ICMP fragments. Possible values: ENABLED, DISABLED Default value: DISABLED

dropIPFragments

Enable dropping of IP fragments. Possible values: ENABLED, DISABLED Default value: DISABLED

AcLogTime

Parameter to tune acl logging time Default value: 5000

[Top](#)

unset L3Param

Synopsis

```
unset L3Param [-srcnat] [-icmpGenRateThreshold] [-overrideRnat] [-dropDFFlag] [-mipRoundRobin] [-externalLoopBack] [-tnIPmtuWoConn] [-usipServerStrayPkt] [-forwardICMPFragments] [-dropIPFragments] [-AcLogTime]
```

Description

Use this command to remove L3Param settings. Refer to the set L3Param command for meanings of the arguments.

[Top](#)

show L3Param

Synopsis

```
show L3Param
```

Description

Displays the settings of global Layer 3 parameters.

[Top](#)

forwardingSession

[[add](#) | [set](#) | [rm](#) | [show](#)]

add forwardingSession

Synopsis

```
add forwardingSession <name> ((<network> [<netmask>]) | -acl6name <string> | -  
aclname <string>) [-connfailover ( ENABLED | DISABLED )]
```

Description

Adds a forwarding session rule, which creates forwarding-session entries for traffic that originates from or is destined for a particular network and is forwarded by the NetScaler appliance. By default, the appliance does not create session entries for traffic that only forwards (L3 mode). Add a forwarding session rule for a case in which a client request that the appliance forwards to a server results in a response that has to return by the same path

Parameters

name

Name for the forwarding session rule. Can begin with a letter, number, or the underscore character (_), and can consist of letters, numbers, and the hyphen (-), period (.) pound (#), space (), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the rule is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my rule" or 'my rule').

network

Network address from which the forwarded traffic originates or to which it is destined.

acl6name

Name of any configured ACL6 whose action is ALLOW. The rule of the ACL6 is used as an forwarding session rule.

aclname

Name of an extended ACL with action set to ALLOW. The rule specified in the ACL is used as a forwarding-session rule.

connfailover

Synchronize connection information with the secondary appliance in a high availability (HA) pair. That is, synchronize all connection-related information for the forwarding session. Possible values: ENABLED, DISABLED Default value: DISABLED

[Top](#)

set forwardingSession

Synopsis

set forwardingSession <name> [-connfailover (ENABLED | DISABLED)]

Description

Modifies parameters of a forwarding session rule.

Parameters

name

Name of the forwarding session rule. Required for identifying the forwarding session rule.

connfailover

Synchronize connection information with the secondary appliance in a high availability (HA) pair. That is, synchronize all connection-related information for the forwarding session. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

```
set forwardsession fw1 -connfailover enabled.
```

[Top](#)

rm forwardingSession

Synopsis

rm forwardingSession <name>

Description

Removes a forwarding session rule from the NetScaler appliance.

Parameters

name

Name of the forwarding session rule to be removed.

Example

```
rm forwardsession name.
```

[Top](#)

show forwardingSession

Synopsis

show forwardingSession [<name>]

Description

Displays the settings of all forwarding session rules configured on the NetScaler appliance, or of the specified forwarding session rule.

Parameters

name

Name of the forwarding session rule whose details you want to display.

[Top](#)

ptp

[[set](#) | [show](#)]

set ptp

Synopsis

set ptp -state (DISABLE | ENABLE)

Description

Specifies whether to use Precision Time Protocol (PTP) to synchronize time across cluster nodes. This command is applicable in a cluster setup only. If you do not want to use PTP, you must disable PTP, by using this command, and instead enable NTP.

Parameters

state

Enables or disables Precision Time Protocol (PTP) on the appliance. If you disable PTP, make sure you enable Network Time Protocol (NTP) on the cluster. Possible values: DISABLE, ENABLE Default value: NSA_PTP_ENABLE

[Top](#)

show ptp

Synopsis

show ptp

Description

Displays the status of Precision Time Protocol (PTP) on the appliance.

[Top](#)

rnat6

[[add](#) | [bind](#) | [unbind](#) | [set](#) | [unset](#) | [clear](#) | [show](#)]

add rnat6

Synopsis

add rnat6 <name> (<network> | (<acl6name> [-redirectPort <port>]))

Description

Adds a Reverse Network Address Translation (RNAT6) rule for IPv6 traffic. When an IPv6 packet generated by a server matches the conditions specified in the RNAT6 rule, the appliance replaces the source IPv6 address of the IPv6 packet with a configured NAT IPv6 address before forwarding it to the destination.

Parameters

name

Name for the RNAT6 rule. Must begin with a letter, number, or the underscore character (_), and can consist of letters, numbers, and the hyphen (-), period (.), pound (#), space (), at sign (@), equals (=), colon (:), and underscore characters. Cannot be changed after the rule is created. Choose a name that helps identify the RNAT6 rule.

network

IPv6 address of the network on whose traffic you want the NetScaler appliance to do RNAT processing.

acl6name

Name of any configured ACL6 whose action is ALLOW. The rule of the ACL6 is used as an RNAT6 rule.

Example

```
add rnat6 rnat6_name 2002::/64
```

[Top](#)

bind rnat6

Synopsis

```
bind rnat6 <name> <natIP6>@ ...
```

Description

Binds specified IPv6 NAT IPs to an RNAT6 rule.

Parameters

name

Name of the RNAT6 rule to which to bind NAT IPs.

natIP6

One or more IP addresses to be bound to the IP set.

Example

```
bind rnat6 <rnat6_name> <natIP6>@ ...
```

[Top](#)

unbind rnat6

Synopsis

`unbind rnat6 <name> <natIP6>@ ...`

Description

Unbinds the associated NAT IPv6 address(es) from an RNAT6 rule.

Parameters

name

Name of the RNAT6 rule from which to unbind the associated NAT IP address(es).

natIP6

IP address, or multiple addresses, to be unbound from the RNAT6 rule. (If using the CLI, use spaces to separate multiple addresses.)

Example

```
unbind rnat6 <rnat6_name> <natIP6>@ ...
```

[Top](#)

set rnat6

Synopsis

`set rnat6 <name> [-redirectPort <port>]`

Description

Modifies the specified parameters of an RNAT6 rule.

Parameters

name

Name of the RNAT6 rule. Required for identifying the RNAT6 rule and cannot be modified.

redirectPort

Port number to which the IPv6 packets are redirected. Applicable to TCP and UDP protocols. Minimum value: 1 Maximum value: 65535

[Top](#)

unset rnat6

Synopsis

`unset rnat6 <name> [-redirectPort]`

Description

Resets the specified parameters of an RNAT6 rule to their default settings. Refer to the set rnat6 command for parameter descriptions..Refer to the set rnat6 command for meanings of the arguments.

[Top](#)

clear rnat6

Synopsis

clear rnat6 <name>

Description

Removes an RNAT6 rule from the NetScaler appliance.

Parameters

name

Name of the RNAT6 rule to be removed.

[Top](#)

show rnat6

Synopsis

show rnat6 [<name>]

Description

Displays the settings of all RNAT6 rules configured on the NetScaler appliance, or of the specified RNAT6 rule.

Parameters

name

Name of the RNAT6 rule whose details you want to display.

[Top](#)

inatparam

[[set](#) | [unset](#) | [show](#)]

set inatparam

Synopsis

set inatparam [-nat46v6Prefix <ipv6_addr|*>] [-nat46IgnoreTOS (YES | NO)] [-nat46ZeroChecksum (ENABLED | DISABLED)] [-nat46v6Mtu <positive_integer>] [-nat46FragHeader (ENABLED | DISABLED)]

Description

Set the inat parameter

Parameters

nat46v6Prefix

The prefix used for translating packets received from private IPv6 servers into IPv4 packets. This prefix has a length of 96 bits ($128 - 32 = 96$). The IPv6 servers embed the destination IP address of the IPv4 servers or hosts in the last 32 bits of the destination IP address field of the IPv6 packets. The first 96 bits of the destination IP address field are set as the IPv6 NAT prefix. IPv6 packets addressed to this prefix have to be routed to the NetScaler appliance to ensure that the IPv6-IPv4 translation is done by the appliance.

nat46IgnoreTOS

Ignore TOS. Possible values: YES, NO Default value: NO

nat46ZeroChecksum

Calculate checksum for UDP packets with zero checksum Possible values: ENABLED, DISABLED Default value: ENABLED

nat46v6Mtu

Calculate checksum for UDP packets with zero checksum Default value: 1280
Minimum value: 1280 Maximum value: 1500

nat46FragHeader

When disabled, translator will not insert IPv6 fragmentation header for non fragmented IPv4 packets Possible values: ENABLED, DISABLED Default value: ENABLED

Example

```
set inat parameter -nat46ignoretos YES
```

[Top](#)

unset inatparam

Synopsis

```
unset inatparam -nat46v6Prefix
```

Description

Use this command to remove inatparam settings. Refer to the set inatparam command for meanings of the arguments.

[Top](#)

show inatparam

Synopsis

```
show inatparam
```

Description

Show the inat parameters.

Example

```
show inat params
```

[Top](#)

nat64

[[add](#) | [set](#) | [unset](#) | [rm](#) | [stat](#) | [show](#)]

add nat64

Synopsis

```
add nat64 <name> <acl6name> [-netProfile <string>]
```

Description

Configure a nat64 rule on the appliance.

Parameters

name

Name of NAT64 rule.

acl6name

The ACL6 name.

netProfile

The name of the network profile.

[Top](#)

set nat64

Synopsis

```
set nat64 <name> [-acl6name <string>] [-netProfile <string>]
```

Description

Set the configured nat64 rule.

Parameters

name

Name of NAT64 rule.

acl6name

The ACL6 name.

netProfile

The name of the network profile.

Example

```
set nat64 rule1 -acl6name acl1 .
```

[Top](#)**unset nat64****Synopsis**

```
unset nat64 <name> -netProfile
```

Description

Use this command to remove nat64 settings. Refer to the set nat64 command for meanings of the arguments.

[Top](#)**rm nat64****Synopsis**

```
rm nat64 <name>
```

Description

Remove the configured nat64 rule.

Parameters**name**

Name of NAT64 rule.

Example

```
rm nat64 name.
```

[Top](#)**stat nat64****Synopsis**

```
stat nat64 [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile  
<input_filename>] [-clearstats ( basic | full )]
```

Description

Display statistics for nat64 sessions.

Parameters**clearstats**

Clear the statistics / counters Possible values: basic, full

Example

```
stat nat64
```

[Top](#)

show nat64

Synopsis

```
show nat64 [<name>]
```

Description

Display the nat64 configuration.

Parameters

name
Name of NAT64 rule.

[Top](#)

rsskeytype

[[set](#) | [show](#)]

set rsskeytype

Synopsis

```
set rsskeytype -rsstype ( ASYMMETRIC | SYMMETRIC )
```

Parameters

rsstype
Type of RSS key, possible values ASYMMETRIC and SYMMETRIC. Possible values:
ASYMMETRIC, SYMMETRIC Default value: NSA_RSSKEY_ASYM

[Top](#)

show rsskeytype

Synopsis

```
show rsskeytype
```

[Top](#)

tunnelip

stat tunnelip

Synopsis

```
stat tunnelip [<tunnelip>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile  
<input_filename>] [-clearstats ( basic | full )]
```

Description

Display the statistics related to IP tunnel.

Parameters

tunnelip

remote IP address of the configured tunnel.

clearstats

Clear the statistics / counters Possible values: basic, full

Example

```
stat tunnelip 2.1.1.1
```

tunnelip6

stat tunnelip6

Synopsis

```
stat tunnelip6 [<tunnelip6>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile  
<input_filename>] [-clearstats ( basic | full )]
```

Description

Display the statistics related to IP tunnel.

Parameters

tunnelip6

remote IPv6 address of the configured tunnel.

clearstats

Clear the statistics / counters Possible values: basic, full

Example

```
stat tunnelip6 2001::1
```

L4Param

[[set](#) | [unset](#) | [show](#)]

set L4Param

Synopsis

set L4Param [-l2ConnMethod <l2ConnMethod>] [-l4switch (ENABLED | DISABLED)]

Description

Set Layer 4 related global settings on the NetScaler

Example

```
set l4param
```

[Top](#)

unset L4Param

Synopsis

unset L4Param [-l2ConnMethod] [-l4switch]

Description

Use this command to remove L4Param settings. Refer to the set L4Param command for meanings of the arguments.

[Top](#)

show L4Param

Synopsis

show L4Param

Description

Displays the settings of global Layer 4 parameters.

[Top](#)

vpath

[[add](#) | [rm](#) | [show](#) | [stat](#)]

add vpath

Synopsis

add vpath <name> [-destIP <ip_addr|ipv6_addr|*>] [-encapMode <encapMode>]

Description

Adds Vpath destination IP to which packets need to be Vpath injected.

Parameters

name

Name for the vpath. Must begin with a letter, number, or the underscore character (_), and can consist of letters, numbers, and the hyphen (-), period (.) pound (#), space (), at sign (@), equals (=), colon (:), and underscore characters. Cannot be changed after the profile is created. Choose a name that helps identify the net profile.

destIP

The IP address assigned to the VLAN.

encapMode

Encapsulation mode (L2/L3). Possible values: L2, L3, DISABLE

Example

```
add vpath vpath1 -destip 10.102.1.10
```

[Top](#)

rm vpath

Synopsis

rm vpath <name> ...

Description

Remove Vpath destination IP.

Parameters

name

Name of the vpath to be removed.

Example

```
rm netProfile prof1
```

[Top](#)

show vpath

Synopsis

show vpath [<name>]

Description

List down all Vpath destination IPs.

Parameters

name

Name of the vpath whose details you want to display.

Example

```
show vpath
```

[Top](#)

stat vpath

Synopsis

```
stat vpath [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile  
<input_filename>] [-clearstats ( basic | full )]
```

Description

Display Vpath statistics.

Parameters

clearstats

Clear the statistics / counters Possible values: basic, full

[Top](#)

vPathParam

[[set](#) | [unset](#) | [show](#)]

set vPathParam

Synopsis

```
set vPathParam -srcIP <ip_addr>
```

Description

Sets the global parameters for vPath

Parameters

srcIP

source-IP address used for all vpath L3 encapsulations. Must be a MIP or SNIP address.

Example

```
set vpathparam -srcip 2.2.2.2
```

[Top](#)

unset vPathParam

Synopsis

```
unset vPathParam -srcIP
```

Description

Use this command to remove vPathParam settings. Refer to the set vPathParam command for meanings of the arguments.

[Top](#)

show vPathParam

Synopsis

```
show vPathParam
```

Description

Display the global parameters for vPath

Example

```
show vpathparam
```

[Top](#)

NS Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [shutdown](#)
- ♦ [reboot](#)
- ♦ [ns](#)
- ♦ [ns limitIdentifier](#)
- ♦ [ns acl](#)
- ♦ [ns acl6](#)
- ♦ [ns ip6](#)
- ♦ [ns ip](#)
- ♦ [ns simpleacl](#)
- ♦ [ns simpleacl6](#)
- ♦ [ns pbr](#)
- ♦ [ns xmlnsnamespace](#)

- ◆ [ns tcpProfile](#)
- ◆ [ns httpProfile](#)
- ◆ [ns stats](#)
- ◆ [ns ns.conf](#)
- ◆ [ns savedConfig](#)
- ◆ [ns runningConfig](#)
- ◆ [ns acls](#)
- ◆ [ns info](#)
- ◆ [ns license](#)
- ◆ [ns version](#)
- ◆ [ns config](#)
- ◆ [ns param](#)
- ◆ [ns acls6](#)
- ◆ [ns pbrs](#)
- ◆ [ns connectiontable](#)
- ◆ [ns limitSessions](#)
- ◆ [ns hostName](#)
- ◆ [ns surgeQ](#)
- ◆ [ns feature](#)
- ◆ [ns mode](#)
- ◆ [ns dhcpParams](#)
- ◆ [ns dhcpIp](#)
- ◆ [ns spParams](#)
- ◆ [ns tcpbufParam](#)
- ◆ [ns tcpParam](#)
- ◆ [ns httpParam](#)
- ◆ [ns weblogparam](#)
- ◆ [ns diameter](#)
- ◆ [ns rateControl](#)
- ◆ [ns rpcNode](#)
- ◆ [ns timeout](#)
- ◆ [ns hardware](#)

- ♦ [ns events](#)
- ♦ [ns encryptionParams](#)
- ♦ [ns rollbackcmd](#)
- ♦ [ns memory](#)
- ♦ [ns pbr6](#)
- ♦ [ns trafficDomain](#)
- ♦ [ns consoleloginprompt](#)
- ♦ [ns timer](#)
- ♦ [ns aptlicense](#)

shutdown

shutdown

Synopsis

shutdown

Description

Stops all operations and powers off the NetScaler appliance. Note: * When a standalone NetScaler appliance is shut down, the unsaved configurations (configurations performed since the last 'save ns config' command was issued) are lost. * In a high availability setup, when the primary appliance is shut down, the secondary appliance takes over and becomes the primary. The unsaved configurations from the old primary are available on the new primary appliance. * In a cluster setup, this command can be executed only through the cluster IP address and it shuts down only the configuration coordinator.

reboot

reboot

Synopsis

reboot [-warm]

Description

Restarts the NetScaler appliance. Note: * When a standalone NetScaler appliance is rebooted, the unsaved configurations (configurations performed since the last 'save ns config' command was issued) are lost. * In the high availability mode, when the primary appliance is rebooted, the secondary system takes over and becomes the primary. The unsaved configurations from the old primary are available on the new primary appliance. * In a cluster setup, this command can be executed only through the cluster IP address and it reboots only the configuration coordinator.

Parameters

warm

Restarts the NetScaler software without rebooting the underlying operating system. The session terminates and you must log on to the appliance after it has restarted. Note: This argument is required only for nCore appliances. Classic appliances ignore this argument.

ns

[[config](#) | [stat](#)]

config ns

Synopsis

config ns

Description

Displays a menu to configure the basic parameters of a NetScaler appliance. Note: The appliance must be rebooted for these changes to take effect.

[Top](#)

stat ns

Synopsis

stat ns [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-clearstats (basic | full)]

Description

Displays generic statistics of the NetScaler appliance.

Parameters

clearstats

Clear the statistics / counters Possible values: basic, full

[Top](#)

ns limitIdentifier

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#) | [stat](#)]

add ns limitIdentifier

Synopsis

add ns limitIdentifier <limitIdentifier> [-threshold <positive_integer>] [-timeSlice <positive_integer>] [-mode <mode> [-limitType (BURSTY | SMOOTH)]] [-selectorName <string>] [-maxBandwidth <positive_integer>] [-trapsInTimeSlice <positive_integer>]

Description

Adds a limit identifier to check if the amount of traffic exceeds a specified value, within a particular time interval.

Parameters

limitIdentifier

Name for a rate limit identifier. Must begin with an ASCII letter or underscore (_) character, and must consist only of ASCII alphanumeric or underscore characters. Reserved words must not be used.

threshold

Maximum number of requests that are allowed in the given timeslice when requests (mode is set as REQUEST_RATE) are tracked per timeslice. When connections (mode is set as CONNECTION) are tracked, it is the total number of connections that would be let through. Default value: 1 Minimum value: 1

timeSlice

Time interval, in milliseconds, specified in multiples of 10, during which requests are tracked to check if they cross the threshold. This argument is needed only when the mode is set to REQUEST_RATE. Default value: 1000 Minimum value: 10

mode

Defines the type of traffic to be tracked. * REQUEST_RATE - Tracks requests/ timeslice. * CONNECTION - Tracks active transactions. Examples 1. To permit 20 requests in 10 ms and 2 traps in 10 ms: add limitIdentifier limit_req -mode request_rate -limitType smooth -timeslice 1000 -Threshold 2000 -trapsInTimeSlice 200 2. To permit 50 requests in 10 ms: set limitIdentifier limit_req -mode request_rate -timeslice 1000 -Threshold 5000 -limitType smooth 3. To permit 1 request in 40 ms: set limitIdentifier limit_req -mode request_rate -timeslice 2000 -Threshold 50 -limitType smooth 4. To permit 1 request in 200 ms and 1 trap in 130 ms: set limitIdentifier limit_req -mode request_rate -timeslice 1000 -Threshold 5 -limitType smooth -trapsInTimeSlice 8 5. To permit 5000 requests in 1000 ms and 200 traps in 1000 ms: set limitIdentifier limit_req -mode request_rate -timeslice 1000 -Threshold 5000 -limitType BURSTY Possible values: CONNECTION, REQUEST_RATE, NONE Default value: PEMGMT_RLT_MODE_REQ_RATE

limitType

Smooth or bursty request type. * SMOOTH - When you want the permitted number of requests in a given interval of time to be spread evenly across the timeslice * BURSTY - When you want the permitted number of requests to exhaust the quota anytime within the timeslice. This argument is needed only when the mode is set to REQUEST_RATE. Possible values: BURSTY, SMOOTH Default value: PEMGMT_RLT_REQ_RATE_TYPE_BURSTY

selectorName

Name of the rate limit selector. If this argument is NULL, rate limiting will be applied on all traffic received by the virtual server or the NetScaler (depending on whether the limit identifier is bound to a virtual server or globally) without any filtering.

maxBandwidth

Maximum bandwidth permitted, in kbps. Maximum value: 4294967287

trapsInTimeSlice

Number of traps to be sent in the timeslice configured. A value of 0 indicates that traps are disabled. Maximum value: 65535

Example

```
add ns limitIdentifier limit_id -threshold 2 -
timeSlice 5000 -mode CONNECTION -selectorName
sel_1 -maxBandwidth 24 -trapsInTimeSlice 8
```

[Top](#)

rm ns limitIdentifier

Synopsis

```
rm ns limitIdentifier <limitIdentifier>
```

Description

Removes a rate limit identifier from the appliance.

Parameters

limitIdentifier

Name of the rate limit identifier to be removed.

Example

```
rm ns limitIdentifier limit_id
```

[Top](#)

set ns limitIdentifier

Synopsis

```
set ns limitIdentifier <limitIdentifier> [-threshold <positive_integer>] [-timeSlice
<positive_integer>] [-mode <mode> [-limitType ( BURSTY | SMOOTH )]] [-selectorName
<string>] [-maxBandwidth <positive_integer>] [-trapsInTimeSlice <positive_integer>]
```

Description

Modifies the attributes of a rate limit identifier.

Parameters

limitIdentifier

Name of the rate limit identifier to be modified.

threshold

Maximum number of requests that are allowed in the given timeslice when requests (mode is set as REQUEST_RATE) are tracked per timeslice. When connections (mode

is set as CONNECTION) are tracked, it is the total number of connections that would be let through. Default value: 1 Minimum value: 1

timeSlice

Time interval, in milliseconds, specified in multiples of 10, during which requests are tracked to check if they cross the threshold. This argument is needed only when the mode is set to REQUEST_RATE. Default value: 1000 Minimum value: 10

mode

Defines the type of traffic to be tracked. * REQUEST_RATE - Tracks requests/ timeslice. * CONNECTION - Tracks active transactions. Examples 1. To permit 20 requests in 10 ms and 2 traps in 10 ms: add limitIdentifier limit_req -mode request_rate -limitType smooth -timeslice 1000 -Threshold 2000 -trapsInTimeSlice 200 2. To permit 50 requests in 10 ms: set limitIdentifier limit_req -mode request_rate -timeslice 1000 -Threshold 5000 -limitType smooth 3. To permit 1 request in 40 ms: set limitIdentifier limit_req -mode request_rate -timeslice 2000 -Threshold 50 -limitType smooth 4. To permit 1 request in 200 ms and 1 trap in 130 ms: set limitIdentifier limit_req -mode request_rate -timeslice 1000 -Threshold 5 -limitType smooth -trapsInTimeSlice 8 5. To permit 5000 requests in 1000 ms and 200 traps in 1000 ms: set limitIdentifier limit_req -mode request_rate -timeslice 1000 -Threshold 5000 -limitType BURSTY Possible values: CONNECTION, REQUEST_RATE, NONE Default value: PEMGMT_RLT_MODE_REQ_RATE

selectorName

Name of the rate limit selector. If this argument is NULL, rate limiting will be applied on all traffic received by the virtual server or the NetScaler (depending on whether the limit identifier is bound to a virtual server or globally) without any filtering.

maxBandwidth

Maximum bandwidth permitted, in kbps. Maximum value: 4294967287

trapsInTimeSlice

Number of traps to be sent in the timeslice configured. A value of 0 indicates that traps are disabled. Maximum value: 65535

Example

```
set ns limitIdentifier limit_id -threshold 2 -
timeSlice 5000 -mode CONNECTION -selectorName
sel_1 -maxBandwidth 24 -trapsInTimeSlice 8
```

[Top](#)

unset ns limitIdentifier

Synopsis

```
unset ns limitIdentifier <limitIdentifier> [-selectorName] [-threshold] [-timeSlice] [-
mode] [-limitType] [-maxBandwidth] [-trapsInTimeSlice]
```

Description

Use this command to remove ns limitIdentifier settings. Refer to the set ns limitIdentifier command for meanings of the arguments.

[Top](#)

show ns limitIdentifier

Synopsis

show ns limitIdentifier [<limitIdentifier>]

Description

Displays information about a rate limit identifier.

Parameters

limitIdentifier

Name of the rate limit identifier about which to display information. If a name is not provided, information about all rate limit identifiers is shown.

Example

```
show ns limitIdentifier limit_id
```

[Top](#)

stat ns limitIdentifier

Synopsis

stat ns limitIdentifier [<name> [<pattern> ...]] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-clearstats (basic | full)] [-sortBy Hits [<sortOrder>]]

Description

Display statistics of a identifier.

Parameters

name

The name of the identifier.

pattern

Pattern for the selector field, ? means field is required, * means field value does not matter, anything else is a regular pattern

clearstats

Clear the statistics / counters Possible values: basic, full

sortBy

use this argument to sort by specific key Possible values: Hits

[Top](#)

ns acl

[[add](#) | [rm](#) | [set](#) | [unset](#) | [enable](#) | [disable](#) | [stat](#) | [rename](#) | [show](#)]

add ns acl

Synopsis

```
add ns acl <aclname> <aclaction> [-td <positive_integer>] [-srcIP [<operator>]
<srcIPVal>] [-srcPort [<operator>] <srcPortVal>] [-destIP [<operator>] <destIPVal>] [-
destPort [<operator>] <destPortVal>] [-TTL <positive_integer>] [-srcMac <mac_addr>]
[(-protocol <protocol> [-established]) | -protocolNumber <positive_integer>] [-vlan
<positive_integer>] [-interface <interface_name>] [-icmpType <positive_integer> [-
icmpCode <positive_integer>]] [-priority <positive_integer>] [-state ( ENABLED |
DISABLED )] [-logstate ( ENABLED | DISABLED ) [-ratelimit <positive_integer>]]
```

Description

Adds an extended ACL rule to the NetScaler appliance. To commit this operation, you must apply the extended ACLs. Extended ACL rules filter data packets on the basis of various parameters, such as IP address, source port, action, and protocol.

Parameters

aclname

Name for the extended ACL rule. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the extended ACL rule is created.

aclaction

Action to perform on incoming IPv4 packets that match the extended ACL rule. Available settings function as follows: * ALLOW - The NetScaler appliance processes the packet. * BRIDGE - The NetScaler appliance bridges the packet to the destination without processing it. * DENY - The NetScaler appliance drops the packet. Possible values: BRIDGE, DENY, ALLOW

td

Traffic Domain Id. Maximum value: 4094

srcIP

IP address or range of IP addresses to match against the source IP address of an incoming IPv4 packet. In the command line interface, separate the range with a hyphen and enclose within brackets. For example: [10.102.29.30-10.102.29.189].

srcPort

Port number or range of port numbers to match against the source port number of an incoming IPv4 packet. In the command line interface, separate the range with a hyphen and enclose within brackets. For example: [40-90].

destIP

IP address or range of IP addresses to match against the destination IP address of an incoming IPv4 packet. In the command line interface, separate the range with a hyphen and enclose within brackets. For example: [10.102.29.30-10.102.29.189].

destPort

Port number or range of port numbers to match against the destination port number of an incoming IPv4 packet. In the command line interface, separate the range with a hyphen and enclose within brackets. For example: [40-90]. Note: The destination port can be specified only for TCP and UDP protocols.

TTL

Number of seconds, in multiples of four, after which the extended ACL rule expires. If you do not want the extended ACL rule to expire, do not specify a TTL value. Minimum value: 1 Maximum value: 2147483647

srcMac

MAC address to match against the source MAC address of an incoming IPv4 packet.

protocol

Protocol to match against the protocol of an incoming IPv4 packet. Possible values: ICMP, IGMP, TCP, EGP, IGP, ARGUS, UDP, RDP, RSVP, EIGRP, L2TP, ISIS

protocolNumber

Protocol to match against the protocol of an incoming IPv4 packet. Minimum value: 1 Maximum value: 255

vlan

ID of the VLAN. The NetScaler appliance applies the ACL rule only to the incoming packets of the specified VLAN. If you do not specify a VLAN ID, the appliance applies the ACL rule to the incoming packets on all VLANs. Minimum value: 1 Maximum value: 4094

interface

ID of an interface. The NetScaler appliance applies the ACL rule only to the incoming packets from the specified interface. If you do not specify any value, the appliance applies the ACL rule to the incoming packets of all interfaces.

established

Allow only incoming TCP packets that have the ACK or RST bit set, if the action set for the ACL rule is ALLOW and these packets match the other conditions in the ACL rule.

icmpType

ICMP Message type to match against the message type of an incoming ICMP packet. For example, to block DESTINATION UNREACHABLE messages, you must specify 3 as the ICMP type. Note: This parameter can be specified only for the ICMP protocol. Maximum value: 65536

icmpCode

Code of a particular ICMP message type to match against the ICMP code of an incoming ICMP packet. For example, to block DESTINATION HOST UNREACHABLE messages, specify 3 as the ICMP type and 1 as the ICMP code. If you set this parameter, you must set the ICMP Type parameter. Maximum value: 65536

priority

Priority for the extended ACL rule that determines the order in which it is evaluated relative to the other extended ACL rules. If you do not specify priorities while creating extended ACL rules, the ACL rules are evaluated in the order in which they are created. Minimum value: 1 Maximum value: 100000

state

Enable or disable the extended ACL rule. After you apply the extended ACL rules, the NetScaler appliance compares incoming packets against the enabled extended ACL rules. Possible values: ENABLED, DISABLED Default value: XACLENABLED

logstate

Enable or disable logging of events related to the extended ACL rule. The log messages are stored in the configured syslog or auditlog server. Possible values: ENABLED, DISABLED Default value: GENDISABLED

ratelimit

Maximum number of log messages to be generated per second. If you set this parameter, you must enable the Log State parameter. Default value: 100 Minimum value: 1 Maximum value: 10000

Example

```
add ns acl restrict DENY -srcport 45-1024 -destIP
192.168.1.1 -protocol TCP
```

[Top](#)**rm ns acl****Synopsis**

```
rm ns acl <aclname> ...
```

Description

Removes an extended ACL rule from the NetScaler appliance. To commit this operation, you must apply the extended ACLs.

Parameters**aclname**

Name of the extended ACL rule that you want to remove.

Example

```
rm ns acl restrict
```

[Top](#)

set ns acl

Synopsis

```
set ns acl <aclname> [-aclaction <aclaction>] [-srcIP [<operator>] <srcIPVal>] [-srcPort  
[<operator>] <srcPortVal>] [-destIP [<operator>] <destIPVal>] [-destPort [<operator>]  
<destPortVal>] [-srcMac <mac_addr>] [-protocol <protocol> | -protocolNumber  
<positive_integer>] [-icmpType <positive_integer>] [-icmpCode <positive_integer>]] [-  
vlan <positive_integer>] [-interface <interface_name>] [-priority <positive_integer>] [-  
logstate ( ENABLED | DISABLED )] [-ratelimit <positive_integer>] [-established]
```

Description

Modifies the parameters of an ACL rule. To commit this operation, you must apply the extended ACLs.

Parameters

aclname

Name of the ACL rule whose parameters you want to modify.

aclaction

Action to perform on incoming IPv4 packets that match the extended ACL rule. Available settings function as follows: * ALLOW - The NetScaler appliance processes the packet. * BRIDGE - The NetScaler appliance bridges the packet to the destination without processing it. * DENY - The NetScaler appliance drops the packet. Possible values: BRIDGE, DENY, ALLOW

srcIP

IP address or range of IP addresses to match against the source IP address of an incoming IPv4 packet. In the command line interface, separate the range with a hyphen and enclose within brackets. For example: [10.102.29.30-10.102.29.189].

srcPort

Port number or range of port numbers to match against the source port number of an incoming IPv4 packet. In the command line interface, separate the range with a hyphen and enclose within brackets. For example: [40-90].

destIP

IP address or range of IP addresses to match against the destination IP address of an incoming IPv4 packet. In the command line interface, separate the range with a hyphen and enclose within brackets. For example: [10.102.29.30-10.102.29.189].

destPort

Port number or range of port numbers to match against the destination port number of an incoming IPv4 packet. In the command line interface, separate the range with a hyphen and enclose within brackets. For example: [40-90]. Note: The destination port can be specified only for TCP and UDP protocols.

srcMac

MAC address to match against the source MAC address of an incoming IPv4 packet.

protocol

Protocol to match against the protocol of an incoming IPv4 packet. Possible values: ICMP, IGMP, TCP, EGP, IGP, ARGUS, UDP, RDP, RSVP, EIGRP, L2TP, ISIS

protocolNumber

Protocol to match against the protocol of an incoming IPv4 packet. Minimum value: 1
Maximum value: 255

icmpType

ICMP Message type to match against the message type of an incoming ICMP packet. For example, to block DESTINATION UNREACHABLE messages, you must specify 3 as the ICMP type. Note: This parameter can be specified only for the ICMP protocol. Maximum value: 65536

vlan

ID of the VLAN. The NetScaler appliance applies the ACL rule only to the incoming packets of the specified VLAN. If you do not specify a VLAN ID, the appliance applies the ACL rule to the incoming packets on all VLANs. Minimum value: 1 Maximum value: 4094

interface

ID of an interface. The NetScaler appliance applies the ACL rule only to the incoming packets from the specified interface. If you do not specify any value, the appliance applies the ACL rule to the incoming packets of all interfaces.

priority

Priority for the extended ACL rule that determines the order in which it is evaluated relative to the other extended ACL rules. If you do not specify priorities while creating extended ACL rules, the ACL rules are evaluated in the order in which they are created. Minimum value: 1 Maximum value: 100000

logstate

Enable or disable logging of events related to the extended ACL rule. The log messages are stored in the configured syslog or auditlog server. Possible values: ENABLED, DISABLED Default value: GENDISABLED

established

Allow only incoming TCP packets that have the ACK or RST bit set, if the action set for the ACL rule is ALLOW and these packets match the other conditions in the ACL rule.

Example

```
set ns acl restrict -srcPort 50
```

[Top](#)

unset ns acl**Synopsis**

```
unset ns acl <aclname> [-srcIP] [-srcPort] [-destIP] [-destPort] [-srcMac] [-protocol] [-icmpType] [-icmpCode] [-vlan] [-interface] [-logstate] [-ratelimit] [-established]
```

Description

Resets the attributes of the specified extended ACL rule. Attributes for which a default value is available revert to their default values. Refer to the `set ns acl` command for a description of the parameters..Refer to the `set ns acl` command for meanings of the arguments.

Example

```
unset ns acl rule1 -srcPort
```

[Top](#)

enable ns acl

Synopsis

`enable ns acl <aclname> ...`

Description

Enables an extended ACL rule. To commit this operation, you must apply the extended ACLs. After you apply the extended ACL rules, the NetScaler appliance compares incoming packets against the enabled extended ACL rules.

Parameters

aclname

Name of the extended ACL rule that you want to enable.

Example

```
enable ns acl foo
```

[Top](#)

disable ns acl

Synopsis

`disable ns acl <aclname> ...`

Description

Disables an extended ACL rule. To commit this operation, you must apply the extended ACLs. After you apply the ACL rules, the NetScaler appliance does not compare incoming packets against the disabled extended ACL rules.

Parameters

aclname

Name of the extended ACL rule that you want to disable.

Example

```
disable ns acl foo
```

[Top](#)

stat ns acl

Synopsis

```
stat ns acl [<aclname>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile  
<input_filename>] [-clearstats ( basic | full )]
```

Description

Displays statistics related to the extended ACL rules. To display statistics of all the extended ACL rules, run the command without any parameters. To display statistics of a particular extended ACL rule, specify the name of the extended ACL rule.

Parameters

aclname

Name of the extended ACL rule whose statistics you want the NetScaler appliance to display.

clearstats

Clear the statistics / counters Possible values: basic, full

Example

```
stat acl
```

[Top](#)

rename ns acl

Synopsis

```
rename ns acl <aclname> <newName>
```

Description

Renames an extended ACL rule.

Parameters

aclname

Name of the extended ACL rule that you want to rename.

newName

New name for the extended ACL rule. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

Example

```
rename acl rule rule-new
```

[Top](#)

show ns acl

Synopsis

```
show ns acl [<aclname>]
```

Description

Displays settings related to the extended ACL rules. To display settings of all the extended ACL rules, run the command without any parameters. To display settings of a particular extended ACL rule, specify the name of the extended ACL rule.

Parameters

aclname

Name of the extended ACL rule whose details you want the NetScaler appliance to display.

Example

```
sh acl foo
  TD: 100
  Name: foo
Action: ALLOW      Hits: 0
  srcIP = 10.102.1.150
  destIP = 202.54.12.47
  srcMac:
Protocol: TCP
  srcPort
destPort = 110
  Vlan:
Interface:
  Active Status: ENABLED
Applied Status: NOTAPPLIED
  Priority: 1027
```

[Top](#)

ns acl6

[[add](#) | [rm](#) | [set](#) | [unset](#) | [enable](#) | [disable](#) | [stat](#) | [rename](#) | [show](#)]

add ns acl6

Synopsis

```
add ns acl6 <acl6name> <acl6action> [-td <positive_integer>] [-srcIPv6 [<operator>]
<srcIPv6Val>] [-srcPort [<operator>] <srcPortVal>] [-destIPv6 [<operator>]
<destIPv6Val>] [-destPort [<operator>] <destPortVal>] [-TTL <positive_integer>] [-
srcMac <mac_addr>] [(-protocol <protocol> [-established]) | -protocolNumber
<positive_integer>] [-vlan <positive_integer>] [-interface <interface_name>] [-
icmpType <positive_integer> [-icmpCode <positive_integer>]] [-priority
<positive_integer>] [-state ( ENABLED | DISABLED )]
```

Description

Adds an ACL6 rule to the NetScaler appliance. To commit this operation, you must apply the ACL6s. ACL6 rules filter data packets on the basis of various parameters, such as IP address, source port, action, and protocol.

Parameters

acl6name

Name for the ACL6 rule. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the ACL6 rule is created.

acl6action

Action to perform on the incoming IPv6 packets that match the ACL6 rule. Available settings function as follows: * ALLOW - The NetScaler appliance processes the packet. * BRIDGE - The NetScaler appliance bridges the packet to the destination without processing it. * DENY - The NetScaler appliance drops the packet. Possible values: BRIDGE, DENY, ALLOW

td

Traffic Domain Id. Maximum value: 4094

srcIPv6

IP address or range of IP addresses to match against the source IP address of an incoming IPv6 packet. In the command line interface, separate the range with a hyphen and enclose within brackets.

srcPort

Port number or range of port numbers to match against the source port number of an incoming IPv6 packet. In the command line interface, separate the range with a hyphen and enclose within brackets. For example: [40-90]. Note: The destination port can be specified only for TCP and UDP protocols.

destIPv6

IP address or range of IP addresses to match against the destination IP address of an incoming IPv6 packet. In the command line interface, separate the range with a hyphen and enclose within brackets.

destPort

Port number or range of port numbers to match against the destination port number of an incoming IPv6 packet. In the command line interface, separate the range with

a hyphen and enclose within brackets. For example: [40-90]. Note: The destination port can be specified only for TCP and UDP protocols.

TTL

Time to expire this ACL6 (in seconds). Minimum value: 1 Maximum value: 2147483647

srcMac

MAC address to match against the source MAC address of an incoming IPv6 packet.

protocol

Protocol, identified by protocol name, to match against the protocol of an incoming IPv6 packet. Possible values: ICMPV6, TCP, UDP

protocolNumber

Protocol, identified by protocol number, to match against the protocol of an incoming IPv6 packet. Minimum value: 1 Maximum value: 255

vlan

ID of the VLAN. The NetScaler appliance applies the ACL6 rule only to the incoming packets on the specified VLAN. If you do not specify a VLAN ID, the appliance applies the ACL6 rule to the incoming packets on all VLANs. Minimum value: 1 Maximum value: 4094

interface

ID of an interface. The NetScaler appliance applies the ACL6 rule only to the incoming packets from the specified interface. If you do not specify any value, the appliance applies the ACL6 rule to the incoming packets from all interfaces.

established

Allow only incoming TCP packets that have the ACK or RST bit set if the action set for the ACL6 rule is ALLOW and these packets match the other conditions in the ACL6 rule.

icmpType

ICMP Message type to match against the message type of an incoming IPv6 ICMP packet. For example, to block DESTINATION UNREACHABLE messages, you must specify 3 as the ICMP type. Note: This parameter can be specified only for the ICMP protocol. Maximum value: 65536

icmpCode

Code of a particular ICMP message type to match against the ICMP code of an incoming IPv6 ICMP packet. For example, to block DESTINATION HOST UNREACHABLE messages, specify 3 as the ICMP type and 1 as the ICMP code. If you set this parameter, you must set the ICMP Type parameter. Maximum value: 65536

priority

Priority for the ACL6 rule, which determines the order in which it is evaluated relative to the other ACL6 rules. If you do not specify priorities while creating ACL6 rules, the ACL6 rules are evaluated in the order in which they are created. Minimum value: 1 Maximum value: 80000

state

State of the ACL6. Possible values: ENABLED, DISABLED Default value: XACLENABLED

Example

```
add ns acl6 rule1 DENY -srcport 45-1024 -destIPv6
2001::45 -protocol TCP
```

[Top](#)**rm ns acl6****Synopsis**

```
rm ns acl6 <acl6name> ...
```

Description

Removes an ACL6 rule from the NetScaler appliance. To commit this operation, you must apply the ACL6s.

Parameters**acl6name**

Name of the ACL6 rule that you want to remove.

Example

```
rm ns acl6 rule1
```

[Top](#)**set ns acl6****Synopsis**

```
set ns acl6 <acl6name> [-aclaction <aclaction>] [-srcIPv6 [<operator>] <srcIPv6Val>] [-
srcPort [<operator>] <srcPortVal>] [-destIPv6 [<operator>] <destIPv6Val>] [-destPort
<operator>] <destPortVal>] [-srcMac <mac_addr>] [-protocol <protocol> | -
protocolNumber <positive_integer>] [-icmpType <positive_integer>] [-icmpCode
<positive_integer>]] [-vlan <positive_integer>] [-interface <interface_name>] [-priority
<positive_integer>] [-established]
```

Description

Modifies the parameters of an ACL6 rule. To commit this operation, you must apply the ACL6s.

Parameters**acl6name**

Name of the ACL6 rule whose parameters you want to modify.

aclaction

Action associated with the ACL6. Possible values: BRIDGE, DENY, ALLOW

srcIPv6

IP address or range of IP addresses to match against the source IP address of an incoming IPv6 packet. In the command line interface, separate the range with a hyphen and enclose within brackets.

srcPort

Source Port (range).

destIPv6

IP address or range of IP addresses to match against the destination IP address of an incoming IPv6 packet. In the command line interface, separate the range with a hyphen and enclose within brackets.

destPort

Destination Port (range).

srcMac

MAC address to match against the source MAC address of an incoming IPv6 packet.

protocol

Protocol, identified by protocol name, to match against the protocol of an incoming IPv6 packet. Possible values: ICMPV6, TCP, UDP

protocolNumber

Protocol, identified by protocol number, to match against the protocol of an incoming IPv6 packet. Minimum value: 1 Maximum value: 255

icmpType

ICMP Message type to match against the message type of an incoming IPv6 ICMP packet. For example, to block DESTINATION UNREACHABLE messages, you must specify 3 as the ICMP type. Note: This parameter can be specified only for the ICMP protocol. Maximum value: 65536

vlan

ID of the VLAN. The NetScaler appliance applies the ACL6 rule only to the incoming packets on the specified VLAN. If you do not specify a VLAN ID, the appliance applies the ACL6 rule to the incoming packets on all VLANs. Minimum value: 1 Maximum value: 4094

interface

ID of an interface. The NetScaler appliance applies the ACL6 rule only to the incoming packets from the specified interface. If you do not specify any value, the appliance applies the ACL6 rule to the incoming packets from all interfaces.

priority

Priority for the ACL6 rule, which determines the order in which it is evaluated relative to the other ACL6 rules. If you do not specify priorities while creating ACL6 rules, the ACL6 rules are evaluated in the order in which they are created. Minimum value: 1 Maximum value: 80000

established

Allow only incoming TCP packets that have the ACK or RST bit set if the action set for the ACL6 rule is ALLOW and these packets match the other conditions in the ACL6 rule.

Example

```
set ns acl6 rule1 -srcPort 50
```

[Top](#)**unset ns acl6****Synopsis**

```
unset ns acl6 <acl6name> [-srcIPv6] [-srcPort] [-destIPv6] [-destPort] [-srcMac] [-protocol] [-icmpType] [-icmpCode] [-vlan] [-interface] [-established]
```

Description

Resets the attributes of the specified ACL6 rule. To commit this operation, you must apply the ACL6s. Attributes for which a default value is available revert to their default values. Refer to the set ns acl6 command for descriptions of the parameters..Refer to the set ns acl6 command for meanings of the arguments.

Example

```
unset ns acl6 rule1 -srcPort
```

[Top](#)**enable ns acl6****Synopsis**

```
enable ns acl6 <acl6name> ...
```

Description

Enables an ACL6 rule. To commit this operation, you must apply the ACL6s. After you apply the ACL6 rules, the NetScaler appliance compares incoming IPv6 packets to the enabled ACL6 rules.

Parameters**acl6name**

Name of ACL6 rule that you want to enable.

Example

```
enable ns acl6 rule1
```

[Top](#)

disable ns acl6

Synopsis

disable ns acl6 <acl6name> ...

Description

Disables an ACL6 rule. To commit this operation, you must apply the ACL6s. After you apply the ACL6 rules, the NetScaler appliance does not compare incoming IPv6 packets to the disabled ACL6 rules.

Parameters

acl6name

Name of ACL6 rule that you want to disable.

Example

```
disable ns acl6 rule1
```

[Top](#)

stat ns acl6

Synopsis

stat ns acl6 [<acl6name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-clearstats (basic | full)]

Description

Displays statistics related to the ACL6 rules. To display statistics of all the ACL6 rules, run the command without any parameters. To display statistics of a particular ACL6 rule, specify the name of the ACL6 rule.

Parameters

acl6name

Name of the ACL6 rule whose statistics you want the NetScaler appliance to display.

clearstats

Clear the statistics / counters Possible values: basic, full

Example

```
stat acl6
```

[Top](#)

rename ns acl6

Synopsis

```
rename ns acl6 <acl6name> <newName>
```

Description

Renames an ACL6 rule. To commit this operation, you must apply the ACL6s.

Parameters

acl6name

Name of the ACL6 rule that you want to rename.

newName

New name for the ACL6 rule. Must begin with an ASCII alphabetic or underscore \(_\) character, and must contain only ASCII alphanumeric, underscore, hash \(\#\), period \(\.\), space, colon \(:\), at \(@\), equals \(\=\), and hyphen \(-\) characters.

Example

```
rename acl6 rule rule-new
```

[Top](#)

show ns acl6

Synopsis

```
show ns acl6 [<acl6name>]
```

Description

Displays settings related to the ACL6 rules. To display settings of all the ACL6 rules, run the command without any parameters. To display settings of a particular ACL6 rule, specify the name of the ACL6 rule.

Parameters

acl6name

Name of the ACL6 rule whose details you want the NetScaler appliance to display.

Example

```
show ns acl6 rule1
1)      Name: r1                      Action:
DENY
      srcIPv6 = 2001::1
      destIPv6
      srcMac:
Protocol:
      Vlan:
Interface:
```

Active Status: ENABLED	Applied
Status: NOTAPPLIED	
Priority: 10	Hits: 0
TTL:	

[Top](#)

ns ip6

[\[add | rm | set | unset | show \]](#)

add ns ip6

Synopsis

```
add ns ip6 <IPv6Address>@ [-scope ( global | link-local )] [-type <type> [-hostRoute
( ENABLED | DISABLED ) [-ip6hostRtGw <ipv6_addr|*>] [-metric <integer>] [-
vserverRHILevel <vserverRHILevel>] [-ospf6LSAType ( INTRA_AREA | EXTERNAL ) [-
ospfArea <positive_integer>]]] ] [-vlan <positive_integer>] [-nd ( ENABLED | DISABLED )]
[-icmp ( ENABLED | DISABLED )] [-vServer ( ENABLED | DISABLED )] [-telnet ( ENABLED |
DISABLED )] [-ftp ( ENABLED | DISABLED )] [-gui <gui>] [-ssh ( ENABLED | DISABLED )] [-
snmp ( ENABLED | DISABLED )] [-mgmtAccess ( ENABLED | DISABLED )] [-restrictAccess
( ENABLED | DISABLED )] [-dynamicRouting ( ENABLED | DISABLED )] [-state ( DISABLED
| ENABLED )] [-map <ip_addr>] [-ownerNode <positive_integer>] [-td
<positive_integer>]
```

Description

Creates an IPv6 address on the NetScaler appliance.

Parameters

IPv6Address

IPv6 address to create on the NetScaler appliance.

scope

Scope of the IPv6 address to be created. Cannot be changed after the IP address is created. Possible values: global, link-local Default value: NS_GLOBAL

type

Type of IP address to be created on the NetScaler appliance. Cannot be changed after the IP address is created. Possible values: NSIP, VIP, SNIP, GSLBsiteIP, ADNSsvcIP, CLIP Default value: NS_IPV6_SNIP

vlan

The VLAN number. Maximum value: 4094

nd

Respond to Neighbor Discovery (ND) requests for this IP address. Possible values: ENABLED, DISABLED Default value: ENABLED

icmp

Respond to ICMP requests for this IP address. Possible values: ENABLED, DISABLED Default value: ENABLED

vServer

Enable or disable the state of all the virtual servers associated with this VIP6 address. Possible values: ENABLED, DISABLED Default value: ENABLED

telnet

Allow Telnet access to this IP address. Possible values: ENABLED, DISABLED Default value: ENABLED

ftp

Allow File Transfer Protocol (FTP) access to this IP address. Possible values: ENABLED, DISABLED Default value: ENABLED

gui

Allow graphical user interface (GUI) access to this IP address. Possible values: ENABLED, SECUREONLY, DISABLED Default value: ENABLED

ssh

Allow secure Shell (SSH) access to this IP address. Possible values: ENABLED, DISABLED Default value: ENABLED

snmp

Allow Simple Network Management Protocol (SNMP) access to this IP address. Possible values: ENABLED, DISABLED Default value: ENABLED

mgmtAccess

Allow access to management applications on this IP address. Possible values: ENABLED, DISABLED Default value: DISABLED

restrictAccess

Block access to nonmanagement applications on this IP address. This option is applicable for MIP6s, SNIP6s, and NSIP6s, and is disabled by default. Nonmanagement applications can run on the underlying NetScaler Free BSD operating system. Possible values: ENABLED, DISABLED Default value: DISABLED

dynamicRouting

Allow dynamic routing on the IP address. Specific to SNIP6 address. Possible values: ENABLED, DISABLED Default value: DISABLED

hostRoute

Advertise a route for the VIP6 address by using the dynamic routing protocols running on the NetScaler appliance. Possible values: ENABLED, DISABLED

ip6hostRtGw

IPv6 address of the gateway for the route.

metric

Integer value to add to or subtract from the cost of the route advertised for the VIP6 address. Minimum value: -16777215

vserverRHILevel

Advertise or do not advertise the route for the Virtual IP (VIP6) address on the basis of the state of the virtual servers associated with that VIP6. * NONE - Advertise the route for the VIP6 address, irrespective of the state of the virtual servers associated with the address. * ONE VSERVER - Advertise the route for the VIP6 address if at least one of the associated virtual servers is in UP state. * ALL VSERVER - Advertise the

route for the VIP6 address if all of the associated virtual servers are in UP state.
Possible values: ONE_VSERVER, ALL_VSERVERS, NONE Default value: RHI_STATE_ONE

ospf6LSAType

Type of LSAs to be used by the IPv6 OSPF protocol, running on the NetScaler appliance, for advertising the route for the VIP6 address. Possible values: INTRA_AREA, EXTERNAL Default value: DISABLED

ospfArea

ID of the area in which the Intra-Area-Prefix LSAs are to be advertised for the VIP6 address by the IPv6 OSPF protocol running on the NetScaler appliance. Default value: -1 Maximum value: 4294967294LU

state

Enable or disable the IP address. Possible values: DISABLED, ENABLED Default value: ENABLED

map

Mapped IPV4 address for the IPV6 address.

ownerNode

ID of the cluster node for which you are adding the IP address. Must be used if you want the IP address to be active only on the specific node. Can be configured only through the cluster IP address. Cannot be changed after the IP address is created. Default value: 255

td

Traffic Domain Id Maximum value: 4094

Example

```
add ns ip6 2001::a/96 -scope GLOBAL
```

[Top](#)

rm ns ip6

Synopsis

```
rm ns ip6 <IPv6Address>@ [-td <positive_integer>]
```

Description

Removes an IPv6 address configured on the NetScaler appliance.

Parameters

IPv6Address

IPv6 address that you want to remove.

td

Traffic Domain Id Maximum value: 4094

Example

```
rm ns ip6 2002::5
```

[Top](#)

set ns ip6

Synopsis

```
set ns ip6 (<IPv6Address>@ [-td <positive_integer>]) [-nd ( ENABLED | DISABLED )] [-icmp ( ENABLED | DISABLED )] [-vServer ( ENABLED | DISABLED )] [-telnet ( ENABLED | DISABLED )] [-ftp ( ENABLED | DISABLED )] [-gui <gui>] [-ssh ( ENABLED | DISABLED )] [-snmp ( ENABLED | DISABLED )] [-mgmtAccess ( ENABLED | DISABLED )] [-restrictAccess ( ENABLED | DISABLED )] [-state ( DISABLED | ENABLED )] [-map <ip_addr>] [-dynamicRouting ( ENABLED | DISABLED )] [-hostRoute ( ENABLED | DISABLED )] [-ip6hostRtGw <ip6v6_addr|*>] [-metric <integer>] [-vserverRHILevel <vserverRHILevel>] [-ospf6LSAType ( INTRA_AREA | EXTERNAL ) [-ospfArea <positive_integer>]]]
```

Description

Modifies the specified parameters of an IPv6 address configured on the NetScaler appliance.

Parameters

IPv6Address

IPv6 address whose parameters you want to modify.

nd

The state of ND responses for the entity. Possible values: ENABLED, DISABLED Default value: ENABLED

icmp

The state of ICMP responses for the entity. Possible values: ENABLED, DISABLED Default value: ENABLED

vServer

The state of vserver attribute for this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

telnet

The state of telnet access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

ftp

The state of ftp access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

gui

The state of GUI access to this IP entity. Possible values: ENABLED, SECUREONLY, DISABLED Default value: ENABLED

ssh

The state of SSH access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

snmp

The state of SNMP access to this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

mgmtAccess

The state of management access to this IP entity. Possible values: ENABLED, DISABLED Default value: DISABLED

restrictAccess

Status of ports not used for management access (blocked/open) for the entity. Possible values: ENABLED, DISABLED Default value: DISABLED

state

Enable or disable the IP address. Possible values: DISABLED, ENABLED Default value: ENABLED

map

Mapped IPV4 address for the IPV6 address.

dynamicRouting

Allow dynamic routing on the IP address. Specific to SNIP6 address. Possible values: ENABLED, DISABLED Default value: DISABLED

hostRoute

Advertise a route for the VIP6 address by using the dynamic routing protocols running on the NetScaler appliance. Possible values: ENABLED, DISABLED

Example

```
set ns ip6 2001::a -map 10.102.33.27
```

[Top](#)

unset ns ip6

Synopsis

```
unset ns ip6 <IPv6Address>@ [-td <positive_integer>] [-nd] [-icmp] [-vServer] [-telnet] [-ftp] [-gui] [-ssh] [-snmp] [-mgmtAccess] [-restrictAccess] [-state] [-map] [-dynamicRouting] [-hostRoute] [-ip6hostRtGw] [-metric] [-vserverRHILevel] [-ospf6LSAType] [-ospfArea]
```

Description

Use this command to remove ns ip6 settings. Refer to the set ns ip6 command for meanings of the arguments.

[Top](#)

show ns ip6

Synopsis

```
show ns ip6 [<IPv6Address> [-td <positive_integer>]]
```

Description

Displays settings of all the IPv6 addresses or of the specified IPv6 address configured on the NetScaler appliance. To display settings of all the IPv6 addresses, run the command without any parameters. To display settings of a particular IPv6 address, specify the IPv6 address.

Parameters

IPv6Address

IPv6 address whose settings you want the NetScaler appliance to display.

Example

```
show ns ip6
```

[Top](#)

ns ip

[[add](#) | [rm](#) | [set](#) | [unset](#) | [enable](#) | [disable](#) | [show](#)]

add ns ip

Synopsis

```
add ns ip <IPAddress>@ <netmask> [-type <type> [-hostRoute ( ENABLED | DISABLED ) [-hostRtGw <ip_addr>] [-metric <integer>] [-vserverRHILevel <vserverRHILevel>] [-ospfLSAType ( TYPE1 | TYPE5 ) [-ospfArea <positive_integer>]]] ] [-arp ( ENABLED | DISABLED )] [-icmp ( ENABLED | DISABLED )] [-vServer ( ENABLED | DISABLED )] [-telnet ( ENABLED | DISABLED )] [-ftp ( ENABLED | DISABLED )] [-gui <gui>] [-ssh ( ENABLED | DISABLED )] [-snmp ( ENABLED | DISABLED )] [-mgmtAccess ( ENABLED | DISABLED )] [-restrictAccess ( ENABLED | DISABLED )] [-dynamicRouting ( ENABLED | DISABLED )] [-state ( ENABLED | DISABLED )] [-vrID <positive_integer>] [-icmpResponse <icmpResponse>] [-ownerNode <positive_integer>] [-arpResponse <arpResponse>] [-td <positive_integer>]
```

Description

Creates an IPv4 address on the NetScaler appliance.

Parameters

IPAddress

IPv4 address to create on the NetScaler appliance. Cannot be changed after the IP address is created.

netmask

Subnet mask associated with the IP address.

type

Type of the IP address to create on the NetScaler appliance. Cannot be changed after the IP address is created. Possible values: SNIP, VIP, MIP, NSIP, GSLBsiteIP, CLIP Default value: NSADDR_SNIP

arp

Respond to respond to ARP requests for this IP address. Possible values: ENABLED, DISABLED Default value: ENABLED

icmp

Respond to ICMP requests for this IP address. Possible values: ENABLED, DISABLED Default value: ENABLED

vServer

Use this option to set (enable or disable) the vserver attribute for this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

telnet

Allow Telnet access to this IP address. Possible values: ENABLED, DISABLED Default value: ENABLED

ftp

Allow File Transfer Protocol (FTP) access to this IP address. Possible values: ENABLED, DISABLED Default value: ENABLED

gui

Allow graphical user interface (GUI) access to this IP address. Possible values: ENABLED, SECUREONLY, DISABLED Default value: ENABLED

ssh

Allow secure shell (SSH) access to this IP address. Possible values: ENABLED, DISABLED Default value: ENABLED

snmp

Allow Simple Network Management Protocol (SNMP) access to this IP address. Possible values: ENABLED, DISABLED Default value: ENABLED

mgmtAccess

Allow access to management applications on this IP address. Possible values: ENABLED, DISABLED Default value: DISABLED

restrictAccess

Block access to nonmanagement applications on this IP. This option is applicable for MIPs, SNIPs, and NSIP, and is disabled by default. Nonmanagement applications can run on the underlying NetScaler Free BSD operating system. Possible values: ENABLED, DISABLED Default value: DISABLED

dynamicRouting

Allow dynamic routing on the IP address. Specific to SNIP addresses. Possible values: ENABLED, DISABLED Default value: DISABLED

ospf

Use this option to enable or disable OSPF on this IP address for the entity. Possible values: ENABLED, DISABLED Default value: DISABLED

bgp

Use this option to enable or disable BGP on this IP address for the entity. Possible values: ENABLED, DISABLED Default value: DISABLED

rip

Use this option to enable or disable RIP on this IP address for the entity. Possible values: ENABLED, DISABLED Default value: DISABLED

hostRoute

Advertise a route for the VIP address, using the dynamic routing protocols running on the NetScaler appliance. Possible values: ENABLED, DISABLED

hostRtGw

IP address of the gateway for the route. Default value: -1

metric

Integer value to add to or subtract from the cost of the route advertised for the VIP address. Minimum value: -16777215

vserverRHILevel

Advertise the route for the Virtual IP (VIP) address on the basis of the state of the virtual servers associated with that VIP. * NONE - Advertise the route for the VIP address, regardless of the state of the virtual servers associated with the address. * ONE VSERVER - Advertise the route for the VIP address if at least one of the associated virtual servers is in UP state. * ALL VSERVER - Advertise the route for the VIP address if all of the associated virtual servers are in UP state. Possible values: ONE_VSERVER, ALL_VSERVERS, NONE Default value: RHI_STATE_ONE

ospfLSAType

Type of LSAs to be used by the OSPF protocol, running on the NetScaler appliance, for advertising the route for this VIP address. Possible values: TYPE1, TYPE5 Default value: DISABLED

ospfArea

ID of the area in which the Type1 LSAs are to be advertised for this VIP address by the OSPF protocol running on the NetScaler appliance. Default value: -1 Maximum value: 4294967294LU

state

Enable or disable the IP address. Possible values: ENABLED, DISABLED Default value: ENABLED

vrID

ID, which uniquely identifies a VMAC address, to bind to a VIP address. This binding is used to set up NetScaler appliances in an active-active configuration using VRRP. Minimum value: 1 Maximum value: 255

icmpResponse

Respond to ICMP requests for a Virtual IP (VIP) address on the basis of the states of the virtual servers associated with that VIP. Available settings function as follows: * NONE - The NetScaler appliance responds to any ICMP request for the VIP address,

irrespective of the states of the virtual servers associated with the address. * ONE VSERVER - The NetScaler appliance responds to any ICMP request for the VIP address if at least one of the associated virtual servers is in UP state. * ALL VSERVER - The NetScaler appliance responds to any ICMP request for the VIP address if all of the associated virtual servers are in UP state. * VSVR_CNTRLD - The behavior depends on the ICMP VSERVER RESPONSE setting on all the associated virtual servers. The following settings can be made for the ICMP VSERVER RESPONSE parameter on a virtual server: * If you set ICMP VSERVER RESPONSE to PASSIVE on all virtual servers, NetScaler always responds. * If you set ICMP VSERVER RESPONSE to ACTIVE on all virtual servers, NetScaler responds if even one virtual server is UP. * When you set ICMP VSERVER RESPONSE to ACTIVE on some and PASSIVE on others, NetScaler responds if even one virtual server set to ACTIVE is UP. Possible values: NONE, ONE_VSERVER, ALL_VSERVERS, VSVR_CNTRLD Default value: NS_IP_NONE

ownerNode

The owner node in a Cluster for this IP address. Owner node can vary from 0 to 31. If ownernode is not specified then the IP is treated as Striped IP. Default value: 255

arpResponse

Respond to ARP requests for a Virtual IP (VIP) address on the basis of the states of the virtual servers associated with that VIP. Available settings function as follows: * NONE - The NetScaler appliance responds to any ARP request for the VIP address, irrespective of the states of the virtual servers associated with the address. * ONE VSERVER - The NetScaler appliance responds to any ARP request for the VIP address if at least one of the associated virtual servers is in UP state. * ALL VSERVER - The NetScaler appliance responds to any ARP request for the VIP address if all of the associated virtual servers are in UP state. Possible values: NONE, ONE_VSERVER, ALL_VSERVERS Default value: NS_IP_NONE

td

Traffic Domain Id Maximum value: 4094

Example

```
add ns ip 10.102.4.123 255.255.255.0
```

[Top](#)

rm ns ip**Synopsis**

```
rm ns ip <IPAddress>@ [-td <positive_integer>]
```

Description

Removes an IPv4 address configured on the NetScaler appliance.

Parameters**IPAddress**

IPv4 address that you want to remove.

td

Traffic Domain Id Maximum value: 4094

Example

```
rm ns ip 10.102.4.123
```

[Top](#)**set ns ip****Synopsis**

```
set ns ip (<IPAddress>@ [-td <positive_integer>]) [-netmask <netmask>] [-arp ( ENABLED
| DISABLED )] [-icmp ( ENABLED | DISABLED )] [-vServer ( ENABLED | DISABLED )] [-
telnet ( ENABLED | DISABLED )] [-ftp ( ENABLED | DISABLED )] [-gui <gui>] [-ssh
( ENABLED | DISABLED )] [-snmp ( ENABLED | DISABLED )] [-mgmtAccess ( ENABLED |
DISABLED )] [-restrictAccess ( ENABLED | DISABLED )] [-dynamicRouting ( ENABLED |
DISABLED )] [-hostRoute ( ENABLED | DISABLED )] [-hostRtGw <ip_addr>] [-metric
<integer>] [-vserverRHILevel <vserverRHILevel>] [-ospfLSAType ( TYPE1 | TYPE5 ) [-
ospfArea <positive_integer>]] [-vrID <positive_integer>] [-icmpResponse
<icmpResponse>] [-arpResponse <arpResponse>]
```

Description

Modifies the parameters of an IPv4 address configured on the NetScaler appliance.

Parameters**IPAddress**

IPv4 address whose parameters you want to modify.

netmask

Subnet mask associated with the IP address.

arp

Respond to respond to ARP requests for this IP address. Possible values: ENABLED, DISABLED Default value: ENABLED

icmp

Respond to ICMP requests for this IP address. Possible values: ENABLED, DISABLED Default value: ENABLED

vServer

Use this option to set (enable or disable) the vserver attribute for this IP entity. Possible values: ENABLED, DISABLED Default value: ENABLED

telnet

Allow Telnet access to this IP address. Possible values: ENABLED, DISABLED Default value: ENABLED

ftp

Allow File Transfer Protocol (FTP) access to this IP address. Possible values: ENABLED, DISABLED Default value: ENABLED

gui

Allow graphical user interface (GUI) access to this IP address. Possible values: ENABLED, SECUREONLY, DISABLED Default value: ENABLED

ssh

Allow secure shell (SSH) access to this IP address. Possible values: ENABLED, DISABLED Default value: ENABLED

snmp

Allow Simple Network Management Protocol (SNMP) access to this IP address. Possible values: ENABLED, DISABLED Default value: ENABLED

mgmtAccess

Allow access to management applications on this IP address. Possible values: ENABLED, DISABLED Default value: DISABLED

restrictAccess

Block access to nonmanagement applications on this IP. This option is applicable for MIPs, SNIPs, and NSIP, and is disabled by default. Nonmanagement applications can run on the underlying NetScaler Free BSD operating system. Possible values: ENABLED, DISABLED Default value: DISABLED

dynamicRouting

Allow dynamic routing on the IP address. Specific to SNIP addresses. Possible values: ENABLED, DISABLED Default value: DISABLED

ospf

The state of OSPF on this IP address for the entity. Possible values: ENABLED, DISABLED Default value: DISABLED

bgp

The state of BGP on this IP address for the entity. Possible values: ENABLED, DISABLED Default value: DISABLED

rip

The state of RIP on this IP address for the entity. Possible values: ENABLED, DISABLED Default value: DISABLED

hostRoute

Advertise a route for the VIP address, using the dynamic routing protocols running on the NetScaler appliance. Possible values: ENABLED, DISABLED

vrID

ID, which uniquely identifies a VMAC address, to bin to a VIP address. This binding is used to set up NetScaler appliances in an active-active configuration using VRRP. Minimum value: 1 Maximum value: 255

icmpResponse

Respond to ICMP requests for a Virtual IP (VIP) address on the basis of the states of the virtual servers associated with that VIP. Available settings function as follows: * NONE - The NetScaler appliance responds to any ICMP request for the VIP address, irrespective of the states of the virtual servers associated with the address. * ONE VSERVER - The NetScaler appliance responds to any ICMP request for the VIP address if at least one of the associated virtual servers is in UP state. * ALL VSERVER - The NetScaler appliance responds to any ICMP request for the VIP address if all of the

associated virtual servers are in UP state. * VSVR_CNTRLD - The behavior depends on the ICMP VSERVER RESPONSE setting on all the associated virtual servers. The following settings can be made for the ICMP VSERVER RESPONSE parameter on a virtual server: * If you set ICMP VSERVER RESPONSE to PASSIVE on all virtual servers, NetScaler always responds. * If you set ICMP VSERVER RESPONSE to ACTIVE on all virtual servers, NetScaler responds if even one virtual server is UP. * When you set ICMP VSERVER RESPONSE to ACTIVE on some and PASSIVE on others, NetScaler responds if even one virtual server set to ACTIVE is UP. Possible values: NONE, ONE_VSERVER, ALL_VSERVERS, VSVR_CNTRLD Default value: NS_IP_NONE

arpResponse

Respond to ARP requests for a Virtual IP (VIP) address on the basis of the states of the virtual servers associated with that VIP. Available settings function as follows: * NONE - The NetScaler appliance responds to any ARP request for the VIP address, irrespective of the states of the virtual servers associated with the address. * ONE VSERVER - The NetScaler appliance responds to any ARP request for the VIP address if at least one of the associated virtual servers is in UP state. * ALL VSERVER - The NetScaler appliance responds to any ARP request for the VIP address if all of the associated virtual servers are in UP state. Possible values: NONE, ONE_VSERVER, ALL_VSERVERS Default value: NS_IP_NONE

Example

```
set ns ip 10.102.4.123 -arp ENABLED
```

[Top](#)

unset ns ip

Synopsis

```
unset ns ip <IPAddress>@ [-td <positive_integer>] [-netmask] [-arp] [-icmp] [-vServer] [-telnet] [-ftp] [-gui] [-ssh] [-snmp] [-mgmtAccess] [-restrictAccess] [-dynamicRouting] [-hostRoute] [-hostRtGw] [-metric] [-vserverRHILevel] [-ospfLSAType] [-ospfArea] [-vrID] [-icmpResponse] [-arpResponse]
```

Description

Use this command to remove ns ip settings. Refer to the set ns ip command for meanings of the arguments.

[Top](#)

enable ns ip

Synopsis

```
enable ns ip (<IPAddress>@ [-td <positive_integer>])
```

Description

Enables the specified IP address configured on the NetScaler appliance.

Parameters

IPAddress

IP address that you want to enable.

Example

```
enable ns ip 10.10.10.10
```

[Top](#)

disable ns ip

Synopsis

disable ns ip (<IPAddress>@ [-td <positive_integer>])

Description

Disables the specified IP address configured on the NetScaler appliance.

Parameters

IPAddress

IP address that you want to disable.

Example

```
disable ns ip 10.10.10.10
```

[Top](#)

show ns ip

Synopsis

show ns ip [<IPAddress> [-td <positive_integer>]] [-type <type>]

Description

Displays settings of all the IPv4 addresses or of the specified IPv4 address configured on the NetScaler appliance. To display settings of all the IPv4 addresses, run the command without any parameters. To display settings of a particular IPv4 address, specify the IPv4 address.

Parameters

IPAddress

IPv4 address whose details you want the NetScaler appliance to display.

type

Display the settings of all IPv4 addresses of a particular type. Possible values: SNIP, VIP, MIP, NSIP, GSLBsiteIP, CLIP

Example

```

show ns ip
Ipaddress      Type      Mode      Arp
Icmp      Vserver  State   Owner
-----
1)10.102.169.16 Cluster IP   Active    Enabled
Enabled NA      Enabled    Configuration
Coordinator
2)10.102.169.18 NetScaler IP Active    Enabled
Enabled NA      Enabled 1
3)10.102.169.19 NetScaler IP Active    Enabled
Enabled NA      Enabled 2
4)10.102.169.17 VIP      Active    Enabled
Enabled Enabled Enabled ALL

```

[Top](#)

ns simpleacl

[\[add | clear | rm | flush | show | stat \]](#)

add ns simpleacl

Synopsis

```
add ns simpleacl <aclname> <aclaction> [-td <positive_integer>] -srcIP <ip_addr> [-
destPort <port> -protocol ( TCP | UDP )] [-TTL <positive_integer>]
```

Description

Adds a simple ACL rule to the NetScaler appliance. Simple ACL rules filter IPv4 packets on the basis of their source IP addresses and, optionally, the destination port and/or protocol. Any packet with the characteristics specified in the simple ACL rule is dropped.

Parameters

aclname

Name for the simple ACL rule. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the simple ACL rule is created.

aclaction

Drop incoming IPv4 packets that match the simple ACL rule. Possible values: DENY

td

Traffic Domain Id. Maximum value: 4094

srcIP

IP address to match against the source IP address of an incoming IPv4 packet.

destPort

Port number to match against the destination port number of an incoming IPv4 packet. Omitting the port number creates an all-ports simple ACL rule, which matches any port. In that case, you cannot create another simple ACL rule specifying a specific port and the same source IPv4 address.

TTL

Number of seconds, in multiples of four, after which the simple ACL rule expires. If you do not want the simple ACL rule to expire, do not specify a TTL value. Minimum value: 4 Maximum value: 2147483647

Example

```
add simpleacl rule1 DENY -srcIP 1.1.1.1 -destPort
80 -protocol TCP
add simpleacl rule2 DENY -srcIP 2.2.2.2 -TTL 600
```

[Top](#)**clear ns simpleacl****Synopsis**

clear ns simpleacl

Description

Removes all simple ACL rules from the NetScaler appliance.

[Top](#)**rm ns simpleacl****Synopsis**

rm ns simpleacl <aclname> ...

Description

Removes a simple ACL rule from the NetScaler appliance.

Parameters

aclname

Name of the simple ACL rule that you want to remove.

Example

```
rm ns simpleacl rule1
```

[Top](#)

flush ns simpleacl

Synopsis

```
flush ns simpleacl -estSessions
```

Description

Terminates all established IPv4 connections that match any of the newly configured simple ACL rules. Note: If you plan to create more than one simple ACL rule and flush existing connections that match any of them, you can minimize the affect on performance by first creating all of the simple ACL rules and then running flush only once.

[Top](#)

show ns simpleacl

Synopsis

```
show ns simpleacl [<aclname>]
```

Description

Displays settings of all the simple ACL rules or of the specified simple ACL rule. To display settings of all the simple ACL rules, run the command without any parameters. To display settings of a particular simple ACL rule, specify the name of the simple ACL rule.

Parameters

aclname

Name of the simple ACL rule whose details you want the NetScaler appliance to display.

Example

```
show simpleacl rule1
  Name: rule1                               Action:
DENY
  srcIP = 10.102.1.150
  Protocol = TCP
DestPort = 110
  Hits: 5                                   TTL:
200 (seconds)
```

[Top](#)

stat ns simpleacl

Synopsis

```
stat ns simpleacl [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile
<input_filename>] [-clearstats ( basic | full )]
```

Description

Displays statistics related to the simple ACL rules.

Parameters

clearstats

Clear the statistics / counters Possible values: basic, full

Example

```
stat simpleacl
```

[Top](#)

ns simpleacl6

[[add](#) | [clear](#) | [flush](#) | [rm](#) | [show](#) | [stat](#)]

add ns simpleacl6

Synopsis

```
add ns simpleacl6 <aclname> [-td <positive_integer>] <aclaction> -srcIPv6 <ipv6_addr|  
null> [-destPort <port> -protocol ( TCP | UDP )] [-TTL <positive_integer>]
```

Description

Adds a simple ACL6 rule to the NetScaler appliance. Simple ACL6 rules filter IPv6 packets on the basis of their source IP addresses and, optionally, the destination port and/or protocol. Any packet with the characteristics specified in the simple ACL6 rule is dropped.

Parameters

aclname

Name for the simple ACL6 rule. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the simple ACL6 rule is created.

td

Traffic Domain Id. Maximum value: 4094

aclaction

Drop incoming IPv6 packets that match the simple ACL6 rule. Possible values: DENY

srcIPv6

IP address to match against the source IP address of an incoming IPv6 packet.

destPort

Port number to match against the destination port number of an incoming IPv6 packet. Omitting the port number creates an all-ports simple ACL6 rule, which

matches any port. In that case, you cannot create another simple ACL6 rule specifying a specific port and the same source IPv6 address.

TTL

Number of seconds, in multiples of four, after which the simple ACL6 rule expires. If you do not want the simple ACL6 rule to expire, do not specify a TTL value. Minimum value: 4 Maximum value: 2147483647

Example

```
add simpleacl6 rule1 DENY -srcIP6  
fe80::2c0:95ff:fec5:d9b8 -destPort 80 -protocol TCP  
add simpleacl rule2 DENY -srcIP6 3ffe:100:100::1 -  
TTL 600
```

[Top](#)**clear ns simpleacl6****Synopsis**

```
clear ns simpleacl6
```

Description

Removes all simple ACL6 rules from the NetScaler appliance.

Example

```
clear ns simpleacl6
```

[Top](#)**flush ns simpleacl6****Synopsis**

```
flush ns simpleacl6 -estSessions
```

Description

Terminates all established IPv6 connections that match any of the newly configured simple ACL6 rules. Note: If you plan to create more than one simple ACL6 rule and flush existing connections that match any of them, you can minimize the affect on performance by first creating all of the simple ACL6 rules and then running flush only once.

[Top](#)

rm ns simpleacl6

Synopsis

rm ns simpleacl6 <aclname> ...

Description

Removes a simple ACL6 rule from the NetScaler appliance.

Parameters

aclname

Name of the simple ACL6 rule that you want to remove.

Example

```
rm ns simpleacl6 rule1
```

[Top](#)

show ns simpleacl6

Synopsis

show ns simpleacl6 [<aclname>]

Description

Displays settings of all the simple ACL6 rules or of the specified simple ACL6 rule. To display settings of all the simple ACL6 rules, run the command without any parameters. To display settings of a particular simple ACL6 rule, specify the name of the simple ACL6 rule.

Parameters

aclname

Name of the simple ACL6 rule whose settings you want the NetScaler appliance to display.

Example

```
show simpleacl6 rule1
  Name: rule1
    Action: DENY                               Hits:
5
  srcIP6 = 3ffe:100:100::1
  Protocol = TCP
  DestPort = 110
  TTL: 200 (seconds)
```

[Top](#)

stat ns simpleacl6

Synopsis

```
stat ns simpleacl6 [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile
<input_filename>] [-clearstats ( basic | full )]
```

Description

Displays statistics related to the simple ACL6 rules.

Parameters

clearstats

Clear the statistics / counters Possible values: basic, full

Example

```
stat simpleacl6
```

[Top](#)

ns pbr

[[add](#) | [rm](#) | [set](#) | [unset](#) | [enable](#) | [disable](#) | [stat](#) | [show](#)]

add ns pbr

Synopsis

```
add ns pbr <name> <action> [-td <positive_integer>] [-srcIP [<operator>] <srcIPVal>] [-
srcPort [<operator>] <srcPortVal>] [-destIP [<operator>] <destIPVal>] [-destPort
<operator>] <destPortVal>] ((-nextHop <nextHopVal>) | (-ipTunnel <ipTunnelName>)) [-
srcMac <mac_addr>] [-protocol <protocol> | -protocolNumber <positive_integer>] [-vlan
<positive_integer>] [-interface <interface_name>] [-priority <positive_integer>] [-msr
( ENABLED | DISABLED )] [-monitor <string>]] [-state ( ENABLED | DISABLED )]
```

Description

Adds a policy based route (PBR) to the NetScaler appliance. To commit this operation, you must apply the PBRs. A PBR specifies criteria for selecting outgoing IPv4 packets and, typically, a next hop to which to send the selected packets. For example, you can configure the NetScaler appliance to route outgoing packets from a specific IP address or range to a particular next hop router. Note: The NetScaler appliance process PBRs before processing the RNAT rules.

Parameters

name

Name for the PBR. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (\#), period (\.), space, colon \(:\), at \(@\), equals \(\=), and hyphen \(-\) characters. Can be changed after the PBR is created.

action

Action to perform on the outgoing IPv4 packets that match the PBR. Available settings function as follows: * ALLOW - The NetScaler appliance sends the packet to the designated next-hop router. * DENY - The NetScaler appliance applies the routing table for normal destination-based routing. Possible values: ALLOW, DENY

td

Traffic Domain Id. Maximum value: 4094

srcIP

IP address or range of IP addresses to match against the source IP address of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen and enclose within brackets. For example: [10.102.29.30-10.102.29.189].

srcPort

Port number or range of port numbers to match against the source port number of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen and enclose within brackets. For example: [40-90]. Note: The destination port can be specified only for TCP and UDP protocols.

destIP

IP address or range of IP addresses to match against the destination IP address of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen and enclose within brackets. For example: [10.102.29.30-10.102.29.189].

destPort

Port number or range of port numbers to match against the destination port number of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen and enclose within brackets. For example: [40-90]. Note: The destination port can be specified only for TCP and UDP protocols.

nextHop

IP address of the next hop router or the name of the link load balancing virtual server to which to send matching packets if action is set to ALLOW. If you specify a link load balancing (LLB) virtual server, which can provide a backup if a next hop link fails, first make sure that the next hops bound to the LLB virtual server are actually next hops that are directly connected to the NetScaler appliance. Otherwise, the NetScaler throws an error when you attempt to create the PBR.

ipTunnel

The Tunnel name.

srcMac

MAC address to match against the source MAC address of an outgoing IPv4 packet.

protocol

Protocol, identified by protocol name, to match against the protocol of an outgoing IPv4 packet. Possible values: ICMP, IGMP, TCP, EGP, IGP, ARGUS, UDP, RDP, RSVP, EIGRP, L2TP, ISIS

protocolNumber

Protocol, identified by protocol number, to match against the protocol of an outgoing IPv4 packet. Minimum value: 1 Maximum value: 255

vlan

ID of the VLAN. The NetScaler appliance compares the PBR only to the outgoing packets on the specified VLAN. If you do not specify any interface ID, the appliance compares the PBR to the outgoing packets on all VLANs. Minimum value: 1 Maximum value: 4094

interface

ID of an interface. The NetScaler appliance compares the PBR only to the outgoing packets on the specified interface. If you do not specify any value, the appliance compares the PBR to the outgoing packets on all interfaces.

priority

Priority of the PBR, which determines the order in which it is evaluated relative to the other PBRs. If you do not specify priorities while creating PBRs, the PBRs are evaluated in the order in which they are created. Minimum value: 1 Maximum value: 81920

msr

Monitor the route specified by the Next Hop parameter. This parameter is not applicable if you specify a link load balancing (LLB) virtual server name with the Next Hop parameter. Possible values: ENABLED, DISABLED Default value: DISABLED

state

Enable or disable the PBR. After you apply the PBRs, the NetScaler appliance compares outgoing packets to the enabled PBRs. Possible values: ENABLED, DISABLED Default value: XACLENABLED

Example

```
add ns pbr a allow -srcip 10.102.37.252 -destip
10.10.10.2 -nexthop 11.11.11.2
```

[Top](#)

rm ns pbr**Synopsis**

```
rm ns pbr <name> ...
```

Description

Removes a PBR from the NetScaler appliance. To commit this operation, you must apply the PBRs.

Parameters**name**

Name of the PBR that you want to remove.

Example

```
rm ns pbr a
```

[Top](#)

set ns pbr

Synopsis

```
set ns pbr <name> [-action ( ALLOW | DENY )] [-srcIP [<operator>] <srcIPVal>] [-srcPort  
[<operator>] <srcPortVal>] [-destIP [<operator>] <destIPVal>] [-destPort [<operator>]  
<destPortVal>] ((-nextHop <nextHopVal>) | (-ipTunnel <ipTunnelName>)) [-srcMac  
<mac_addr>] [-protocol <protocol> | -protocolNumber <positive_integer>] [-vlan  
<positive_integer>] [-interface <interface_name>] [-priority <positive_integer>] [-msr  
( ENABLED | DISABLED )] [-monitor <string>]]
```

Description

Modifies the specified parameters of a PBR. To commit this operation, you must apply the PBRs.

Parameters

name

Name of the PBR whose parameters you want to modify.

action

Action to perform on the outgoing IPv4 packets that match the PBR. Available settings function as follows: * ALLOW - The NetScaler appliance sends the packet to the designated next-hop router. * DENY - The NetScaler appliance applies the routing table for normal destination-based routing. Possible values: ALLOW, DENY

srcIP

IP address or range of IP addresses to match against the source IP address of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen and enclose within brackets. For example: [10.102.29.30-10.102.29.189].

srcPort

Port number or range of port numbers to match against the source port number of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen and enclose within brackets. For example: [40-90]. Note: The destination port can be specified only for TCP and UDP protocols.

destIP

IP address or range of IP addresses to match against the destination IP address of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen and enclose within brackets. For example: [10.102.29.30-10.102.29.189].

destPort

Port number or range of port numbers to match against the destination port number of an outgoing IPv4 packet. In the command line interface, separate the range with a

hyphen and enclose within brackets. For example: [40-90]. Note: The destination port can be specified only for TCP and UDP protocols.

nextHop

IP address of the next hop router or the name of the link load balancing virtual server to which to send matching packets if action is set to ALLOW. If you specify a link load balancing (LLB) virtual server, which can provide a backup if a next hop link fails, first make sure that the next hops bound to the LLB virtual server are actually next hops that are directly connected to the NetScaler appliance. Otherwise, the NetScaler throws an error when you attempt to create the PBR.

ipTunnel

The Tunnel name.

srcMac

MAC address to match against the source MAC address of an outgoing IPv4 packet.

protocol

Protocol, identified by protocol name, to match against the protocol of an outgoing IPv4 packet. Possible values: ICMP, IGMP, TCP, EGP, IGP, ARGUS, UDP, RDP, RSVP, EIGRP, L2TP, ISIS

protocolNumber

Protocol, identified by protocol number, to match against the protocol of an outgoing IPv4 packet. Minimum value: 1 Maximum value: 255

vlan

ID of the VLAN. The NetScaler appliance compares the PBR only to the outgoing packets on the specified VLAN. If you do not specify any interface ID, the appliance compares the PBR to the outgoing packets on all VLANs. Minimum value: 1 Maximum value: 4094

interface

ID of an interface. The NetScaler appliance compares the PBR only to the outgoing packets on the specified interface. If you do not specify any value, the appliance compares the PBR to the outgoing packets on all interfaces.

priority

Priority of the PBR, which determines the order in which it is evaluated relative to the other PBRs. If you do not specify priorities while creating PBRs, the PBRs are evaluated in the order in which they are created. Minimum value: 1 Maximum value: 81920

msr

Monitor the route specified by Next Hop parameter. This parameter is not applicable if you specify a link load balancing (LLB) virtual server name with the Next Hop parameter. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

```
set ns pbr a -srcPort 50
```

[Top](#)

unset ns pbr

Synopsis

```
unset ns pbr <name> [-srcIP] [-srcPort] [-destIP] [-destPort] [-nextHop] [-ipTunnel] [-srcMac] [-protocol] [-vlan] [-interface] [-msr] [-monitor]
```

Description

Resets the attributes of the specified PBR. Attributes for which a default value is available revert to their default values. Refer to the set ns pbr command for descriptions of the parameters..Refer to the set ns pbr command for meanings of the arguments.

Example

```
unset ns pbr rule1 -srcPort
```

[Top](#)

enable ns pbr

Synopsis

```
enable ns pbr <name> ...
```

Description

Enables a PBR. To commit this operation, you must apply the PBRs. After you apply the PBRs, the NetScaler appliance compares outgoing packets to the enabled PBRs.

Parameters

name

Name of PBR that you want to enable.

Example

```
enable ns pbr foo
```

[Top](#)

disable ns pbr

Synopsis

```
disable ns pbr <name> ...
```

Description

Disables a PBR. To commit this operation, you must apply the PBRs. After you apply the PBRs, the NetScaler appliance does not compare outgoing packets against the disabled PBRs

Parameters

name

Name of PBR that you want to disable.

Example

```
disable ns pbr foo
```

[Top](#)

stat ns pbr

Synopsis

```
stat ns pbr [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile  
<input_filename>] [-clearstats ( basic | full )]
```

Description

Displays statistics related to the PBRs. To display statistics of all the PBRs, run the command without any parameters. To display statistics of a particular PBR, specify the name of the PBR.

Parameters

name

Name of the PBR whose statistics you want the NetScaler appliance to display.

clearstats

Clear the statistics / counters Possible values: basic, full

Example

```
stat pbr
```

[Top](#)

show ns pbr

Synopsis

```
show ns pbr [<name>] [-detail]
```

Description

Displays settings related to the PBRs. To display settings of all the PBRs, run the command without any parameters. To display settings of a particular PBR, specify the name of the PBR.

Parameters

name

Name of the PBR whose details you want the NetScaler appliance to display.

detail

To get a detailed view.

Example

```
show ns pbr a
  Name: a                               Action:
ALLOW      Hits: 0
  srcIP = 10.102.37.252
  destIP = 10.10.10.2
  srcMac:
Protocol:
  Vlan:
Interface:
  Active Status: ENABLED
Applied Status: NOTAPPLIED
  Priority: 10
  NextHop: 11.11.11.2
```

[Top](#)

ns xmlnsnamespace

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add ns xmlnsnamespace

Synopsis

```
add ns xmlnsnamespace <prefix> <namespace>
```

Description

Adds a mapping between an XML prefix and a namespace URI (Uniform Resource Identifier).

Parameters

prefix

XML prefix.

namespace

Expanded namespace for which the XML prefix is provided.

Example

```
add ns xmlnsnamespace soap http://  
schemas.xmlsoap.org/soap/envelope/
```

[Top](#)**rm ns xmlnsnamespace****Synopsis**

```
rm ns xmlnsnamespace <prefix>
```

Description

Removes the mapping between an XML prefix and a namespace URI.

Parameters**prefix**

XML prefix for which the mapping must be removed.

Example

```
rm ns xmlnsnamespace soap
```

[Top](#)**set ns xmlnsnamespace****Synopsis**

```
set ns xmlnsnamespace <prefix> [<namespace>] [-description <string>]
```

Description

Modifies the mapping between an XML prefix and a namespace URI.

Parameters**prefix**

XML prefix for which the namespace or description must be added or updated.

namespace

Expanded namespace for which the XML prefix is provided.

description

Description for the prefix.

Example

```
set ns xmlnsnamespace soap -description SOAP/1.1
```

[Top](#)

unset ns xmlnspace

Synopsis

```
unset ns xmlnspace <prefix> [-namespace] [-description]
```

Description

Use this command to remove ns xmlnspace settings. Refer to the set ns xmlnspace command for meanings of the arguments.

[Top](#)

show ns xmlnspace

Synopsis

```
show ns xmlnspace [<prefix>]
```

Description

Displays the mappings between XML prefixes to namespace URIs.

Parameters

prefix

Name of the prefix for which the mappings must be displayed.

Example

```
show ns xmlnspace soap
```

[Top](#)

ns tcpProfile

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add ns tcpProfile

Synopsis

```
add ns tcpProfile <name> [-WS ( ENABLED | DISABLED )] [-SACK ( ENABLED |
DISABLED )] [-WSVal <positive_integer>] [-nagle ( ENABLED | DISABLED )] [-ackOnPush
( ENABLED | DISABLED )] [-mss <positive_integer>] [-maxBurst <positive_integer>] [-
initialCwnd <positive_integer>] [-delayedAck <positive_integer>] [-oooQSize
<positive_integer>] [-maxPktPerMss <positive_integer>] [-pktPerRetx
<positive_integer>] [-minRTO <positive_integer>] [-slowStartIncr <positive_integer>] [-
bufferSize <positive_integer>] [-synCookie ( ENABLED | DISABLED )] [-
KAproubUpdateLastactivity ( ENABLED | DISABLED )] [-flavor ( Default | Westwood )] [-
dynamicReceiveBuffering ( ENABLED | DISABLED )] [-KA ( ENABLED | DISABLED )] [-
KAconnIdleTime <positive_integer>] [-KAmaxProbes <positive_integer>] [-
```


KApobelInterval <positive_integer>] [-sendBuffsize <positive_integer>] [-mptcp
(ENABLED | DISABLED)]

Description

Adds a TCP profile to the NetScaler appliance.

Parameters

name

Name for a TCP profile. Must begin with a letter, number, or the underscore \(_) character. Other characters allowed, after the first character, are the hyphen \(-\), period \(. \), hash \(\#\), space \(\), at \(@\), and equal \(\=\) characters. The name of a TCP profile cannot be changed after it is created. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks \(" for example, "my tcp profile" or 'my tcp profile'\).

WS

Enable or disable window scaling. Possible values: ENABLED, DISABLED Default value: DISABLED

SACK

Enable or disable Selective ACKnowledgement (SACK). Possible values: ENABLED, DISABLED Default value: DISABLED

WSVal

Factor used to calculate the new window size. This argument is needed only when window scaling is enabled. Default value: 4 Maximum value: 14

nagle

Enable or disable the Nagle algorithm on TCP connections. Possible values: ENABLED, DISABLED Default value: DISABLED

ackOnPush

Send immediate positive acknowledgement (ACK) on receipt of TCP packets when doing Web 2.0 PUSH. Possible values: ENABLED, DISABLED Default value: ENABLED

mss

Maximum number of octets to allow in a TCP data segment. Maximum value: 1460

maxBurst

Maximum number of TCP segments allowed in a burst. Default value: 6 Minimum value: 1 Maximum value: 255

initialCwnd

Initial maximum upper limit on the number of TCP packets that can be outstanding on the TCP link to the server. Default value: 4 Minimum value: 1 Maximum value: 44

delayedAck

Timeout for TCP delayed ACK, in milliseconds. Default value: 100 Minimum value: 10 Maximum value: 300

oooQSize

Maximum size of out-of-order packets queue. A value of 0 means infinite. Default value: 64 Maximum value: 65535

maxPktPerMss

Maximum number of TCP packets allowed per maximum segment size (MSS).

Maximum value: 512

pktPerRetx

Maximum limit on the number of packets that should be retransmitted on receiving a partial ACK. Default value: 1 Minimum value: 1 Maximum value: 512

minRTO

Minimum retransmission timeout, in milliseconds. Default value: 1000 Minimum value: 10 Maximum value: 64000

slowStartIncr

Multiplier that determines the rate at which slow start increases the size of the TCP transmission window after each acknowledgement of successful transmission. Default value: 2 Minimum value: 1 Maximum value: 100

bufferSize

TCP buffering size, in bytes. Default value: 8190 Minimum value: 8190 Maximum value: 4194304

synCookie

Enable or disable the SYNCOOKIE mechanism for TCP handshake with clients.

Disabling SYNCOOKIE prevents SYN attack protection on the NetScaler appliance.

Possible values: ENABLED, DISABLED Default value: ENABLED

KAprobeUpdateLastactivity

Update last activity for the connection after receiving keep-alive (KA) probes.

Possible values: ENABLED, DISABLED Default value: ENABLED

flavor

Set TCP congestion control algorithm. Possible values: Default, Westwood Default

value: NS_TCP_DEFAULT

dynamicReceiveBuffering

Enable or disable dynamic receive buffering. When enabled, allows the receive buffer to be adjusted dynamically based on memory and network conditions. Note:

The buffer size argument must be set for dynamic adjustments to take place.

Possible values: ENABLED, DISABLED Default value: ENABLED

KA

Send periodic TCP keep-alive (KA) probes to check if peer is still up. Possible values:

ENABLED, DISABLED Default value: DISABLED

KAcnnIdleTime

Duration, in seconds, for the connection to be idle, before sending a keep-alive (KA) probe. Default value: NSTCP_KA_DEFAULT_CONN_IDLETIME Minimum value: 1

Maximum value: 4095

KAmxProbes

Number of keep-alive (KA) probes to be sent when not acknowledged, before

assuming the peer to be down. Default value: NSTCP_KA_DEFAULT_PROBE_COUNT

Minimum value: 1 Maximum value: 255

KAprobeInterval

Time interval, in seconds, before the next keep-alive (KA) probe, if the peer does not respond. Default value: NSTCP_KA_DEFAULT_INTERVAL Minimum value: 1 Maximum value: 4095

sendBuffsize

TCP Send Buffer Size Default value: 8190 Minimum value: 8190 Maximum value: 4194304

mptcp

Enable/Disable Multi-Path TCP Possible values: ENABLED, DISABLED Default value: DISABLED

Example

```
add tcpprofile <profile name> -WS ENABLED -WSVAL 4
```

[Top](#)

rm ns tcpProfile**Synopsis**

```
rm ns tcpProfile <name>
```

Description

Removes a TCP profile from the appliance.

Parameters**name**

Name of the TCP profile to be removed.

Example

```
rm tcpprofile <profile name>
```

[Top](#)

set ns tcpProfile**Synopsis**

```
set ns tcpProfile <name> [-WS ( ENABLED | DISABLED )] [-SACK ( ENABLED | DISABLED )]
[-WSVal <positive_integer>] [-nagle ( ENABLED | DISABLED )] [-ackOnPush ( ENABLED |
DISABLED )] [-mss <positive_integer>] [-maxBurst <positive_integer>] [-initialCwnd
<positive_integer>] [-delayedAck <positive_integer>] [-oooQSize <integer>] [-
maxPktPerMss <positive_integer>] [-pktPerRetx <positive_integer>] [-minRTO
<positive_integer>] [-slowStartIncr <positive_integer>] [-bufferSize <positive_integer>]
[-synCookie ( ENABLED | DISABLED )] [-KAprobeUpdateLastactivity ( ENABLED |
DISABLED )] [-flavor ( Default | Westwood )] [-dynamicReceiveBuffering ( ENABLED |
```

```
DISABLED )) [-KA ( ENABLED | DISABLED )) [-KAconnIdleTime <positive_integer>] [-KAmuxProbes <positive_integer>] [-KAprobeInterval <positive_integer>] [-sendBuffsize <positive_integer>] [-mptcp ( ENABLED | DISABLED )]
```

Description

Modifies the attributes of a TCP profile.

Parameters

name

Name of the TCP profile to be modified.

WS

Enable or disable window scaling. Possible values: ENABLED, DISABLED Default value: DISABLED

SACK

Enable or disable Selective ACKnowledgement (SACK). Possible values: ENABLED, DISABLED Default value: DISABLED

WSVal

Factor used to calculate the new window size. This argument is needed only when window scaling is enabled. Default value: 4 Maximum value: 14

nagle

Enable or disable the Nagle algorithm on TCP connections. Possible values: ENABLED, DISABLED Default value: DISABLED

ackOnPush

Send immediate positive acknowledgement (ACK) on receipt of TCP packets when doing Web 2.0 PUSH. Possible values: ENABLED, DISABLED Default value: ENABLED

mss

Set Maximum Segment Size(MSS) to use for TCP Connection(0 forces use of global setting) Maximum value: 1460

maxBurst

Maximum number of TCP segments allowed in a burst. Default value: 6 Minimum value: 1 Maximum value: 255

initialCwnd

Initial maximum upper limit on the number of TCP packets that can be outstanding on the TCP link to the server. Default value: 4 Minimum value: 1 Maximum value: 44

delayedAck

Timeout for TCP delayed ACK, in milliseconds. Default value: 100 Minimum value: 10 Maximum value: 300

oooQSize

Maximum size of out-of-order packets queue. A value of 0 means infinite. Default value: 64 Maximum value: 65535

maxPktPerMss

Maximum number of TCP packets allowed per maximum segment size (MSS). Maximum value: 512

pktPerRetx

Maximum limit on the number of packets that should be retransmitted on receiving a partial ACK. Default value: 1 Minimum value: 1 Maximum value: 512

minRTO

Minimum retransmission timeout, in milliseconds. Default value: 1000 Minimum value: 10 Maximum value: 64000

slowStartIncr

Multiplier that determines the rate at which slow start increases the size of the TCP transmission window after each acknowledgement of successful transmission. Default value: 2 Minimum value: 1 Maximum value: 100

bufferSize

TCP buffering size, in bytes. Default value: 8190 Minimum value: 8190 Maximum value: 4194304

synCookie

Enable or disable the SYNCOOKIE mechanism for TCP handshake with clients. Disabling SYNCOOKIE prevents SYN attack protection on the NetScaler appliance. Possible values: ENABLED, DISABLED Default value: ENABLED

KAprobeUpdateLastactivity

Update last activity for the connection after receiving keep-alive (KA) probes. Possible values: ENABLED, DISABLED Default value: ENABLED

flavor

Set TCP congestion control algorithm. Possible values: Default, Westwood Default value: NS_TCP_DEFAULT

dynamicReceiveBuffering

Enable or disable dynamic receive buffering. When enabled, allows the receive buffer to be adjusted dynamically based on memory and network conditions. Note: The buffer size argument must be set for dynamic adjustments to take place. Possible values: ENABLED, DISABLED Default value: ENABLED

KA

Send periodic TCP keep-alive (KA) probes to check if peer is still up. Possible values: ENABLED, DISABLED Default value: DISABLED

KAconnIdleTime

Duration, in seconds, for the connection to be idle, before sending a keep-alive (KA) probe. Default value: NSTCP_KA_DEFAULT_CONN_IDLETIME Minimum value: 1 Maximum value: 4095

KAmatrixProbes

Number of keep-alive (KA) probes to be sent when not acknowledged, before assuming the peer to be down. Default value: NSTCP_KA_DEFAULT_PROBE_COUNT Minimum value: 1 Maximum value: 255

KAprobeInterval

Time interval, in seconds, before the next keep-alive (KA) probe, if the peer does not respond. Default value: NSTCP_KA_DEFAULT_INTERVAL Minimum value: 1 Maximum value: 4095

sendBufferSize

TCP Send Buffer Size Default value: 8190 Minimum value: 8190 Maximum value: 4194304

mptcp

Enable/Disable Multi-Path TCP Possible values: ENABLED, DISABLED Default value: DISABLED

Example

```
set tcpprofile <profile name> -WS ENABLED -WSVAL 4
```

[Top](#)

unset ns tcpProfile

Synopsis

```
unset ns tcpProfile <name> [-WS] [-SACK] [-WSVal] [-nagle] [-ackOnPush] [-mss] [-maxBurst] [-initialCwnd] [-delayedAck] [-oooQSize] [-maxPktPerMss] [-pktPerRetx] [-minRTO] [-slowStartIncr] [-bufferSize] [-synCookie] [-KAprounUpdateLastactivity] [-flavor] [-dynamicReceiveBuffering] [-KA] [-KAmuxProbes] [-KAconnIdleTime] [-KAprobeInterval] [-sendBufferSize] [-mptcp]
```

Description

Removes the attributes of the TCP profile. Attributes for which a default value is available revert to their default values. Refer to the 'set ns tcpProfile' command for a description of the parameters..Refer to the set ns tcpProfile command for meanings of the arguments.

[Top](#)

show ns tcpProfile

Synopsis

```
show ns tcpProfile [<name>]
```

Description

Displays information about TCP profiles configured on the appliance.

Parameters

name

Name of the TCP profile to be displayed. If a name is not provided, information about all TCP profiles is shown.

Example

```
show tcp profile [profile name]
```

[Top](#)

ns httpProfile

[\[add | rm | set | unset | show \]](#)

add ns httpProfile

Synopsis

```
add ns httpProfile <name> [-dropInvalReqs ( ENABLED | DISABLED )] [-markHttp09Inval
( ENABLED | DISABLED )] [-markConnReqInval ( ENABLED | DISABLED )] [-cmpOnPush
( ENABLED | DISABLED )] [-conMultiplex ( ENABLED | DISABLED )] [-maxReusePool
<positive_integer>] [-dropExtraCRLF ( ENABLED | DISABLED )] [-incompHdrDelay
<positive_integer>] [-webSocket ( ENABLED | DISABLED )] [-reqTimeout
<positive_integer>] [-adptTimeout ( ENABLED | DISABLED )] [-reqTimeoutAction
<string>] [-dropExtraData ( ENABLED | DISABLED )] [-webLog ( ENABLED | DISABLED )] [-
clientIpHdrExpr <expression>] [-maxReq <positive_integer>] [-persistentETag ( ENABLED
| DISABLED )] [-spdy ( ENABLED | DISABLED )]
```

Description

Adds an HTTP profile to the NetScaler appliance.

Parameters

name

Name for an HTTP profile. Must begin with a letter, number, or the underscore \(_) character. Other characters allowed, after the first character, are the hyphen \(-\), period \(. \), hash \(\#\), space \(\), at \@ \), and equal \(\= \) characters. The name of a HTTP profile cannot be changed after it is created. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks \(\for example, "my http profile" or 'my http profile' \).

dropInvalReqs

Drop invalid HTTP requests or responses. Possible values: ENABLED, DISABLED Default value: DISABLED

markHttp09Inval

Mark HTTP/0.9 requests as invalid. Possible values: ENABLED, DISABLED Default value: DISABLED

markConnReqInval

Mark CONNECT requests as invalid. Possible values: ENABLED, DISABLED Default value: DISABLED

cmpOnPush

Start data compression on receiving a TCP packet with PUSH flag set. Possible values: ENABLED, DISABLED Default value: DISABLED

conMultiplex

Reuse server connections for requests from more than one client connections. Possible values: ENABLED, DISABLED Default value: ENABLED

maxReusePool

Maximum limit on the number of connections, from the NetScaler to a particular server that are kept in the reuse pool. This setting is helpful for optimal memory utilization and for reducing the idle connections to the server just after the peak time. Maximum value: 360000

dropExtraCRLF

Drop any extra 'CR' and 'LF' characters present after the header. Possible values: ENABLED, DISABLED Default value: ENABLED

incompHdrDelay

Maximum time to wait, in milliseconds, between incomplete header packets. If the header packets take longer to arrive at NetScaler, the connection is silently dropped. Default value: 7000 Maximum value: 4294967294LU

webSocket

HTTP connection to be upgraded to a web socket connection. Once upgraded, NetScaler does not process Layer 7 traffic on this connection. Possible values: ENABLED, DISABLED Default value: DISABLED

reqTimeout

Time, in seconds, within which the HTTP request must complete. If the request does not complete within this time, the specified request timeout action is executed. Maximum value: 86400

adptTimeout

Adapts the configured request timeout based on flow conditions. The timeout is increased or decreased internally and applied on the flow. Possible values: ENABLED, DISABLED Default value: DISABLED

reqTimeoutAction

Action to take when the HTTP request does not complete within the specified request timeout duration. You can configure the following actions: * RESET - Send RST (reset) to client when timeout occurs. * DROP - Drop silently when timeout occurs. * Custom responder action - Name of the responder action to trigger when timeout occurs, used to send custom message.

dropExtraData

Drop any extra data when server sends more data than the specified content-length. Possible values: ENABLED, DISABLED Default value: DISABLED

webLog

Enable or disable web logging. Possible values: ENABLED, DISABLED Default value: ENABLED

clientIpHdrExpr

Name of the header that contains the real client IP address.

maxReq

Maximum requests allowed on a single connection. Maximum value: 65534

persistentETag

Generate the persistent NetScaler specific ETag for the HTTP response with ETag header. Possible values: ENABLED, DISABLED Default value: DISABLED

spdy

Allow SPDY over SSL vserver. SSL will advertise SPDY support during NPN Handshake.
Possible values: ENABLED, DISABLED Default value: DISABLED

Example

```
add httpprofile <profile name> -dropInvalReqs ON -
markHttp09Inval ON
```

[Top](#)

rm ns httpProfile**Synopsis**

```
rm ns httpProfile <name>
```

Description

Removes an HTTP profile from the appliance.

Parameters**name**

Name of the HTTP profile to be removed.

Example

```
rm httpprofile <profile name>
```

[Top](#)

set ns httpProfile**Synopsis**

```
set ns httpProfile <name> [-dropInvalReqs ( ENABLED | DISABLED )] [-markHttp09Inval
( ENABLED | DISABLED )] [-markConnReqInval ( ENABLED | DISABLED )] [-cmpOnPush
( ENABLED | DISABLED )] [-conMultiplex ( ENABLED | DISABLED )] [-maxReusePool
<positive_integer>] [-dropExtraCRLF ( ENABLED | DISABLED )] [-incompHdrDelay
<positive_integer>] [-webSocket ( ENABLED | DISABLED )] [-reqTimeout
<positive_integer>] [-adptTimeout ( ENABLED | DISABLED )] [-reqTimeoutAction
<string>] [-dropExtraData ( ENABLED | DISABLED )] [-webLog ( ENABLED | DISABLED )] [-
clientIpHdrExpr <expression>] [-maxReq <positive_integer>] [-persistentETag ( ENABLED
| DISABLED )] [-spdy ( ENABLED | DISABLED )]
```

Description

Modifies the attributes of an HTTP profile.

Parameters

name

Name of the HTTP profile to be modified.

dropInvalReqs

Drop invalid HTTP requests or responses. Possible values: ENABLED, DISABLED Default value: DISABLED

markHttp09Inval

Mark HTTP/0.9 requests as invalid. Possible values: ENABLED, DISABLED Default value: DISABLED

markConnReqInval

Mark CONNECT requests as invalid. Possible values: ENABLED, DISABLED Default value: DISABLED

cmpOnPush

Start data compression on receiving a TCP packet with PUSH flag set. Possible values: ENABLED, DISABLED Default value: DISABLED

conMultiplex

Reuse server connections for requests from more than one client connections. Possible values: ENABLED, DISABLED Default value: ENABLED

maxReusePool

Maximum limit on the number of connections, from the NetScaler to a particular server that are kept in the reuse pool. This setting is helpful for optimal memory utilization and for reducing the idle connections to the server just after the peak time. Maximum value: 360000

dropExtraCRLF

Drop any extra 'CR' and 'LF' characters present after the header. Possible values: ENABLED, DISABLED Default value: ENABLED

incompHdrDelay

Maximum time to wait, in milliseconds, between incomplete header packets. If the header packets take longer to arrive at NetScaler, the connection is silently dropped. Default value: 7000 Maximum value: 4294967294LU

webSocket

HTTP connection to be upgraded to a web socket connection. Once upgraded, NetScaler does not process Layer 7 traffic on this connection. Possible values: ENABLED, DISABLED Default value: DISABLED

reqTimeout

Time, in seconds, within which the HTTP request must complete. If the request does not complete within this time, the specified request timeout action is executed. Maximum value: 86400

adptTimeout

Adapts the configured request timeout based on flow conditions. The timeout is increased or decreased internally and applied on the flow. Possible values: ENABLED, DISABLED Default value: DISABLED

reqTimeoutAction

Action to take when the HTTP request does not complete within the specified request timeout duration. You can configure the following actions: * RESET - Send RST (reset) to client when timeout occurs. * DROP - Drop silently when timeout occurs. * Custom responder action - Name of the responder action to trigger when timeout occurs, used to send custom message.

dropExtraData

Drop any extra data when server sends more data than the specified content-length. Possible values: ENABLED, DISABLED Default value: DISABLED

webLog

Enable or disable web logging. Possible values: ENABLED, DISABLED Default value: ENABLED

clientIpHdrExpr

Name of the header that contains the real client IP address.

maxReq

Maximum requests allowed on a single connection. Maximum value: 65534

persistentETag

Generate the persistent NetScaler specific ETag for the HTTP response with ETag header. Possible values: ENABLED, DISABLED Default value: DISABLED

spdy

Allow SPDY over SSL vserver. SSL will advertise SPDY support during NPN Handshake. Possible values: ENABLED, DISABLED Default value: DISABLED

Example

```
set httpprofile <profile name> -dropInvalReqs ON -
markHttp09Inval ON
```

[Top](#)

unset ns httpProfile**Synopsis**

```
unset ns httpProfile <name> [-dropInvalReqs] [-markHttp09Inval] [-markConnReqInval]
[-cmpOnPush] [-conMultiplex] [-maxReusePool] [-dropExtraCRLF] [-incompHdrDelay] [-
webSocket] [-dropExtraData] [-clientIpHdrExpr] [-reqTimeout] [-adptTimeout] [-
reqTimeoutAction] [-webLog] [-maxReq] [-persistentETag] [-spdy]
```

Description

Removes the attributes of the HTTP profile. Attributes for which a default value is available revert to their default values. Refer to the 'set ns httpProfile' command for a description of the parameters..Refer to the set ns httpProfile command for meanings of the arguments.

[Top](#)

show ns httpProfile

Synopsis

show ns httpProfile [<name>]

Description

Displays information about HTTP profiles configured on the appliance.

Parameters

name

Name of the HTTP profile to be displayed. If a name is not provided, information about all HTTP profiles is shown.

Example

```
show http profile [profile name]
```

[Top](#)

ns stats

[[show](#) | [clear](#)]

show ns stats

Synopsis

show ns stats - alias for 'stat ns'

Description

show ns stats is an alias for stat ns

[Top](#)

clear ns stats

Synopsis

clear ns stats <cleanuplevel>

Description

Clearing stats

Parameters

cleanuplevel

The level of stats to be cleared. 'global' option will clear global counters only, 'all' option will clear all device counters also along with global counters. For both the cases only 'ever incrementing counters' i.e. total counters will be cleared. Possible values: global, all

[Top](#)

ns ns.conf

show ns ns.conf

Synopsis

show ns ns.conf

Description

Displays the saved configurations.

ns savedConfig

show ns savedConfig

Synopsis

show ns savedConfig

Description

Displays the saved configurations.

ns runningConfig

show ns runningConfig

Synopsis

show ns runningConfig [-withDefaults]

Description

Displays all the configurations that have been executed on the appliance, including the configurations that have not yet been saved. Note: The unsaved configurations are lost when the appliance is rebooted or shut down.

Parameters

withDefaults

Include default values of parameters that have not been explicitly configured. If this argument is disabled, such parameters are not included.

ns acls

[[renumber](#) | [clear](#) | [apply](#)]

renumber ns acls

Synopsis

renumber ns acls

Description

Renumbers the priorities of extended ACL rules to multiples of 10. To commit this operation, you must apply the extended ACLs. Enables you to assign a new extended ACL rule a priority that is between two existing, consecutively numbered priorities. For example, if two extended ACLs, ACL1 and ACL2, have priorities 2 and 3 renumbering changes those priorities to 20 and 30. You can then add ACL3 with priority 25.

Example

```
renumber acls
```

[Top](#)

clear ns acls

Synopsis

```
clear ns acls
```

Description

Removes all simple ACL rules from the NetScaler appliance. This operation does not require an explicit apply.

Example

```
clear ns acls
```

[Top](#)

apply ns acls

Synopsis

```
apply ns acls
```

Description

Updates the extended ACL rule's memory tree (lookup table), adding any new extended ACL rules and applying any modifications to existing ACL rules. The lookup table includes the configuration of all the extended ACL rules on the NetScaler appliance. The NetScaler appliance uses the lookup table (not the configuration file) to filter the incoming IPv4 packets.

Example

```
apply ns acls
```

[Top](#)

ns info

show ns info

Synopsis

show ns info

Description

Displays the following details of the NetScaler appliance: * Software version * NetScaler IP address and subnet mask * Number of mapped IP addresses * Identifies the appliance as a standalone appliance, a part of an HA pair, or is a cluster node * Current time on the system and timestamp when the appliance was last updated * Features that are enabled or disabled * Modes that are enabled or disabled

Example

An example of this command's output is shown below:

```
System Rainier: Build 24, Date: Apr 25 2002,
21:13:25
System IP: 10.101.4.22      (mask: 255.255.0.0)
Mapped IP: 10.101.4.23
Node: Standalone
HTTP port(s): (none)
Max connections: 0
Max requests per connection: 0
Client IP insertion enabled: NO
Cookie version: 0
Feature status:
Web Logging: ON
Surge Protection: ON
Load Balancing: ON
Content Switching: ON
Cache Redirection: ON

Sure Connect: ON
Compression Control: OFF
Priority Queuing: ON
SSL Offloading: ON
Global Server Load Balancing: ON
HTTP DoS Protection: OFF
N+1: OFF
Dynamic Routing: OFF
Content Filtering: ON
Internal Caching: ON
SSL VPN: OFF
Mode status:
Fast Ramp: ON
Layer 2 mode: ON
Use Source IP: OFF
Client Keep-alive: ON
TCP Buffering: OFF
MAC-based forwarding: ON
```

```
Edge configuration: OFF
Use Subnet IP: OFF
Layer 3 mode (ip forwarding): ON
```

ns license

show ns license

Synopsis

show ns license

Description

Displays the state of all the licensed features.

ns version

show ns version

Synopsis

show ns version

Description

Displays the version and build number of the appliance.

ns config

[[clear](#) | [set](#) | [unset](#) | [save](#) | [show](#) | [diff](#)]

clear ns config

Synopsis

clear ns config [-force] <level>

Description

Clears the NetScaler running configurations based on different levels.

Parameters

force

Configurations will be cleared without prompting for confirmation.

level

Types of configurations to be cleared. * basic: Clears all configurations except the following: - NSIP, default route (gateway), MIPs, and SNIPs - Network settings (DG, VLAN, RHI, NTP and DNS settings) - Cluster settings - HA node definitions - Feature and mode settings - nsroot password * extended: Clears the same configurations as the 'basic' option. In addition, it clears the nsroot password and feature and mode settings. * full: Clears all configurations except NSIP, default route, and interface

settings. Note: When you clear the configurations through the cluster IP address, by specifying the level as 'full', the cluster is deleted and all cluster nodes become standalone appliances. The 'basic' and 'extended' levels are propagated to the cluster nodes. Possible values: basic, extended, full

[Top](#)

set ns config

Synopsis

```
set ns config [-IPAddress <ip_addr> -netmask <netmask>] [-nsvlan <positive_integer> -
ifnum <interface_name> ... [-tagged ( YES | NO )]] [-nwfwmode <nwfwmode>]
```

Description

Sets the NetScaler IP address and NetScaler VLAN. To set other NetScaler parameters, use the 'set ns param' command. Note: To change the NSIP address or the NSVLAN of an appliance that is part of a cluster, first remove the appliance from the cluster, change the NSIP or the NSVLAN, and then add the appliance back to the cluster.

Parameters

IPAddress

IP address of the NetScaler appliance. Commonly referred to as NSIP address. This parameter is mandatory to bring up the appliance.

nsvlan

VLAN (NSVLAN) for the subnet on which the IP address resides. Minimum value: 2
Maximum value: 4094

httpPort

The HTTP ports on the Web server. This allows the system to perform connection off-load for any client request that has a destination port matching one of these configured ports. Minimum value: 1

maxConn

The maximum number of connections that will be made from the system to the web server(s) attached to it. The value entered here is applied globally to all attached servers. Maximum value: 4294967294

maxReq

The maximum number of requests that the system can pass on a particular connection between the system and a server attached to it. Setting this value to 0 allows an unlimited number of requests to be passed. Maximum value: 65535

cip

The option to control (enable or disable) the insertion of the actual client IP address into the HTTP header request passed from the client to one, some, or all servers attached to the system. The passed address can then be accessed through a minor modification to the server. If cipHeader is specified, it will be used as the client IP header. If it is not specified, then the value that has been set by the set ns config CLI command will be used as the client IP header. Possible values: ENABLED, DISABLED

cookieversion

The version of the cookie inserted by system. Possible values: 0, 1

secureCookie

enable/disable secure flag for persistence cookie Possible values: ENABLED, DISABLED
Default value: ENABLED

pmtuMin

The minimum Path MTU. Default value: 576 Minimum value: 168 Maximum value: 1500

pmtuTimeout

The timeout value in minutes. Default value: 10 Minimum value: 1 Maximum value: 1440

ftpPortRange

Port range configured for FTP services. Minimum value: 1024 Maximum value: 64000

crPortRange

Port range for cache redirection services. Minimum value: 1 Maximum value: 65535

timezone

Name of the timezone Possible values: CoordinatedUniversalTime, GMT+01:00-CET-Europe/Andorra, GMT+04:00-GST-Asia/Dubai, GMT+04:30-AFT-Asia/Kabul, GMT-04:00-AST-America/Antigua, GMT-04:00-AST-America/Anguilla, GMT+01:00-CET-Europe/Tirane, GMT+04:00-AMT-Asia/Yerevan, GMT+01:00-WAT-Africa/Luanda, GMT+13:00-NZDT-Antarctica/McMurdo, GMT+13:00-NZDT-Antarctica/South_Pole, GMT-03:00-ROTT-Antarctica/Rothera, GMT-04:00-CLT-Antarctica/Palmer, GMT+05:00-MAWT-Antarctica/Mawson, GMT+07:00-DAVT-Antarctica/Davis, GMT+08:00-WST-Antarctica/Casey, GMT+06:00-VOST-Antarctica/Vostok, GMT+10:00-DDUT-Antarctica/DumontDURville, GMT+03:00-SYOT-Antarctica/Syowa, GMT+11:00-MIST-Antarctica/Macquarie, GMT-03:00-ART-America/Argentina/Buenos_Aires, GMT-03:00-ART-America/Argentina/Cordoba, GMT-03:00-ART-America/Argentina/Salta, GMT-03:00-ART-America/Argentina/Jujuy, GMT-03:00-ART-America/Argentina/Tucuman, GMT-03:00-ART-America/Argentina/Catamarca, GMT-03:00-ART-America/Argentina/La_Rioja, GMT-03:00-ART-America/Argentina/San_Juan, GMT-03:00-ART-America/Argentina/Mendoza, GMT-03:00-WARST-America/Argentina/San_Luis, GMT-03:00-ART-America/Argentina/Rio_Gallegos, GMT-03:00-ART-America/Argentina/Ushuaia, GMT-11:00-SST-Pacific/Pago_Pago, GMT+01:00-CET-Europe/Vienna, GMT+11:00-LHST-Australia/Lord_Howe, GMT+11:00-EST-Australia/Hobart, GMT+11:00-EST-Australia/Currie, GMT+11:00-EST-Australia/Melbourne, GMT+11:00-EST-Australia/Sydney, GMT+10:30-CST-Australia/Broken_Hill, GMT+10:00-EST-Australia/Brisbane, GMT+10:00-EST-Australia/Lindeman, GMT+10:30-CST-Australia/Adelaide, GMT+09:30-CST-Australia/Darwin, GMT+08:00-WST-Australia/Perth, GMT+08:45-CWST-Australia/Eucla, GMT-04:00-AST-America/Aruba, GMT+02:00-EET-Europe/Mariehamn, GMT+04:00-AZT-Asia/Baku, GMT+01:00-CET-Europe/Sarajevo, GMT-04:00-AST-America/Barbados, GMT+06:00-BDT-Asia/Dhaka, GMT+01:00-CET-Europe/Brussels, GMT+00:00-GMT-Africa/Ouagadougou, GMT+02:00-EET-Europe/Sofia, GMT+03:00-AST-Asia/Bahrain, GMT+02:00-CAT-Africa/Bujumbura, GMT+01:00-WAT-Africa/Porto-Novo, GMT-04:00-AST-America/St_Barthelemy, GMT-03:00-ADT-Atlantic/Bermuda, GMT+08:00-BNT-Asia/Brunei, GMT-04:00-BOT-America/La_Paz, GMT-02:00-FNT-America/Noronha, GMT-03:00-BRT-America/Belem, GMT-03:00-BRT-America/Fortaleza, GMT-03:00-BRT-America/Recife, GMT-03:00-BRT-America/Araguaina, GMT-03:00-BRT-

America/Maceio, GMT-03:00-BRT-America/Bahia, GMT-03:00-BRT-America/Sao_Paulo, GMT-04:00-AMT-America/Campo_Grande, GMT-04:00-AMT-America/Cuiaba, GMT-03:00-BRT-America/Santarem, GMT-04:00-AMT-America/Porto_Velho, GMT-04:00-AMT-America/Boa_Vista, GMT-04:00-AMT-America/Manaus, GMT-04:00-AMT-America/Eirunepe, GMT-04:00-AMT-America/Rio_Branco, GMT-04:00-EDT-America/Nassau, GMT+06:00-BTT-Asia/Thimphu, GMT+02:00-CAT-Africa/Gaborone, GMT+03:00-FET-Europe/Minsk, GMT-06:00-CST-America/Belize, GMT-02:30-NDT-America/St_Johns, GMT-03:00-ADT-America/Halifax, GMT-03:00-ADT-America/Glace_Bay, GMT-03:00-ADT-America/Moncton, GMT-03:00-ADT-America/Goose_Bay, GMT-04:00-AST-America/Blanc-Sablon, GMT-04:00-EDT-America/Montreal, GMT-04:00-EDT-America/Toronto, GMT-04:00-EDT-America/Nipigon, GMT-04:00-EDT-America/Thunder_Bay, GMT-04:00-EDT-America/Iqaluit, GMT-04:00-EDT-America/Pangnirtung, GMT-05:00-CDT-America/Resolute, GMT-05:00-EST-America/Atikokan, GMT-05:00-CDT-America/Rankin_Inlet, GMT-05:00-CDT-America/Winnipeg, GMT-05:00-CDT-America/Rainy_River, GMT-06:00-CST-America/Regina, GMT-06:00-CST-America/Swift_Current, GMT-06:00-MDT-America/Edmonton, GMT-06:00-MDT-America/Cambridge_Bay, GMT-06:00-MDT-America/Yellowknife, GMT-06:00-MDT-America/Inuvik, GMT-07:00-MST-America/Dawson_Creek, GMT-07:00-PDT-America/Vancouver, GMT-07:00-PDT-America/Whitehorse, GMT-07:00-PDT-America/Dawson, GMT+06:30-CCT-Indian/Cocos, GMT+01:00-WAT-Africa/Kinshasa, GMT+02:00-CAT-Africa/Lubumbashi, GMT+01:00-WAT-Africa/Bangui, GMT+01:00-WAT-Africa/Brazzaville, GMT+01:00-CET-Europe/Zurich, GMT+00:00-GMT-Africa/Abidjan, GMT-10:00-CKT-Pacific/Rarotonga, GMT-04:00-CLT-America/Santiago, GMT-06:00-EAST-Pacific/Easter, GMT+01:00-WAT-Africa/Douala, GMT+08:00-CST-Asia/Shanghai, GMT+08:00-CST-Asia/Harbin, GMT+08:00-CST-Asia/Chongqing, GMT+08:00-CST-Asia/Urumqi, GMT+08:00-CST-Asia/Kashgar, GMT-05:00-COT-America/Bogota, GMT-06:00-CST-America/Costa_Rica, GMT-04:00-CDT-America/Havana, GMT-01:00-CVT-Atlantic/Cape_Verde, GMT+07:00-CXT-Indian/Christmas, GMT+02:00-EET-Asia/Nicosia, GMT+01:00-CET-Europe/Prague, GMT+01:00-CET-Europe/Berlin, GMT+03:00-EAT-Africa/Djibouti, GMT+01:00-CET-Europe/Copenhagen, GMT-04:00-AST-America/Dominica, GMT-04:00-AST-America/Santo_Domingo, GMT+01:00-CET-Africa/Algiers, GMT-05:00-ECT-America/Guayaquil, GMT-06:00-GALT-Pacific/Galapagos, GMT+02:00-EET-Europe/Tallinn, GMT+02:00-EET-Africa/Cairo, GMT+00:00-WET-Africa/El_Aaiun, GMT+03:00-EAT-Africa/Asmara, GMT+01:00-CET-Europe/Madrid, GMT+01:00-CET-Africa/Ceuta, GMT+00:00-WET-Atlantic/Canary, GMT+03:00-EAT-Africa/Addis_Ababa, GMT+02:00-EET-Europe/Helsinki, GMT+12:00-FJT-Pacific/Fiji, GMT-03:00-FKST-Atlantic/Stanley, GMT+10:00-CHUT-Pacific/Chuuk, GMT+11:00-PONT-Pacific/Pohnpei, GMT+11:00-KOST-Pacific/Kosrae, GMT+00:00-WET-Atlantic/Faroe, GMT+01:00-CET-Europe/Paris, GMT+01:00-WAT-Africa/Libreville, GMT+00:00-GMT-Europe/London, GMT-04:00-AST-America/Grenada, GMT+04:00-GET-Asia/Tbilisi, GMT-03:00-GFT-America/Cayenne, GMT+00:00-GMT-Europe/Guernsey, GMT+00:00-GMT-Africa/Accra, GMT+01:00-CET-Europe/Gibraltar, GMT-03:00-WGT-America/Godthab, GMT+00:00-GMT-America/Danmarkshavn, GMT-01:00-EGT-America/Scoresbysund, GMT-03:00-ADT-America/Thule, GMT+00:00-GMT-Africa/Banjul, GMT+00:00-GMT-Africa/Conakry, GMT-04:00-AST-America/Guadeloupe, GMT+01:00-WAT-Africa/Malabo, GMT+02:00-EET-Europe/Athens, GMT-02:00-GST-Atlantic/South_Georgia, GMT-06:00-CST-America/Guatemala, GMT+10:00-ChST-Pacific/Guam, GMT+00:00-GMT-Africa/Bissau, GMT-04:00-GYT-America/Guyana, GMT+08:00-HKT-Asia/Hong_Kong, GMT-06:00-CST-America/Tegucigalpa, GMT+01:00-CET-Europe/Zagreb, GMT-05:00-EST-America/Port-au-Prince, GMT+01:00-CET-Europe/Budapest, GMT+07:00-WIT-Asia/Jakarta, GMT+07:00-WIT-Asia/Pontianak, GMT+08:00-CIT-Asia/Makassar, GMT+09:00-EIT-Asia/Jayapura, GMT+00:00-GMT-Europe/Dublin, GMT+02:00-

IST-Asia/Jerusalem, GMT+00:00-GMT-Europe/Isle_of_Man, GMT+05:30-IST-Asia/Kolkata, GMT+06:00-IOT-Indian/Chagos, GMT+03:00-AST-Asia/Baghdad, GMT+03:30-IRST-Asia/Tehran, GMT+00:00-GMT-Atlantic/Reykjavik, GMT+01:00-CET-Europe/Rome, GMT+00:00-GMT-Europe/Jersey, GMT-05:00-EST-America/Jamaica, GMT+02:00-EET-Asia/Amman, GMT+09:00-JST-Asia/Tokyo, GMT+03:00-EAT-Africa/Nairobi, GMT+06:00-KGT-Asia/Bishkek, GMT+07:00-ICT-Asia/Phnom_Penh, GMT+12:00-GILT-Pacific/Tarawa, GMT+13:00-PHOT-Pacific/Enderbury, GMT+14:00-LINT-Pacific/Kiritimati, GMT+03:00-EAT-Indian/Comoro, GMT-04:00-AST-America/St_Kitts, GMT+09:00-KST-Asia/Pyongyang, GMT+09:00-KST-Asia/Seoul, GMT+03:00-AST-Asia/Kuwait, GMT-05:00-EST-America/Cayman, GMT+06:00-ALMT-Asia/Almaty, GMT+06:00-QYZT-Asia/Quyzyldora, GMT+05:00-AQTT-Asia/Aqtobe, GMT+05:00-AQTT-Asia/Aqtau, GMT+05:00-ORAT-Asia/Oral, GMT+07:00-ICT-Asia/Vientiane, GMT+02:00-EET-Asia/Beirut, GMT-04:00-AST-America/St_Lucia, GMT+01:00-CET-Europe/Vaduz, GMT+05:30-IST-Asia/Colombo, GMT+00:00-GMT-Africa/Monrovia, GMT+02:00-SAST-Africa/Maseru, GMT+02:00-EET-Europe/Vilnius, GMT+01:00-CET-Europe/Luxembourg, GMT+02:00-EET-Europe/Riga, GMT+02:00-EET-Africa/Tripoli, GMT+00:00-WET-Africa/Casablanca, GMT+01:00-CET-Europe/Monaco, GMT+02:00-EET-Europe/Chisinau, GMT+01:00-CET-Europe/Podgorica, GMT-04:00-AST-America/Marigot, GMT+03:00-EAT-Indian/Antananarivo, GMT+12:00-MHT-Pacific/Majuro, GMT+12:00-MHT-Pacific/Kwajalein, GMT+01:00-CET-Europe/Skopje, GMT+00:00-GMT-Africa/Bamako, GMT+06:30-MMT-Asia/Rangoon, GMT+08:00-ULAT-Asia/Ulaanbaatar, GMT+07:00-HOVT-Asia/Hovd, GMT+08:00-CHOT-Asia/Choibalsan, GMT+08:00-CST-Asia/Macau, GMT+10:00-ChST-Pacific/Saipan, GMT-04:00-AST-America/Martinique, GMT+00:00-GMT-Africa/Nouakchott, GMT-04:00-AST-America/Montserrat, GMT+01:00-CET-Europe/Malta, GMT+04:00-MUT-Indian/Mauritius, GMT+05:00-MVT-Indian/Maldives, GMT+02:00-CAT-Africa/Blantyre, GMT-06:00-CST-America/Mexico_City, GMT-06:00-CST-America/Cancun, GMT-06:00-CST-America/Merida, GMT-06:00-CST-America/Monterrey, GMT-05:00-CDT-America/Matamoros, GMT-07:00-MST-America/Mazatlan, GMT-07:00-MST-America/Chihuahua, GMT-06:00-MDT-America/Ojinaga, GMT-07:00-MST-America/Hermosillo, GMT-07:00-PDT-America/Tijuana, GMT-08:00-PST-America/Santa_Isabel, GMT-06:00-CST-America/Bahia_Banderas, GMT+08:00-MYT-Asia/Kuala_Lumpur, GMT+08:00-MYT-Asia/Kuching, GMT+02:00-CAT-Africa/Maputo, GMT+02:00-WAST-Africa/Windhoek, GMT+11:00-NCT-Pacific/Noumea, GMT+01:00-WAT-Africa/Niamey, GMT+11:30-NFT-Pacific/Norfolk, GMT+01:00-WAT-Africa/Lagos, GMT-06:00-CST-America/Managua, GMT+01:00-CET-Europe/Amsterdam, GMT+01:00-CET-Europe/Oslo, GMT+05:45-NPT-Asia/Kathmandu, GMT+12:00-NRT-Pacific/Nauru, GMT-11:00-NUT-Pacific/Niue, GMT+13:00-NZDT-Pacific/Auckland, GMT+13:45-CHADT-Pacific/Chatham, GMT+04:00-GST-Asia/Muscat, GMT-05:00-EST-America/Panama, GMT-05:00-PET-America/Lima, GMT-10:00-TAHT-Pacific/Tahiti, GMT-09:30-MART-Pacific/Marquesas, GMT-09:00-GAMT-Pacific/Gambier, GMT+10:00-PGT-Pacific/Port_Moresby, GMT+08:00-PHT-Asia/Manila, GMT+05:00-PKT-Asia/Karachi, GMT+01:00-CET-Europe/Warsaw, GMT-02:00-PMDT-America/Miquelon, GMT-08:00-PST-Pacific/Pitcairn, GMT-04:00-AST-America/Puerto_Rico, GMT+02:00-EET-Asia/Gaza, GMT+02:00-EET-Asia/Hebron, GMT+00:00-WET-Europe/Lisbon, GMT+00:00-WET-Atlantic/Madeira, GMT-01:00-AZOT-Atlantic/Azores, GMT+09:00-PWT-Pacific/Palau, GMT-03:00-PYST-America/Asuncion, GMT+03:00-AST-Asia/Qatar, GMT+04:00-RET-Indian/Reunion, GMT+02:00-EET-Europe/Bucharest, GMT+01:00-CET-Europe/Belgrade, GMT+03:00-FET-Europe/Kaliningrad, GMT+04:00-MSK-Europe/Moscow, GMT+04:00-VOLT-Europe/Volgograd, GMT+04:00-SAMT-Europe/Samara, GMT+06:00-YEKT-Asia/Yekaterinburg, GMT+07:00-OMST-Asia/Omsk, GMT+07:00-NOVT-Asia/Novosibirsk, GMT+07:00-NOVT-Asia/Novokuznetsk, GMT+08:00-KRAT-Asia/Krasnoyarsk, GMT+09:00-IRKT-Asia/Irkutsk, GMT+10:00-YAKT-Asia/Yakutsk, GMT

+11:00-VLAT-Asia/Vladivostok, GMT+11:00-SAKT-Asia/Sakhalin, GMT+12:00-MAGT-Asia/Magadan, GMT+12:00-PETT-Asia/Kamchatka, GMT+12:00-ANAT-Asia/Anadyr, GMT+02:00-CAT-Africa/Kigali, GMT+03:00-AST-Asia/Riyadh, GMT+11:00-SBT-Pacific/Guadalcanal, GMT+04:00-SCT-Indian/Mahe, GMT+03:00-EAT-Africa/Khartoum, GMT+01:00-CET-Europe/Stockholm, GMT+08:00-SGT-Asia/Singapore, GMT+00:00-GMT-Atlantic/St_Helena, GMT+01:00-CET-Europe/Ljubljana, GMT+01:00-CET-Arctic/Longyearbyen, GMT+01:00-CET-Europe/Bratislava, GMT+00:00-GMT-Africa/Freetown, GMT+01:00-CET-Europe/San_Marino, GMT+00:00-GMT-Africa/Dakar, GMT+03:00-EAT-Africa/Mogadishu, GMT-03:00-SRT-America/Paramaribo, GMT+00:00-GMT-Africa/Sao_Tome, GMT-06:00-CST-America/El_Salvador, GMT+02:00-EET-Asia/Damascus, GMT+02:00-SAST-Africa/Mbabane, GMT-04:00-EDT-America/Grand_Turk, GMT+01:00-WAT-Africa/Ndjamena, GMT+05:00-TFT-Indian/Kerguelen, GMT+00:00-GMT-Africa/Lome, GMT+07:00-ICT-Asia/Bangkok, GMT+05:00-TJT-Asia/Dushanbe, GMT-10:00-TKT-Pacific/Fakaofu, GMT+09:00-TLT-Asia/Dili, GMT+05:00-TMT-Asia/Ashgabat, GMT+01:00-CET-Africa/Tunis, GMT+13:00-TOT-Pacific/Tongatapu, GMT+02:00-EET-Europe/Istanbul, GMT-04:00-AST-America/Port_of_Spain, GMT+12:00-TVT-Pacific/Funafuti, GMT+08:00-CST-Asia/Taipei, GMT+03:00-EAT-Africa/Dar_es_Salaam, GMT+02:00-EET-Europe/Kiev, GMT+02:00-EET-Europe/Uzhgorod, GMT+02:00-EET-Europe/Zaporozhye, GMT+02:00-EET-Europe/Simferopol, GMT+03:00-EAT-Africa/Kampala, GMT-10:00-HST-Pacific/Johnston, GMT-11:00-SST-Pacific/Midway, GMT+12:00-WAKT-Pacific/Wake, GMT-04:00-EDT-America/New_York, GMT-04:00-EDT-America/Detroit, GMT-04:00-EDT-America/Kentucky/Louisville, GMT-04:00-EDT-America/Kentucky/Monticello, GMT-04:00-EDT-America/Indiana/Indianapolis, GMT-04:00-EDT-America/Indiana/Vincennes, GMT-04:00-EDT-America/Indiana/Winamac, GMT-04:00-EDT-America/Indiana/Marengo, GMT-04:00-EDT-America/Indiana/Petersburg, GMT-04:00-EDT-America/Indiana/Vevay, GMT-05:00-CDT-America/Chicago, GMT-05:00-CDT-America/Indiana/Tell_City, GMT-05:00-CDT-America/Indiana/Knox, GMT-05:00-CDT-America/Menominee, GMT-05:00-CDT-America/North_Dakota/Center, GMT-05:00-CDT-America/North_Dakota/New_Salem, GMT-05:00-CDT-America/North_Dakota/Beulah, GMT-06:00-MDT-America/Denver, GMT-06:00-MDT-America/Boise, GMT-06:00-MDT-America/Shiprock, GMT-07:00-MST-America/Phoenix, GMT-07:00-PDT-America/Los_Angeles, GMT-08:00-AKDT-America/Anchorage, GMT-08:00-AKDT-America/Juneau, GMT-08:00-AKDT-America/Sitka, GMT-08:00-AKDT-America/Yakutat, GMT-08:00-AKDT-America/Nome, GMT-09:00-HADT-America/Adak, GMT-08:00-MeST-America/Metlakatla, GMT-10:00-HST-Pacific/Honolulu, GMT-03:00-UYT-America/Montevideo, GMT+05:00-UZT-Asia/Samarkand, GMT+05:00-UZT-Asia/Tashkent, GMT+01:00-CET-Europe/Vatican, GMT-04:00-AST-America/St_Vincent, GMT-04:30-VET-America/Caracas, GMT-04:00-AST-America/Tortola, GMT-04:00-AST-America/St_Thomas, GMT+07:00-ICT-Asia/Ho_Chi_Min, GMT+11:00-VUT-Pacific/Efate, GMT+12:00-WFT-Pacific/Wallis, GMT+14:00-WSDT-Pacific/Apia, GMT+03:00-AST-Asia/Aden, GMT+03:00-EAT-Indian/Mayotte, GMT+02:00-SAST-Africa/Johannesburg, GMT+02:00-CAT-Africa/Lusaka, GMT+02:00-CAT-Africa/Harare

grantQuotaMaxClient

The percentage of shared quota to be granted at a time for maxClient Default value: 10 Maximum value: 100

exclusiveQuotaMaxClient

The percentage of maxClient to be given to PEs Default value: 80 Maximum value: 100

grantQuotaSpillOver

The percentage of shared quota to be granted at a time for spillover Default value: 10 Maximum value: 100

exclusiveQuotaSpillOver

The percentage of max limit to be given to PEs Default value: 80 Maximum value: 100

nwfwmode

Network Firewall mode to be used. NOFIREWALL - No Network firewall setting BASIC - DENY-ALL behavior and DENY-ALL AT BOOTUP EXTENDED - NS_NWFWMODE_BASIC + drop IP fragments + TCP and ACL logging + packet drop on closed port EXTENDEDPLUS - NS_NWFWMODE_EXTENDED + block traffic on 3008-3011 + drop non-session packets FULL - NS_NWFWMODE_EXTENDEDPLUS + drop non-ip packets. Possible values: NOFIREWALL, BASIC, EXTENDED, EXTENDEDPLUS, FULL Default value: NS_NWFWMODE_NO

[Top](#)

unset ns config**Synopsis**

unset ns config [-nsvlan] [-IPAddress] [-netmask] [-ifnum] [-tagged] [-nwfwmode]

Description

Removes the attributes of the NetScaler appliance. Attributes for which a default value is available revert to their default values. Refer to the 'set ns config' command for a description of the parameters..Refer to the set ns config command for meanings of the arguments.

[Top](#)

save ns config**Synopsis**

save ns config

Description

Save the configurations to the appliances FLASH memory in the /nsconfig/ns.conf file. Backup configuration files are named ns.conf.n. The most recent backup file has the smallest value for n.

[Top](#)

show ns config**Synopsis**

show ns config

Description

Displays the following details of the NetScaler appliance: * NetScaler IP address and subnet mask * Number of mapped IP addresses * Identifies the appliance as a

standalone appliance, a part of a HA pair, or is a cluster node * Current time on the system and timestamp when the appliance was last updated Note: To view the complete configurations that have been executed on the appliance, run the 'show ns runningConfig' command.

[Top](#)

diff ns config

Synopsis

```
diff ns config [<config1>] [<config2>] [-outtype ( cli | xml )] [-template] [-ignoreDeviceSpecific]
```

Description

Difference between two configuration

Parameters

config1

Location of the configurations.

config2

Location of the configurations.

outtype

Format to display the difference in configurations. Possible values: cli, xml

template

File that contains the commands to be compared.

ignoreDeviceSpecific

Suppress device specific differences.

Example

```
Generates the differences between two
configurations.
Note: If no parameters are provided, then the
differences between the saved configurations and
the running configurations are shown.
```

[Top](#)

ns param

[[set](#) | [unset](#) | [show](#)]

set ns param

Synopsis

```
set ns param [-httpPort <port> ...] [-maxConn <positive_integer>] [-maxReq
<positive_integer>] [-cip ( ENABLED | DISABLED ) <cipHeader>] [-cookieversion ( 0 | 1 )]
```

```
[-secureCookie ( ENABLED | DISABLED )] [-pmtuMin <positive_integer>] [-pmtuTimeout  
<mins>] [-ftpPortRange <int[-int]>] [-crPortRange <int[-int]>] [-timezone <timezone>] [-  
grantQuotaMaxClient <positive_integer>] [-exclusiveQuotaMaxClient <positive_integer>]  
[-grantQuotaSpillOver <positive_integer>] [-exclusiveQuotaSpillOver <positive_integer>]  
[-useproxyport ( ENABLED | DISABLED )] [-internaluserlogin ( ENABLED | DISABLED )] [-  
aftpAllowRandomSourcePort ( ENABLED | DISABLED )] [-icaPorts <port> ...]
```

Description

Sets the parameters of the NetScaler appliance.

Parameters

httpPort

HTTP ports on the web server. This allows the system to perform connection off-load for any client request that has a destination port matching one of these configured ports. Minimum value: 1

maxConn

Maximum number of connections that will be made from the appliance to the web server(s) attached to it. The value entered here is applied globally to all attached servers. Maximum value: 4294967294

maxReq

Maximum number of requests that the system can pass on a particular connection between the appliance and a server attached to it. Setting this value to 0 allows an unlimited number of requests to be passed. This value is overridden by the maximum number of requests configured on the individual service. Maximum value: 65535

cip

Enable or disable the insertion of the actual client IP address into the HTTP header request passed from the client to one, some, or all servers attached to the system. The passed address can then be accessed through a minor modification to the server. * If the CIP header is specified, it will be used as the client IP header. * If the CIP header is not specified, the value that has been set will be used as the client IP header. Possible values: ENABLED, DISABLED

cookieversion

Version of the cookie inserted by the system. Possible values: 0, 1

secureCookie

Enable or disable secure flag for persistence cookie. Possible values: ENABLED, DISABLED Default value: ENABLED

pmtuMin

Minimum path MTU value that NetScaler will process in the ICMP fragmentation needed message. If the ICMP message contains a value less than this value, then this value is used instead. Default value: 576 Minimum value: 168 Maximum value: 1500

pmtuTimeout

Interval, in minutes, for flushing the PMTU entries. Default value: 10 Minimum value: 1 Maximum value: 1440

ftpPortRange

Minimum and maximum port (port range) that FTP services are allowed to use.

Minimum value: 1024 Maximum value: 64000

crPortRange

Port range for cache redirection services. Minimum value: 1 Maximum value: 65535

timezone

Time zone for the NetScaler appliance. Name of the time zone should be specified as argument. Possible values: CoordinatedUniversalTime, GMT+01:00-CET-Europe/Andorra, GMT+04:00-GST-Asia/Dubai, GMT+04:30-AFT-Asia/Kabul, GMT-04:00-AST-America/Antigua, GMT-04:00-AST-America/Anguilla, GMT+01:00-CET-Europe/Tirane, GMT+04:00-AMT-Asia/Yerevan, GMT+01:00-WAT-Africa/Luanda, GMT+13:00-NZDT-Antarctica/McMurdo, GMT+13:00-NZDT-Antarctica/South_Pole, GMT-03:00-ROTT-Antarctica/Rothera, GMT-04:00-CLT-Antarctica/Palmer, GMT+05:00-MAWT-Antarctica/Mawson, GMT+07:00-DAVT-Antarctica/Davis, GMT+08:00-WST-Antarctica/Casey, GMT+06:00-VOST-Antarctica/Vostok, GMT+10:00-DDUT-Antarctica/DumontDUrville, GMT+03:00-SYOT-Antarctica/Syowa, GMT+11:00-MIST-Antarctica/Macquarie, GMT-03:00-ART-America/Argentina/Buenos_Aires, GMT-03:00-ART-America/Argentina/Cordoba, GMT-03:00-ART-America/Argentina/Salta, GMT-03:00-ART-America/Argentina/Jujuy, GMT-03:00-ART-America/Argentina/Tucuman, GMT-03:00-ART-America/Argentina/Catamarca, GMT-03:00-ART-America/Argentina/La_Rioja, GMT-03:00-ART-America/Argentina/San_Juan, GMT-03:00-ART-America/Argentina/Mendoza, GMT-03:00-WARST-America/Argentina/San_Luis, GMT-03:00-ART-America/Argentina/Rio_Gallegos, GMT-03:00-ART-America/Argentina/Ushuaia, GMT-11:00-SST-Pacific/Pago_Pago, GMT+01:00-CET-Europe/Vienna, GMT+11:00-LHST-Australia/Lord_Howe, GMT+11:00-EST-Australia/Hobart, GMT+11:00-EST-Australia/Currie, GMT+11:00-EST-Australia/Melbourne, GMT+11:00-EST-Australia/Sydney, GMT+10:30-CST-Australia/Broken_Hill, GMT+10:00-EST-Australia/Brisbane, GMT+10:00-EST-Australia/Lindeman, GMT+10:30-CST-Australia/Adelaide, GMT+09:30-CST-Australia/Darwin, GMT+08:00-WST-Australia/Perth, GMT+08:45-CWST-Australia/Eucla, GMT-04:00-AST-America/Aruba, GMT+02:00-EET-Europe/Mariehamn, GMT+04:00-AZT-Asia/Baku, GMT+01:00-CET-Europe/Sarajevo, GMT-04:00-AST-America/Barbados, GMT+06:00-BDT-Asia/Dhaka, GMT+01:00-CET-Europe/Brussels, GMT+00:00-GMT-Africa/Ouagadougou, GMT+02:00-EET-Europe/Sofia, GMT+03:00-AST-Asia/Bahrain, GMT+02:00-CAT-Africa/Bujumbura, GMT+01:00-WAT-Africa/Porto-Novo, GMT-04:00-AST-America/St_Barthelemy, GMT-03:00-ADT-Atlantic/Bermuda, GMT+08:00-BNT-Asia/Brunei, GMT-04:00-BOT-America/La_Paz, GMT-02:00-FNT-America/Noronha, GMT-03:00-BRT-America/Belem, GMT-03:00-BRT-America/Fortaleza, GMT-03:00-BRT-America/Recife, GMT-03:00-BRT-America/Araguaina, GMT-03:00-BRT-America/Maceio, GMT-03:00-BRT-America/Bahia, GMT-03:00-BRT-America/Sao_Paulo, GMT-04:00-AMT-America/Campo_Grande, GMT-04:00-AMT-America/Cuiaba, GMT-03:00-BRT-America/Santarem, GMT-04:00-AMT-America/Porto_Velho, GMT-04:00-AMT-America/Boa_Vista, GMT-04:00-AMT-America/Manaus, GMT-04:00-AMT-America/Eirunepe, GMT-04:00-AMT-America/Rio_Branco, GMT-04:00-EDT-America/Nassau, GMT+06:00-BTT-Asia/Thimphu, GMT+02:00-CAT-Africa/Gaborone, GMT+03:00-FET-Europe/Minsk, GMT-06:00-CST-America/Belize, GMT-02:30-NDT-America/St_Johns, GMT-03:00-ADT-America/Halifax, GMT-03:00-ADT-America/Glace_Bay, GMT-03:00-ADT-America/Moncton, GMT-03:00-ADT-America/Goose_Bay, GMT-04:00-AST-America/Blanc-Sablon, GMT-04:00-EDT-America/Montreal, GMT-04:00-EDT-America/Toronto, GMT-04:00-EDT-America/Nipigon, GMT-04:00-EDT-America/Thunder_Bay, GMT-04:00-EDT-America/

Iqaluit, GMT-04:00-EDT-America/Pangnirtung, GMT-05:00-CDT-America/Resolute,
 GMT-05:00-EST-America/Atikokan, GMT-05:00-CDT-America/Rankin_Inlet, GMT-05:00-
 CDT-America/Winnipeg, GMT-05:00-CDT-America/Rainy_River, GMT-06:00-CST-
 America/Regina, GMT-06:00-CST-America/Swift_Current, GMT-06:00-MDT-America/
 Edmonton, GMT-06:00-MDT-America/Cambridge_Bay, GMT-06:00-MDT-America/
 Yellowknife, GMT-06:00-MDT-America/Inuvik, GMT-07:00-MST-America/
 Dawson_Creek, GMT-07:00-PDT-America/Vancouver, GMT-07:00-PDT-America/
 Whitehorse, GMT-07:00-PDT-America/Dawson, GMT+06:30-CCT-Indian/Cocos, GMT
 +01:00-WAT-Africa/Kinshasa, GMT+02:00-CAT-Africa/Lubumbashi, GMT+01:00-WAT-
 Africa/Bangui, GMT+01:00-WAT-Africa/Brazzaville, GMT+01:00-CET-Europe/Zurich,
 GMT+00:00-GMT-Africa/Abidjan, GMT-10:00-CKT-Pacific/Rarotonga, GMT-04:00-CLT-
 America/Santiago, GMT-06:00-EAST-Pacific/Easter, GMT+01:00-WAT-Africa/Douala,
 GMT+08:00-CST-Asia/Shanghai, GMT+08:00-CST-Asia/Harbin, GMT+08:00-CST-Asia/
 Chongqing, GMT+08:00-CST-Asia/Urumqi, GMT+08:00-CST-Asia/Kashgar, GMT-05:00-
 COT-America/Bogota, GMT-06:00-CST-America/Costa_Rica, GMT-04:00-CDT-America/
 Havana, GMT-01:00-CVT-Atlantic/Cape_Verde, GMT+07:00-CXT-Indian/Christmas,
 GMT+02:00-EET-Asia/Nicosia, GMT+01:00-CET-Europe/Prague, GMT+01:00-CET-
 Europe/Berlin, GMT+03:00-EAT-Africa/Djibouti, GMT+01:00-CET-Europe/Copenhagen,
 GMT-04:00-AST-America/Dominica, GMT-04:00-AST-America/Santo_Domingo, GMT
 +01:00-CET-Africa/Algiers, GMT-05:00-ECT-America/Guayaquil, GMT-06:00-GALT-
 Pacific/Galapagos, GMT+02:00-EET-Europe/Tallinn, GMT+02:00-EET-Africa/Cairo, GMT
 +00:00-WET-Africa/El_Aaiun, GMT+03:00-EAT-Africa/Asmara, GMT+01:00-CET-Europe/
 Madrid, GMT+01:00-CET-Africa/Ceuta, GMT+00:00-WET-Atlantic/Canary, GMT+03:00-
 EAT-Africa/Addis_Ababa, GMT+02:00-EET-Europe/Helsinki, GMT+12:00-FJT-Pacific/
 Fiji, GMT-03:00-FKST-Atlantic/Stanley, GMT+10:00-CHUT-Pacific/Chuuk, GMT+11:00-
 PONT-Pacific/Pohnpei, GMT+11:00-KOST-Pacific/Kosrae, GMT+00:00-WET-Atlantic/
 Faroe, GMT+01:00-CET-Europe/Paris, GMT+01:00-WAT-Africa/Libreville, GMT+00:00-
 GMT-Europe/London, GMT-04:00-AST-America/Grenada, GMT+04:00-GET-Asia/Tbilisi,
 GMT-03:00-GFT-America/Cayenne, GMT+00:00-GMT-Europe/Guernsey, GMT+00:00-
 GMT-Africa/Accra, GMT+01:00-CET-Europe/Gibraltar, GMT-03:00-WGT-America/
 Godthab, GMT+00:00-GMT-America/Danmarkshavn, GMT-01:00-EGT-America/
 Scoresbysund, GMT-03:00-ADT-America/Thule, GMT+00:00-GMT-Africa/Banjul, GMT
 +00:00-GMT-Africa/Conakry, GMT-04:00-AST-America/Guadeloupe, GMT+01:00-WAT-
 Africa/Malabo, GMT+02:00-EET-Europe/Athens, GMT-02:00-GST-Atlantic/
 South_Georgia, GMT-06:00-CST-America/Guatemala, GMT+10:00-ChST-Pacific/Guam,
 GMT+00:00-GMT-Africa/Bissau, GMT-04:00-GYT-America/Guyana, GMT+08:00-HKT-
 Asia/Hong_Kong, GMT-06:00-CST-America/Tegucigalpa, GMT+01:00-CET-Europe/
 Zagreb, GMT-05:00-EST-America/Port-au-Prince, GMT+01:00-CET-Europe/Budapest,
 GMT+07:00-WIT-Asia/Jakarta, GMT+07:00-WIT-Asia/Pontianak, GMT+08:00-CIT-Asia/
 Makassar, GMT+09:00-EIT-Asia/Jayapura, GMT+00:00-GMT-Europe/Dublin, GMT+02:00-
 IST-Asia/Jerusalem, GMT+00:00-GMT-Europe/Isle_of_Man, GMT+05:30-IST-Asia/
 Kolkata, GMT+06:00-IOT-Indian/Chagos, GMT+03:00-AST-Asia/Baghdad, GMT+03:30-
 IRST-Asia/Tehran, GMT+00:00-GMT-Atlantic/Reykjavik, GMT+01:00-CET-Europe/Rome,
 GMT+00:00-GMT-Europe/Jersey, GMT-05:00-EST-America/Jamaica, GMT+02:00-EET-
 Asia/Amman, GMT+09:00-JST-Asia/Tokyo, GMT+03:00-EAT-Africa/Nairobi, GMT+06:00-
 KGT-Asia/Bishkek, GMT+07:00-ICT-Asia/Phnom_Penh, GMT+12:00-GILT-Pacific/
 Tarawa, GMT+13:00-PHOT-Pacific/Enderbury, GMT+14:00-LINT-Pacific/Kiritimati, GMT
 +03:00-EAT-Indian/Comoro, GMT-04:00-AST-America/St_Kitts, GMT+09:00-KST-Asia/
 Pyongyang, GMT+09:00-KST-Asia/Seoul, GMT+03:00-AST-Asia/Kuwait, GMT-05:00-EST-
 America/Cayman, GMT+06:00-ALMT-Asia/Almaty, GMT+06:00-QYZT-Asia/Qyzylorda,
 GMT+05:00-AQTT-Asia/Aqtobe, GMT+05:00-AQTT-Asia/Aqtau, GMT+05:00-ORAT-Asia/

Oral, GMT+07:00-ICT-Asia/Vientiane, GMT+02:00-EET-Asia/Beirut, GMT-04:00-AST-America/St_Lucia, GMT+01:00-CET-Europe/Vaduz, GMT+05:30-IST-Asia/Colombo, GMT+00:00-GMT-Africa/Monrovia, GMT+02:00-SAST-Africa/Maseru, GMT+02:00-EET-Europe/Vilnius, GMT+01:00-CET-Europe/Luxembourg, GMT+02:00-EET-Europe/Riga, GMT+02:00-EET-Africa/Tripoli, GMT+00:00-WET-Africa/Casablanca, GMT+01:00-CET-Europe/Monaco, GMT+02:00-EET-Europe/Chisinau, GMT+01:00-CET-Europe/Podgorica, GMT-04:00-AST-America/Marigot, GMT+03:00-EAT-Indian/Antananarivo, GMT+12:00-MHT-Pacific/Majuro, GMT+12:00-MHT-Pacific/Kwajalein, GMT+01:00-CET-Europe/Skopje, GMT+00:00-GMT-Africa/Bamako, GMT+06:30-MMT-Asia/Rangoon, GMT+08:00-ULAT-Asia/Ulaanbaatar, GMT+07:00-HOVT-Asia/Hovd, GMT+08:00-CHOT-Asia/Choibalsan, GMT+08:00-CST-Asia/Macau, GMT+10:00-ChST-Pacific/Saipan, GMT-04:00-AST-America/Martinique, GMT+00:00-GMT-Africa/Nouakchott, GMT-04:00-AST-America/Montserrat, GMT+01:00-CET-Europe/Malta, GMT+04:00-MUT-Indian/Mauritius, GMT+05:00-MVT-Indian/Maldives, GMT+02:00-CAT-Africa/Blantyre, GMT-06:00-CST-America/Mexico_City, GMT-06:00-CST-America/Cancun, GMT-06:00-CST-America/Merida, GMT-06:00-CST-America/Monterrey, GMT-05:00-CDT-America/Matamoros, GMT-07:00-MST-America/Mazatlan, GMT-07:00-MST-America/Chihuahua, GMT-06:00-MDT-America/Ojinaga, GMT-07:00-MST-America/Hermosillo, GMT-07:00-PDT-America/Tijuana, GMT-08:00-PST-America/Santa_Isabel, GMT-06:00-CST-America/Bahia_Banderas, GMT+08:00-MYT-Asia/Kuala_Lumpur, GMT+08:00-MYT-Asia/Kuching, GMT+02:00-CAT-Africa/Maputo, GMT+02:00-WAST-Africa/Windhoek, GMT+11:00-NCT-Pacific/Noumea, GMT+01:00-WAT-Africa/Niamey, GMT+11:30-NFT-Pacific/Norfolk, GMT+01:00-WAT-Africa/Lagos, GMT-06:00-CST-America/Managua, GMT+01:00-CET-Europe/Amsterdam, GMT+01:00-CET-Europe/Oslo, GMT+05:45-NPT-Asia/Kathmandu, GMT+12:00-NRT-Pacific/Nauru, GMT-11:00-NUT-Pacific/Niue, GMT+13:00-NZDT-Pacific/Auckland, GMT+13:45-CHADT-Pacific/Chatham, GMT+04:00-GST-Asia/Muscat, GMT-05:00-EST-America/Panama, GMT-05:00-PET-America/Lima, GMT-10:00-TAHT-Pacific/Tahiti, GMT-09:30-MART-Pacific/Marquesas, GMT-09:00-GAMT-Pacific/Gambier, GMT+10:00-PGT-Pacific/Port_Moresby, GMT+08:00-PHT-Asia/Manila, GMT+05:00-PKT-Asia/Karachi, GMT+01:00-CET-Europe/Warsaw, GMT-02:00-PMDT-America/Miquelon, GMT-08:00-PST-Pacific/Pitcairn, GMT-04:00-AST-America/Puerto_Rico, GMT+02:00-EET-Asia/Gaza, GMT+02:00-EET-Asia/Hebron, GMT+00:00-WET-Europe/Lisbon, GMT+00:00-WET-Atlantic/Madeira, GMT-01:00-AZOT-Atlantic/Azores, GMT+09:00-PWT-Pacific/Palau, GMT-03:00-PYST-America/Asuncion, GMT+03:00-AST-Asia/Qatar, GMT+04:00-RET-Indian/Reunion, GMT+02:00-EET-Europe/Bucharest, GMT+01:00-CET-Europe/Belgrade, GMT+03:00-FET-Europe/Kaliningrad, GMT+04:00-MSK-Europe/Moscow, GMT+04:00-VOLT-Europe/Volgograd, GMT+04:00-SAMT-Europe/Samara, GMT+06:00-YEKT-Asia/Yekaterinburg, GMT+07:00-OMST-Asia/Omsk, GMT+07:00-NOVT-Asia/Novosibirsk, GMT+07:00-NOVT-Asia/Novokuznetsk, GMT+08:00-KRAT-Asia/Krasnoyarsk, GMT+09:00-IRKT-Asia/Irkutsk, GMT+10:00-YAKT-Asia/Yakutsk, GMT+11:00-VLAT-Asia/Vladivostok, GMT+11:00-SAKT-Asia/Sakhalin, GMT+12:00-MAGT-Asia/Magadan, GMT+12:00-PETT-Asia/Kamchatka, GMT+12:00-ANAT-Asia/Anadyr, GMT+02:00-CAT-Africa/Kigali, GMT+03:00-AST-Asia/Riyadh, GMT+11:00-SBT-Pacific/Guadalcanal, GMT+04:00-SCT-Indian/Mahe, GMT+03:00-EAT-Africa/Khartoum, GMT+01:00-CET-Europe/Stockholm, GMT+08:00-SGT-Asia/Singapore, GMT+00:00-GMT-Atlantic/St_Helena, GMT+01:00-CET-Europe/Ljubljana, GMT+01:00-CET-Arctic/Longyearbyen, GMT+01:00-CET-Europe/Bratislava, GMT+00:00-GMT-Africa/Freetown, GMT+01:00-CET-Europe/San_Marino, GMT+00:00-GMT-Africa/Dakar, GMT+03:00-EAT-Africa/Mogadishu, GMT-03:00-SRT-America/Paramaribo, GMT+00:00-GMT-Africa/Sao_Tome, GMT-06:00-CST-America/El_Salvador, GMT+02:00-EET-Asia/Damascus, GMT+02:00-SAST-Africa/Mbabane, GMT-04:00-EDT-America/Grand_Turk, GMT+01:00-WAT-

Africa/Ndjamena, GMT+05:00-TFT-Indian/Kerguelen, GMT+00:00-GMT-Africa/Lome, GMT+07:00-ICT-Asia/Bangkok, GMT+05:00-TJT-Asia/Dushanbe, GMT-10:00-TKT-Pacific/Fakaofu, GMT+09:00-TLT-Asia/Dili, GMT+05:00-TMT-Asia/Ashgabat, GMT+01:00-CET-Africa/Tunis, GMT+13:00-TOT-Pacific/Tongatapu, GMT+02:00-EET-Europe/Istanbul, GMT-04:00-AST-America/Port_of_Spain, GMT+12:00-TVT-Pacific/Funafuti, GMT+08:00-CST-Asia/Taipei, GMT+03:00-EAT-Africa/Dar_es_Salaam, GMT+02:00-EET-Europe/Kiev, GMT+02:00-EET-Europe/Uzhgorod, GMT+02:00-EET-Europe/Zaporozhye, GMT+02:00-EET-Europe/Simferopol, GMT+03:00-EAT-Africa/Kampala, GMT-10:00-HST-Pacific/Johnston, GMT-11:00-SST-Pacific/Midway, GMT+12:00-WAKT-Pacific/Wake, GMT-04:00-EDT-America/New_York, GMT-04:00-EDT-America/Detroit, GMT-04:00-EDT-America/Kentucky/Louisville, GMT-04:00-EDT-America/Kentucky/Monticello, GMT-04:00-EDT-America/Indiana/Indianapolis, GMT-04:00-EDT-America/Indiana/Vincennes, GMT-04:00-EDT-America/Indiana/Winamac, GMT-04:00-EDT-America/Indiana/Marengo, GMT-04:00-EDT-America/Indiana/Petersburg, GMT-04:00-EDT-America/Indiana/Vevay, GMT-05:00-CDT-America/Chicago, GMT-05:00-CDT-America/Indiana/Tell_City, GMT-05:00-CDT-America/Indiana/Knox, GMT-05:00-CDT-America/Menominee, GMT-05:00-CDT-America/North_Dakota/Center, GMT-05:00-CDT-America/North_Dakota/New_Salem, GMT-05:00-CDT-America/North_Dakota/Beulah, GMT-06:00-MDT-America/Denver, GMT-06:00-MDT-America/Boise, GMT-06:00-MDT-America/Shiprock, GMT-07:00-MST-America/Phoenix, GMT-07:00-PDT-America/Los_Angeles, GMT-08:00-AKDT-America/Anchorage, GMT-08:00-AKDT-America/Juneau, GMT-08:00-AKDT-America/Sitka, GMT-08:00-AKDT-America/Yakutat, GMT-08:00-AKDT-America/Nome, GMT-09:00-HADT-America/Adak, GMT-08:00-MeST-America/Metlakatla, GMT-10:00-HST-Pacific/Honolulu, GMT-03:00-UYT-America/Montevideo, GMT+05:00-UZT-Asia/Samarkand, GMT+05:00-UZT-Asia/Tashkent, GMT+01:00-CET-Europe/Vatican, GMT-04:00-AST-America/St_Vincent, GMT-04:30-VET-America/Caracas, GMT-04:00-AST-America/Tortola, GMT-04:00-AST-America/St_Thomas, GMT+07:00-ICT-Asia/Ho_Chi_Minh, GMT+11:00-VUT-Pacific/Efate, GMT+12:00-WFT-Pacific/Wallis, GMT+14:00-WSDT-Pacific/Apia, GMT+03:00-AST-Asia/Aden, GMT+03:00-EAT-Indian/Mayotte, GMT+02:00-SAST-Africa/Johannesburg, GMT+02:00-CAT-Africa/Lusaka, GMT+02:00-CAT-Africa/Harare

grantQuotaMaxClient

Percentage of shared quota to be granted at a time for maxClient. Default value: 10
Maximum value: 100

exclusiveQuotaMaxClient

Percentage of maxClient to be given to PEs. Default value: 80 Maximum value: 100

grantQuotaSpillOver

Percentage of shared quota to be granted at a time for spillover. Default value: 10
Maximum value: 100

exclusiveQuotaSpillOver

Percentage of maximum limit to be given to PEs. Default value: 80 Maximum value: 100

useproxyport

Enable/Disable use_proxy_port setting Possible values: ENABLED, DISABLED Default value: ENABLED

internaluserlogin

Enables/disables the internal user from logging in to the appliance. Before disabling internal user login, you must have key-based authentication set up on the appliance. The file name for the key pair must be "ns_comm_key". Possible values: ENABLED, DISABLED Default value: ENABLED

aftpAllowRandomSourcePort

Allow the FTP server to come from a random source port for active FTP data connections Possible values: ENABLED, DISABLED Default value: DISABLED

icaPorts

The ICA ports on the Web server. This allows the system to perform connection off-load for any client request that has a destination port matching one of these configured ports. Minimum value: 1

[Top](#)

unset ns param**Synopsis**

```
unset ns param [-ftpPortRange] [-crPortRange] [-timezone] [-aftpAllowRandomSourcePort] [-httpPort] [-maxConn] [-maxReq] [-cip] [-cipHeader] [-cookieversion] [-secureCookie] [-pmtuMin] [-pmtuTimeout] [-grantQuotaMaxClient] [-exclusiveQuotaMaxClient] [-grantQuotaSpillOver] [-exclusiveQuotaSpillOver] [-useproxyport] [-internaluserlogin] [-icaPorts]
```

Description

Removes the attributes of the NetScaler parameters. Attributes for which a default value is available revert to their default values. Refer to the 'set ns param' command for a description of the parameters..Refer to the set ns param command for meanings of the arguments.

[Top](#)

show ns param**Synopsis**

```
show ns param
```

Description

Displays the information of the parameters of the NetScaler appliance that were set by using the 'set ns param' command.

[Top](#)

ns acls6

[[clear](#) | [apply](#) | [renumber](#)]

clear ns acls6

Synopsis

clear ns acls6

Description

Removes all simple ACL6 rules from the NetScaler appliance. This operation does not require an explicit apply.

Example

```
clear ns acls6
```

[Top](#)

apply ns acls6

Synopsis

apply ns acls6

Description

Updates the ACL6 rules' memory tree (lookup table), adding any new ACL6 rules and applying any modifications to existing ACL rules. The lookup table includes the configuration of all the ACL6 rules on the NetScaler appliance. The NetScaler appliance uses the lookup table (not the configuration file) to filter the incoming IPv4 packets.

Example

```
apply ns acls6
```

[Top](#)

renumber ns acls6

Synopsis

renumber ns acls6

Description

Renumbers the priorities of ACL6 rules to multiples of 10. To commit this operation, you must apply the ACL6s. Enables you to assign a new ACL6 rule a priority that is between two existing, consecutively numbered priorities. For example, if two ACL6s, ACL6-1 and ACL6-2, have priorities 2 and 3 renumbering changes those priorities to 20 and 30. You can then add ACL6-3 with priority 25.

Example

```
renumber ac1s6
```

[Top](#)

ns pbrs

[[renumber](#) | [clear](#) | [apply](#)]

renumber ns pbrs

Synopsis

```
renumber ns pbrs
```

Description

Renumbers the priorities of PBRs to multiples of 10. To commit this operation, you must apply the PBRs. Enables you to assign a new PBR a priority that is between two existing, consecutively numbered priorities. For example, if two PBRs, PBR1 and PBR2, have priorities 2 and 3 renumbering changes those priorities to 20 and 30. You can then add PBR3 with priority 25.

Example

```
renumber pbrs
```

[Top](#)

clear ns pbrs

Synopsis

```
clear ns pbrs
```

Description

Removes all PBRs from the NetScaler appliance. This operation does not require an explicit apply.

Example

```
clear ns pbrs
```

[Top](#)

apply ns pbrs

Synopsis

apply ns pbrs

Description

Updates the PBR's memory tree (lookup table), adding any new PBR and applying any modifications to existing PBRs. The lookup table includes the configuration of all the extended PBRs on the NetScaler appliance. The NetScaler appliance uses the lookup table (not the configuration file) to filter the outgoing IPv4 packets.

Example

```
apply ns pbrs
```

[Top](#)

ns connectiontable

show ns connectiontable

Synopsis

show ns connectiontable [<filterexpression>] [-detail <detail> ...]

Description

Displays the current TCP/IP connection table.

Parameters

filterexpression

Expression using which TCP/IP connections must be filtered. Maximum length of filter is 255 and it can be of the following format: "<expression> \[<relop> <expression>\]" where, <relop> can be the && or the || relational operators. <expression> is a string in the following format: <qualifier> <operator> <qualifier-value> where, <operator> can be any one of the following (except the commas): ==, eq, !=, neq, >, gt, <, lt, >=, ge, <=, le, BETWEEN Following are the valid qualifier - qualifier value combinations: SOURCEIP - A valid IP address SOURCEPORT - A valid port number DESTIP - A valid IP address DESTPORT - A valid port number IP - A valid IP address PORT - A valid port number IDLETIME - A positive integer indicating the idle time SVCNAME - The name of a service VSVRNAME - The name of a vserver STATE - CLOSE_WAIT, CLOSED, CLOSING, ESTABLISHED, FIN_WAIT_1, FIN_WAIT_2, LAST_ACK, LISTEN, SYN_RECEIVED, SYN_SENT, TIME_WAIT SVCTYPE - HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, RPCSVR, RPCSVRS, RPCCLNT, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, MONITOR, MONITOR_UDP, MONITOR_PING, SIP_UDP, MYSQL, MSSQL, UNKNOWN.

link

Display link information if available

name

Display name instead of IP for local entities

detail

Specify display options for the connection table. * LINK - Displays the linked PCB (Protocol Control Block). * NAME - Displays along with the service name. * CONNFAILOVER - Displays PCB with connection failover. * FULL - Displays all available details.

ns limitSessions

[[show](#) | [clear](#)]

show ns limitSessions

Synopsis

show ns limitSessions <limitIdentifier> [-detail]

Description

Displays the rate limit sessions available on the appliance.

Parameters**limitIdentifier**

Name of the rate limit identifier for which to display the sessions.

detail

Show the individual hash values.

[Top](#)

clear ns limitSessions

Synopsis

clear ns limitSessions <limitIdentifier>

Description

Clears the rate limit sessions available on the appliance.

Parameters**limitIdentifier**

Name of the rate limit identifier for which the sessions must be cleared.

[Top](#)

ns hostName

[[set](#) | [show](#)]

set ns hostName

Synopsis

set ns hostName <hostName> [-ownerNode <positive_integer>]

Description

Sets the hostname for the NetScaler appliance. The hostname is displayed on the shell prompt.

Parameters

hostName

Host name for the NetScaler appliance.

ownerNode

ID of the cluster node for which you are setting the hostname. Can be configured only through the cluster IP address. Default value: 255 Maximum value: 31

Example

```
set ns hostname nspri
```

[Top](#)

show ns hostName

Synopsis

show ns hostName

Description

Displays the host name of the system.

Example

```
show ns hostname
```

[Top](#)

ns surgeQ

flush ns surgeQ

Synopsis

flush ns surgeQ [-name <string> [-serverName <string> <port>]]

Description

Flushes the connections that are waiting in SurgeQ. SurgeQ contains the client connections waiting for a server connection.

Parameters

name

Name of a virtual server, service or service group for which the SurgeQ must be flushed.

serverName

Name of a service group member. This argument is needed when you want to flush the SurgeQ of a service group.

Example

```
To flush the surgeQ system wide, use the command:
flush ns SurgeQ.
To flush the surgeQ specific to a vserver/service/
svcgrp use the command: flush ns SurgeQ -name
<name>
To flush the surgeQ specific to a svcgrp member,
use the command: flush ns surgeQ [-name <string>
[-serverName <string> <port>]]
```

ns feature

[[enable](#) | [disable](#) | [show](#)]

enable ns feature

Synopsis

enable ns feature <feature> ...

Description

Enables NetScaler feature(s).

Parameters

feature

Feature to be enabled. Multiple features can be specified by providing a blank space between each feature.

Example

```
enable ns feature sc
This CLI command enables the SureConnect feature.
```

[Top](#)

disable ns feature

Synopsis

disable ns feature <feature> ...

Description

Disables NetScaler feature(s).

Parameters

feature

Feature to be disabled. Multiple features can be specified by providing a blank space between each feature.

[Top](#)

show ns feature

Synopsis

show ns feature

Description

Displays the current state of NetScaler features.

[Top](#)

ns mode

[[enable](#) | [disable](#) | [show](#)]

enable ns mode

Synopsis

enable ns mode <Mode> ...

Description

Enables NetScaler mode(s).

Parameters

Mode

Mode to be enabled. Multiple modes can be specified by providing a blank space between each mode.

Example

```
This CLI command enables the system's client keep-  
alive feature:  
enable ns mode CKA
```

[Top](#)

disable ns mode

Synopsis

disable ns mode <Mode> ...

Description

Disables NetScaler mode(s).

Parameters

Mode

Mode to be disabled. Multiple modes can be specified by providing a blank space between each mode.

Example

```
This example shows the command to disable the
system's client keep-alive feature:
disable ns mode CKA
```

[Top](#)

show ns mode

Synopsis

show ns mode

Description

Displays the current state of NetScaler modes.

[Top](#)

ns dhcpParams

[[set](#) | [unset](#) | [show](#)]

set ns dhcpParams

Synopsis

set ns dhcpParams [-dhcpClient (ON | OFF)] [-saveroute (ON | OFF)]

Description

Sets the DHCP client parameters.

Parameters

dhcpClient

Enables DHCP client to acquire IP address from the DHCP server in the next boot.
When set to OFF, disables the DHCP client in the next boot. Possible values: ON, OFF
Default value: OFF

saveroute

DHCP acquired routes are saved on the NetScaler appliance. Possible values: ON, OFF
Default value: OFF

[Top](#)

unset ns dhcpParams

Synopsis

unset ns dhcpParams [-dhcpClient] [-saveroute]

Description

Use this command to remove ns dhcpParams settings. Refer to the set ns dhcpParams command for meanings of the arguments.

[Top](#)

show ns dhcpParams

Synopsis

show ns dhcpParams

Description

Displays the parameters configured for the DHCP client.

[Top](#)

ns dhcpIp

release ns dhcpIp

Synopsis

release ns dhcpIp

Description

Releases the IP address acquired by the DHCP client.

ns spParams

[[set](#) | [unset](#) | [show](#)]

set ns spParams

Synopsis

set ns spParams [-baseThreshold <integer>] [-throttle <throttle>]

Description

Sets surge protection attributes on the appliance.

Parameters

baseThreshold

Maximum number of server connections that can be opened before surge protection is activated. Default value: 200 Maximum value: 32767

throttle

Rate at which the system opens connections to the server. Possible values: Aggressive, Normal, Relaxed Default value: NORM_SP_TABLE

Example

```
set ns sparams -baseThreshold 1000 -throttle
aggressive
set ns sparams -throttle relaxed
```

[Top](#)

unset ns spParams

Synopsis

unset ns spParams [-baseThreshold] [-throttle]

Description

Use this command to remove ns spParams settings. Refer to the set ns spParams command for meanings of the arguments.

[Top](#)

show ns spParams

Synopsis

show ns spParams

Description

Displays the surge protection configuration on the appliance. Surge protection parameters are set by using the 'set ns spParams' command.

Example

```
> show ns sparams
    Surge Protection parameters:
    BaseThreshold:    200
    Throttle:    Normal
Done
```

[Top](#)

ns tcpbufParam

[[set](#) | [unset](#) | [show](#)]

set ns tcpbufParam

Synopsis

```
set ns tcpbufParam [-size <KBytes>] [-memLimit <MBytes>]
```

Description

Sets the attributes for the TCP buffering per connection.

Parameters

size

TCP buffering size per connection, in kilobytes. Default value: 64 Minimum value: 4
Maximum value: 20480

memLimit

Maximum memory, in megabytes, that can be used for buffering. Default value: 64

[Top](#)

unset ns tcpbufParam

Synopsis

```
unset ns tcpbufParam [-size] [-memLimit]
```

Description

Use this command to remove ns tcpbufParam settings. Refer to the set ns tcpbufParam command for meanings of the arguments.

[Top](#)

show ns tcpbufParam

Synopsis

```
show ns tcpbufParam
```

Description

Displays the TCP buffering configuration on the appliance.

Example

An example of this command's output is as follows:
 TCP buffer size: 64KBytes
 TCP buffer percentage: 50%

[Top](#)

ns tcpParam

[\[set | unset | show \]](#)

set ns tcpParam

Synopsis

```
set ns tcpParam [-WS ( ENABLED | DISABLED )] [-WSVal <positive_integer>] [-SACK
( ENABLED | DISABLED )] [-learnVsvrMSS ( ENABLED | DISABLED )] [-maxBurst
<positive_integer>] [-initialCwnd <positive_integer>] [-delayedAck <positive_integer>]
[-downStateRST ( ENABLED | DISABLED )] [-nagle ( ENABLED | DISABLED )] [-
limitedPersist ( ENABLED | DISABLED )] [-oooQSize <positive_integer>] [-ackOnPush
( ENABLED | DISABLED )] [-maxPktPerMss <integer>] [-pktPerRetx <integer>] [-minRTO
<integer>] [-slowStartIncr <integer>] [-maxDynServerProbes <positive_integer>] [-
synHoldFastGiveup <positive_integer>] [-maxSynholdPerprobe <positive_integer>] [-
maxSynhold <positive_integer>] [-mssLearnInterval <positive_integer>] [-mssLearnDelay
<positive_integer>] [-maxTimeWaitConn <positive_integer>] [-maxSynAckRetx
<positive_integer>] [-synAttackDetection ( ENABLED | DISABLED )] [-connFlushIfNoMem
<connFlushIfNoMem>] [-connFlushThres <positive_integer>] [-
mptcpConCloseOnPassiveSF ( ENABLED | DISABLED )] [-mptcpChecksum ( ENABLED |
DISABLED )] [-mptcpSFtimeout <secs>] [-mptcpSFReplaceTimeout <secs>] [-mptcpMaxSF
<positive_integer>] [-mptcpMaxPendingSF <positive_integer>] [-
mptcpPendingJoinThreshold <positive_integer>] [-mptcpRTOsToSwitchSF
<positive_integer>] [-mptcpUseBackupOnDSS ( ENABLED | DISABLED )] [-TcpMaxRetries
<positive_integer>] [-mptcpImmediateSFCloseOnFIN ( ENABLED | DISABLED )]
```

Description

Sets the TCP parameters for the NetScaler appliance.

Parameters

WS

Enable or disable window scaling. Possible values: ENABLED, DISABLED Default value: DISABLED

WSVal

Factor used to calculate the new window size. This argument is needed only when the window scaling is enabled. Default value: 4 Maximum value: 8

SACK

Enable or disable Selective ACKnowledgement (SACK). Possible values: ENABLED, DISABLED Default value: DISABLED

learnVsvrMSS

Enable or disable maximum segment size (MSS) learning for virtual servers. Possible values: ENABLED, DISABLED Default value: DISABLED

maxBurst

Maximum number of TCP segments allowed in a burst. Default value: 6 Minimum value: 1 Maximum value: 255

initialCwnd

Initial maximum upper limit on the number of TCP packets that can be outstanding on the TCP link to the server. Default value: 4 Minimum value: 1 Maximum value: 44

recvBuffSize

TCP Receive buffer size Default value: 8190 Minimum value: 8190 Maximum value: 20971520

delayedAck

Timeout for TCP delayed ACK, in milliseconds. Default value: 100 Minimum value: 10 Maximum value: 300

downStateRST

Flag to switch on RST on down services. Possible values: ENABLED, DISABLED Default value: DISABLED

nagle

Enable or disable the Nagle algorithm on TCP connections. Possible values: ENABLED, DISABLED Default value: DISABLED

limitedPersist

Limit the number of persist (zero window) probes. Possible values: ENABLED, DISABLED Default value: ENABLED

oooQSize

Maximum size of out-of-order packets queue. A value of 0 means infinite. Default value: 64 Maximum value: 65535

ackOnPush

Send immediate positive acknowledgement (ACK) on receipt of TCP packets when doing Web 2.0 PUSH. Possible values: ENABLED, DISABLED Default value: ENABLED

maxPktPerMss

Maximum number of TCP packets allowed per maximum segment size (MSS). Maximum value: 1460

pktPerRetx

Maximum limit on the number of packets that should be retransmitted on receiving a partial ACK. Default value: 1 Minimum value: 1 Maximum value: 100

minRTO

Minimum retransmission timeout, in milliseconds. Default value: 1000 Minimum value: 10 Maximum value: 64000

slowStartIncr

Multiplier that determines the rate at which slow start increases the size of the TCP transmission window after each acknowledgement of successful transmission. Default value: 2 Minimum value: 1 Maximum value: 100

maxDynServerProbes

Maximum number of probes that NetScaler can send out in 10 milliseconds, to dynamically learn a service. NetScaler probes for the existence of the origin in case of wildcard virtual server or services. Default value: 7 Minimum value: 1 Maximum value: 65535

synHoldFastGiveup

Maximum threshold. After crossing this threshold number of outstanding probes for origin, the NetScaler reduces the number of connection retries for probe connections. Default value: 1024 Minimum value: 256 Maximum value: 65535

maxSynholdPerprobe

Limit the number of client connections (SYN) waiting for status of single probe. Any new SYN packets will be dropped. Default value: 128 Minimum value: 1 Maximum value: 255

maxSynhold

Limit the number of client connections (SYN) waiting for status of probe system wide. Any new SYN packets will be dropped. Default value: 16384 Minimum value: 256 Maximum value: 65535

mssLearnInterval

Duration, in seconds, to sample the Maximum Segment Size (MSS) of the services. The NetScaler appliance determines the best MSS to set for the virtual server based on this sampling. The argument to enable maximum segment size (MSS) for virtual servers must be enabled. Default value: 180 Minimum value: 1 Maximum value: 1048576

mssLearnDelay

Frequency, in seconds, at which the virtual servers learn the Maximum segment size (MSS) from the services. The argument to enable maximum segment size (MSS) for virtual servers must be enabled. Default value: 3600 Minimum value: 1 Maximum value: 1048576

maxTimeWaitConn

Maximum number of connections to hold in the TCP TIME_WAIT state. New connections entering TIME_WAIT state are proactively cleaned up. Default value: 7000 Minimum value: 1

KAprrobeUpdateLastactivity

Update last activity for KA probes Possible values: ENABLED, DISABLED Default value: ENABLED

maxSynAckRetx

When 'syncookie' is disabled in the TCP profile that is bound to the virtual server or service, and the number of TCP SYN+ACK retransmission by NetScaler for that virtual server or service crosses this threshold, the NetScaler appliance responds by using the TCP SYN-Cookie mechanism. Default value: 100 Minimum value: 100 Maximum value: 1048576

synAttackDetection

Detect TCP SYN packet flood and send an SNMP trap. Possible values: ENABLED, DISABLED Default value: ENABLED

connFlushIfNoMem

Flush an existing connection if no memory can be obtained for new connection. HALF_CLOSED_AND_IDLE: Flush a connection that is closed by us but not by peer, or failing that, a connection that is past configured idle time. New connection fails if no such connection can be found. FIFO: If no half-closed or idle connection can be found, flush the oldest non-management connection, even if it is active. New connection fails if the oldest few connections are management connections. Note: If you enable this setting, you should also consider lowering the zombie timeout and half-close timeout (see NSCLI command: set ns timeout). See Also: connFlushThres argument below. Possible values: NONE, HALFCLOSED_AND_IDLE, FIFO Default value: NSA_CONNFLUSH_NONE

connFlushThres

Flush an existing connection (as configured through -connFlushIfNoMem FIFO) if the system has more than specified number of connections, and a new connection is to be established. Note: This value may be rounded down to be a whole multiple of the number of packet engines running. Minimum value: 1

mptcpConCloseOnPassiveSF

Accept DATA_FIN/FAST_CLOSE on passive subflow Possible values: ENABLED, DISABLED Default value: ENABLED

mptcpChecksum

Use MPTCP DSS checksum Possible values: ENABLED, DISABLED Default value: ENABLED

mptcpSFtimeout

The timeout value in seconds for idle mptcp subflows. If this timeout is not set, idle subflows are cleared after cltTimeout of vserver Maximum value: 31536000

mptcpSFReplaceTimeout

The minimum idle time value in seconds for idle mptcp subflows after which the subflow is replaced by new incoming subflow if maximum subflow limit is reached. The priority for replacement is given to those subflow without any transaction Default value: 10 Maximum value: 31536000

mptcpMaxSF

Maximum number of subflow connections supported in established state per mptcp connection. Default value: 4 Minimum value: 2 Maximum value: 6

mptcpMaxPendingSF

Maximum number of subflow connections supported in pending join state per mptcp connection. Default value: 4 Maximum value: 4

mptcpPendingJoinThreshold

Maximum system level pending join connections allowed. Maximum value: 4294967294

mptcpRTOsToSwitchSF

Number of RTO's at subflow level, after which MPCTP should start using other subflow. Default value: 2 Minimum value: 1 Maximum value: 6

mptcpUseBackupOnDSS

When enabled, if NS receives a DSS on a backup subflow, NS will start using that subflow to send data. And if disabled, NS will continue to transmit on current chosen subflow. In case there is some error on a subflow (like RTO's/RST etc.) then NS can choose a backup subflow irrespective of this tunable. Possible values: ENABLED, DISABLED Default value: ENABLED

TcpMaxRetries

Number of RTO's after which a connection should be freed. Default value: 7 Minimum value: 1 Maximum value: 7

mptcpImmediateSFCloseOnFIN

Allow subflows to close immediately on FIN before the DATA_FIN exchange is completed at mptcp level. Possible values: ENABLED, DISABLED Default value: DISABLED

[Top](#)

unset ns tcpParam**Synopsis**

```
unset ns tcpParam [-WS] [-WSVal] [-SACK] [-learnVsvrMSS] [-maxBurst] [-initialCwnd] [-delayedAck] [-downStateRST] [-nagle] [-limitedPersist] [-oooQSize] [-ackOnPush] [-maxPktPerMss] [-pktPerRetx] [-minRTO] [-slowStartIncr] [-maxDynServerProbes] [-synHoldFastGiveup] [-maxSynholdPerprobe] [-maxSynhold] [-mssLearnInterval] [-mssLearnDelay] [-maxTimeWaitConn] [-maxSynAckRetx] [-synAttackDetection] [-connFlushIfNoMem] [-connFlushThres] [-mptcpConCloseOnPassiveSF] [-mptcpChecksum] [-mptcpSFtimeout] [-mptcpSFReplaceTimeout] [-mptcpMaxSF] [-mptcpMaxPendingSF] [-mptcpPendingJoinThreshold] [-mptcpRTOsToSwitchSF] [-mptcpUseBackupOnDSS] [-TcpMaxRetries] [-mptcpImmediateSFCloseOnFIN]
```

Description

Use this command to remove ns tcpParam settings. Refer to the set ns tcpParam command for meanings of the arguments.

[Top](#)

show ns tcpParam**Synopsis**

```
show ns tcpParam
```

Description

Displays the TCP parameters configured on the NetScaler appliance.

[Top](#)

ns httpParam

[[set](#) | [unset](#) | [show](#)]

set ns httpParam

Synopsis

```
set ns httpParam [-dropInvalReqs ( ON | OFF )] [-markHttp09Inval ( ON | OFF )] [-markConnReqInval ( ON | OFF )] [-insNsSrvrHdr ( ON | OFF ) [<nsSrvrHdr>]] [-logErrResp ( ON | OFF )] [-conMultiplex ( ENABLED | DISABLED )] [-maxReusePool <positive_integer>]
```

Description

Sets the configurable HTTP parameters for the NetScaler appliance.

Parameters

dropInvalReqs

Drop invalid HTTP requests or responses. Possible values: ON, OFF Default value: OFF

markHttp09Inval

Mark HTTP/0.9 requests as invalid. Possible values: ON, OFF Default value: OFF

markConnReqInval

Mark CONNECT requests as invalid. Possible values: ON, OFF Default value: OFF

insNsSrvrHdr

Enable or disable NetScaler server header insertion for NetScaler generated HTTP responses. Possible values: ON, OFF Default value: OFF

logErrResp

Server header value to be inserted. Possible values: ON, OFF Default value: ON

conMultiplex

Reuse server connections for requests from more than one client connections. Possible values: ENABLED, DISABLED Default value: ENABLED

maxReusePool

Maximum limit on the number of connections, from the NetScaler to a particular server that are kept in the reuse pool. This setting is helpful for optimal memory utilization and for reducing the idle connections to the server just after the peak time.

Example

```
set ns httpParam -dropInvalReqs ON
```

[Top](#)

unset ns httpParam

Synopsis

unset ns httpParam [-dropInvalReqs] [-markHttp09Inval] [-markConnReqInval] [-insNsSrvrHdr] [-nsSrvrHdr] [-logErrResp] [-conMultiplex] [-maxReusePool]

Description

Use this command to remove ns httpParam settings. Refer to the set ns httpParam command for meanings of the arguments.

[Top](#)

show ns httpParam

Synopsis

show ns httpParam

Description

Displays the HTTP parameters configured on the NetScaler appliance.

[Top](#)

ns weblogparam

[[set](#) | [unset](#) | [show](#)]

set ns weblogparam

Synopsis

set ns weblogparam [-bufferSizeMB <positive_integer>] [-customReqHdrs <string> ...] [-customRspHdrs <string> ...]

Description

Sets the Weblog parameters.

Parameters

bufferSizeMB

Buffer size, in MB, allocated for log transaction data on the system. The maximum value is limited to the memory available on the system. Note: For the change in buffer size to take effect, you must disable and then re-enable the Web Server Logging feature on the appliance. Default value: 16 Minimum value: 1 Maximum value: 4294967294LU

customReqHdrs

Name(s) of HTTP request headers whose values should be exported by the Web Logging feature. A maximum of two header names can be configured, with each header name having a maximum length of 31 characters.

customRspHdrs

Name(s) of HTTP response headers whose values should be exported by the Web Logging feature. A maximum of two header names can be configured, with each header name having a maximum length of 31 characters.

[Top](#)

unset ns weblogparam**Synopsis**

unset ns weblogparam [-bufferSizeMB] [-customReqHdrs] [-customRspHdrs]

Description

Use this command to remove ns weblogparam settings. Refer to the set ns weblogparam command for meanings of the arguments.

[Top](#)

show ns weblogparam**Synopsis**

show ns weblogparam

Description

Displays the Weblog parameters.

[Top](#)

ns diameter

[[set](#) | [unset](#) | [show](#)]

set ns diameter**Synopsis**

set ns diameter [-identity <string>] [-realm <string>] [-serverClosePropagation (YES | NO)]

Description

Set the diameter configuration on NS.

Parameters**identity**

DiameterIdentity to be used by NS. DiameterIdentity is used to identify a Diameter node uniquely. Before setting up diameter configuration, Netscaler (as a Diameter node) MUST be assigned a unique DiameterIdentity. example => set ns diameter - identity netscaler.com Now whenever Netscaler system needs to use identity in diameter messages. It will use 'netscaler.com' as Origin-Host AVP as defined in RFC3588

realm

Diameter Realm to be used by NS. example => set ns diameter -realm com Now whenever Netscaler system needs to use realm in diameter messages. It will use 'com' as Origin-Realm AVP as defined in RFC3588

serverClosePropagation

when a Server connection goes down, whether to close the corresponding client connection if there were requests pending on the server. Possible values: YES, NO
Default value: NO

[Top](#)**unset ns diameter****Synopsis**

unset ns diameter -serverClosePropagation

Description

Use this command to remove ns diameter settings. Refer to the set ns diameter command for meanings of the arguments.

[Top](#)**show ns diameter****Synopsis**

show ns diameter

Description

Displays the diameter parameters configured on the NetScaler appliance.

[Top](#)**ns rateControl**

[[set](#) | [unset](#) | [show](#)]

set ns rateControl**Synopsis**

set ns rateControl [-tcpThreshold <positive_integer>] [-udpThreshold <positive_integer>] [-icmpThreshold <positive_integer>] [-tcprstThreshold <positive_integer>]

Description

Sets the UDP/TCP/ICMP packet rate controls for any application that is not configured at System (direct access to the backend through System).

Parameters**tcpThreshold**

Number of SYNs permitted per 10 milliseconds.

udpThreshold

Number of UDP packets permitted per 10 milliseconds.

icmpThreshold

Number of ICMP packets permitted per 10 milliseconds. Default value: 100

tcprstThreshold

The number of TCP RST packets permitted per 10 milli second. zero means rate control is disabled and 0xffffffff means every thing is rate controlled Default value: 100

Example

The following command will set the SYN rate to 100, icmp rate to 10 and the udp rate to unlimited.

```
set ns ratecontrol -tcpThreshold 100 -  
udpThreshold 0 -icmpThreshold 10
```

The 'show ns rate control' command can be used to view the current settings of the rate controls.

```
> show ns ratecontrol  
    UDP threshold:           0 per 10 ms  
    TCP threshold:           0 per 10 ms  
    ICMP threshold:         100 per 10 ms  
Done
```

[Top](#)

unset ns rateControl**Synopsis**

unset ns rateControl [-tcpThreshold] [-udpThreshold] [-icmpThreshold] [-tcprstThreshold]

Description

Use this command to remove ns rateControl settings. Refer to the set ns rateControl command for meanings of the arguments.

[Top](#)

show ns rateControl**Synopsis**

show ns rateControl

Description

Displays the values configured for rate control on the appliance.

Example

By default, there is no rate control for TCP/UDP and for ICMP it will be 100. The output of the "show ns ratecontrol" command, with default setting,

```
> show ns ratecontrol
      UDP threshold:          0 per 10 ms
      TCP threshold:          0 per 10 ms
      ICMP threshold:         100 per 10 ms
Done
```

[Top](#)

ns rpcNode

[[set](#) | [unset](#) | [show](#)]

set ns rpcNode

Synopsis

```
set ns rpcNode <IPAddress> {-password } [-srcIP <ip_addr|ipv6_addr|*>] [-secure ( YES | NO )]
```

Description

Sets the authentication attributes associated with peer system node. All system nodes use Remote Procedure Calls (RPC) to communicate.

Parameters

IPAddress

IP address of the node. This has to be in the same subnet as the NSIP address.

password

Password to be used in authentication with the peer system node.

srcIP

Source IP address to be used to communicate with the peer system node. The default value is 0, which means that the appliance uses the NSIP address as the source IP address.

secure

State of the channel when talking to the node. Possible values: YES, NO

Example

```
Example-1: Failover configuration
In a failover configuration define peer NS as:
    add node 1 10.101.4.87
Set peer ha-unit's password as:
    set ns rpcnode 10.101.4.87 -password
```

```
testpass -secure yes
```

System will now use the configured password to authenticate with its failover unit.

Example-2: GSLB configuration

In a GSLB configuration define peer NS GSLB site as:

```
add gslb site us_east_coast remote
206.123.3.4
```

Set peer GSLB-NS's password as:

```
set ns rpcnode 206.123.3.4 -password testrun
```

System will now use the configured password to authenticate with east-coast GSLB site.

[Top](#)

unset ns rpcNode

Synopsis

```
unset ns rpcNode <IPAddress> [-password] [-srcIP] [-secure]
```

Description

Use this command to remove ns rpcNode settings. Refer to the set ns rpcNode command for meanings of the arguments.

[Top](#)

show ns rpcNode

Synopsis

```
show ns rpcNode [<IPAddress>]
```

Description

Display a list of nodes currently communicating by using Remote Procedure Calls (RPC).

Parameters

IPAddress

IP address of the node.

Example

Following example shows list of nodes communicating using RPC:

```
> sh rpcnode
```

```
1)      IPAddress:      10.101.4.84 Password:  ..
8a7b474124957776b56cf03b28 Srcip: 1.1.1.1
2)      IPAddress:      10.101.4.87
Password:  ..ca2a035465d22c          Srcip:
```

```
2.2.2.2
Done
```

[Top](#)

ns timeout

[\[set | unset | show \]](#)

set ns timeout

Synopsis

```
set ns timeout [-zombie <positive_integer>] [-httpClient <positive_integer>] [-
httpServer <positive_integer>] [-tcpClient <positive_integer>] [-tcpServer
<positive_integer>] [-anyClient <positive_integer>] [-anyServer <positive_integer>] [-
halfclose <positive_integer>] [-nontcpZombie <positive_integer>] [-ReducedFinTimeOut
<positive_integer>] [-NewConnIdleTimeOut <positive_integer>]
```

Description

Sets timeout values for various aspects of the NetScaler appliance. Caution: Modifying these values can affect system performance.

Parameters

zombie

Interval, in seconds, at which the NetScaler zombie cleanup process must run. This process cleans up inactive TCP connections. Default value: 120 Minimum value: 1 Maximum value: 600

client

Client idle timeout (in seconds). If zero, the service-type default value is taken when service is created. Maximum value: 18000

server

Server idle timeout (in seconds). If zero, the service-type default is taken when service is created. Maximum value: 18000

httpClient

Global idle timeout, in seconds, for client connections of HTTP service type. This value is over ridden by the client timeout that is configured on individual entities. Maximum value: 18000

httpServer

Global idle timeout, in seconds, for server connections of HTTP service type. This value is over ridden by the server timeout that is configured on individual entities. Maximum value: 18000

tcpClient

Global idle timeout, in seconds, for non-HTTP client connections of TCP service type. This value is over ridden by the client timeout that is configured on individual entities. Maximum value: 18000

tcpServer

Global idle timeout, in seconds, for non-HTTP server connections of TCP service type. This value is over ridden by the server timeout that is configured on entities. Maximum value: 18000

anyClient

Global idle timeout, in seconds, for non-TCP client connections. This value is over ridden by the client timeout that is configured on individual entities. Maximum value: 31536000

anyServer

Global idle timeout, in seconds, for non TCP server connections. This value is over ridden by the server timeout that is configured on individual entities. Maximum value: 31536000

halfclose

Idle timeout, in seconds, for connections that are in TCP half-closed state. Default value: 10 Minimum value: 1 Maximum value: 600

nontcpZombie

Interval at which the zombie clean-up process for non-TCP connections should run. Inactive IP NAT connections will be cleaned up. Default value: 60 Minimum value: 1 Maximum value: 600

ReducedFinTimeOut

Alternative idle timeout for new TCP NATPCB connections. Default value: 30 Minimum value: 1 Maximum value: 300

NewConnIdleTimeOut

Timer interval(in seconds) for new NATPCB for tcp connections. Default value: 4 Minimum value: 1 Maximum value: 20

Example

```
set ns timeout -zombie 200
```

[Top](#)

unset ns timeout

Synopsis

```
unset ns timeout [-zombie] [-httpClient] [-httpServer] [-tcpClient] [-tcpServer] [-anyClient] [-anyServer] [-halfclose] [-nontcpZombie] [-ReducedFinTimeOut] [-NewConnIdleTimeOut]
```

Description

Use this command to remove ns timeout settings.Refer to the set ns timeout command for meanings of the arguments.

[Top](#)

show ns timeout

Synopsis

show ns timeout

Description

Displays the timeouts configured for various NetScaler entities. Note: The timeouts having default values are not displayed.

Example

```
show ns timeout
```

[Top](#)

ns hardware

show ns hardware

Synopsis

show ns hardware

Description

Displays details of the appliance hardware and information such as the host ID and the serial number.

ns events

show ns events

Synopsis

show ns events [<eventNo>]

Description

Displays events that occur on the appliance.

Parameters

eventNo

Event number starting from which events must be shown.

Example

```
show ns events
```

ns encryptionParams

[[set](#) | [show](#)]

set ns encryptionParams

Synopsis

set ns encryptionParams -method <method> [-keyValue]

Description

Sets the parameters required for encrypting or decrypting content.

Parameters

method

Cipher method (and key length) to be used to encrypt and decrypt content. The default value is AES256. Possible values: NONE, RC4, DES3, AES128, AES192, AES256

keyValue

The base64-encoded key generation number, method, and key value. Note: * Do not include this argument if you are changing the encryption method. * To generate a new key value for the current encryption method, specify an empty string \"\" as the value of this parameter. The parameter is passed implicitly, with its automatically generated value, to the NetScaler packet engines even when it is not included in the command. Passing the parameter to the packet engines enables the appliance to save the key value to the configuration file and to propagate the key value to the secondary appliance in a high availability setup.

Example

```
set ns encryptionParams -method aes128
```

[Top](#)

show ns encryptionParams

Synopsis

show ns encryptionParams

Description

Displays the encryption method configured on the NetScaler appliance.

[Top](#)

ns rollbackcmd

show ns rollbackcmd

Synopsis

```
show ns rollbackcmd [-fileName <input_filename>] [-outtype ( cli | xml )]
```

Description

Generates the command(s) that can be used to roll back the command(s) that are specified in an input file. For example, if you want to roll back the creation of a load balancing virtual server named vserver_test, you must include the 'add lb vserver vserver_test ..' command in the input file. The output of this command is the 'rm lb vserver vserver_test' command.

Parameters

fileName

File that contains the commands for which the rollback commands must be generated. Specify the full path of the file name.

outtype

Format in which the rollback commands must be generated. Possible values: cli, xml

Example

```
show ns rollbackcmd -file <file_name>
```

ns memory

stat ns memory

Synopsis

```
stat ns memory [<pool>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile  
<input_filename>] [-clearstats ( basic | full )]
```

Description

Displays memory statistics of NetScaler features.

Parameters

pool

Feature name for which to display memory statistics.

clearstats

Clear the statistics / counters Possible values: basic, full

ns pbr6

```
[ add | renumber | rm | set | unset | enable | disable | stat | show | clear | apply ]
```

add ns pbr6

Synopsis

```
add ns pbr6 <name> [-td <positive_integer>] <action> [-srcIPv6 [<operator>]  
<srcIPv6Val>] [-srcPort [<operator>] <srcPortVal>] [-destIPv6 [<operator>]  
<destIPv6Val>] [-destPort [<operator>] <destPortVal>] [-srcMac <mac_addr>] [-protocol  
<protocol> | -protocolNumber <positive_integer>] [-vlan <positive_integer>] [-interface  
<interface_name>] [-priority <positive_integer>] [-state ( ENABLED | DISABLED )] [-msr  
( ENABLED | DISABLED ) [-monitor <string>]] [-nextHop <nextHopVal>] [-nextHopVlan  
<positive_integer>]
```

Description

Adds an IPv6 policy based route (PBR6) to the NetScaler appliance. To commit this operation, you must apply the PBR6s. A PBR6 specifies criteria for selecting outgoing IPv6 packets and, typically, a next hop to which to send the selected packets. For example, you can configure the NetScaler appliance to route outgoing packets from a specific IP address or range to a particular next hop router. Note: The NetScaler appliance process PBR6s before processing the RNAT rules.

Parameters

name

Name for the PBR6. Must begin with an ASCII alphabetic or underscore \(_\) character, and must contain only ASCII alphanumeric, underscore, hash \(\#\), period \(. \), space, colon \(:\) , at \(@\) , equals \(\=\), and hyphen \(-\) characters. Can be changed after the PBR6 is created.

td

Traffic Domain Id. Maximum value: 4094

action

Action to perform on the outgoing IPv6 packets that match the PBR6. Available settings function as follows: * ALLOW - The NetScaler appliance sends the packet to the designated next-hop router. * DENY - The NetScaler appliance applies the routing table for normal destination-based routing. Possible values: ALLOW, DENY

srcIPv6

IP address or range of IP addresses to match against the source IP address of an outgoing IPv6 packet. In the command line interface, separate the range with a hyphen and enclose within brackets.

srcPort

Port number or range of port numbers to match against the source port number of an outgoing IPv6 packet. In the command line interface, separate the range with a hyphen and enclose within brackets. For example: [40-90].

destIPv6

IP address or range of IP addresses to match against the destination IP address of an outgoing IPv6 packet. In the command line interface, separate the range with a hyphen and enclose within brackets.

destPort

Port number or range of port numbers to match against the destination port number of an outgoing IPv6 packet. In the command line interface, separate the range with a hyphen and enclose within brackets. For example: [40-90]. Note: The destination port can be specified only for TCP and UDP protocols.

srcMac

MAC address to match against the source MAC address of an outgoing IPv6 packet.

protocol

Protocol, identified by protocol name, to match against the protocol of an outgoing IPv6 packet. Possible values: ICMPV6, TCP, UDP

protocolNumber

Protocol, identified by protocol number, to match against the protocol of an outgoing IPv6 packet. Minimum value: 1 Maximum value: 255

vlan

ID of the VLAN. The NetScaler appliance compares the PBR6 only to the outgoing packets on the specified VLAN. If you do not specify an interface ID, the appliance compares the PBR6 to the outgoing packets on all VLANs. Minimum value: 1 Maximum value: 4094

interface

ID of an interface. The NetScaler appliance compares the PBR6 only to the outgoing packets on the specified interface. If you do not specify a value, the appliance compares the PBR6 to the outgoing packets on all interfaces.

priority

Priority of the PBR6, which determines the order in which it is evaluated relative to the other PBR6s. If you do not specify priorities while creating PBR6s, the PBR6s are evaluated in the order in which they are created. Minimum value: 1 Maximum value: 80000

state

Enable or disable the PBR6. After you apply the PBR6s, the NetScaler appliance compares outgoing packets to the enabled PBR6s. Possible values: ENABLED, DISABLED Default value: XACLENABLED

msr

Monitor the route specified by the Next Hop parameter. Possible values: ENABLED, DISABLED Default value: DISABLED

nextHop

IP address of the next hop router to which to send matching packets if action is set to ALLOW. This next hop should be directly reachable from the appliance.

nextHopVlan

VLAN number to be used for link local nexthop . Minimum value: 1 Maximum value: 4094

Example

```
add ns pbr6 rule1 ALLOW -srcport 45-1024 -destIPv6
2001::45 -nexthop 2001::49
```

[Top](#)**renumber ns pbr6****Synopsis**

```
renumber ns pbr6
```

Description

Renumbers the priorities of PBR6s to multiples of 10. To commit this operation, you must apply the PBR6s. Enables you to assign a new PBR6 a priority that is between two existing, consecutively numbered priorities. For example, if two PBR6s, PBR6-1 and PBR6-2, have priorities 2 and 3 renumbering changes those priorities to 20 and 30. You can then add PBR6-3 with priority 25.

Example

```
renumber pbr6
```

[Top](#)**rm ns pbr6****Synopsis**

```
rm ns pbr6 <name> ...
```

Description

Removes a PBR6 from the NetScaler appliance. To commit this operation, you must apply the PBR6s.

Parameters**name**

Name of the PBR6 that you want to remove.

Example

```
rm ns pbr6 rule1
```

[Top](#)

set ns pbr6

Synopsis

```
set ns pbr6 <name> [-action ( ALLOW | DENY )] [-srcIPv6 [<operator>] <srcIPv6Val>] [-srcPort [<operator>] <srcPortVal>] [-destIPv6 [<operator>] <destIPv6Val>] [-destPort [<operator>] <destPortVal>] [-srcMac <mac_addr>] [-protocol <protocol> | -protocolNumber <positive_integer>] [-vlan <positive_integer>] [-interface <interface_name>] [-priority <positive_integer>] [-msr ( ENABLED | DISABLED )] [-monitor <string>]] [-nextHop <nextHopVal>] [-nextHopVlan <positive_integer>]
```

Description

Modifies the specified parameters of a PBR6. To commit this operation, you must apply the PBR6s.

Parameters

name

Name of the PBR6 whose parameters you want to modify.

action

Action to perform on the outgoing IPv6 packets that match the PBR6. Available settings function as follows: * ALLOW - The NetScaler appliance sends the packet to the designated next-hop router. * DENY - The NetScaler appliance applies the routing table for normal destination-based routing. Possible values: ALLOW, DENY

srcIPv6

IP address or range of IP addresses to match against the source IP address of an outgoing IPv6 packet. In the command line interface, separate the range with a hyphen and enclose within brackets.

srcPort

Source Port (range).

destIPv6

IP address or range of IP addresses to match against the destination IP address of an outgoing IPv6 packet. In the command line interface, separate the range with a hyphen and enclose within brackets.

destPort

Destination Port (range).

srcMac

MAC address to match against the source MAC address of an outgoing IPv6 packet.

protocol

Protocol, identified by protocol name, to match against the protocol of an outgoing IPv6 packet. Possible values: ICMPV6, TCP, UDP

protocolNumber

Protocol, identified by protocol number, to match against the protocol of an outgoing IPv6 packet. Minimum value: 1 Maximum value: 255

vlan

ID of the VLAN. The NetScaler appliance compares the PBR6 only to the outgoing packets on the specified VLAN. If you do not specify an interface ID, the appliance compares the PBR6 to the outgoing packets on all VLANs. Minimum value: 1 Maximum value: 4094

interface

ID of an interface. The NetScaler appliance compares the PBR6 only to the outgoing packets on the specified interface. If you do not specify a value, the appliance compares the PBR6 to the outgoing packets on all interfaces.

priority

Priority of the PBR6, which determines the order in which it is evaluated relative to the other PBR6s. If you do not specify priorities while creating PBR6s, the PBR6s are evaluated in the order in which they are created. Minimum value: 1 Maximum value: 80000

msr

Monitor the route specified by the Next Hop parameter. Possible values: ENABLED, DISABLED Default value: DISABLED

nextHop

IP address of the next hop router to which to send matching packets if action is set to ALLOW. This next hop should be directly reachable from the appliance.

nextHopVlan

VLAN number to be used for link local nexthop . Minimum value: 1 Maximum value: 4094

Example

```
set ns pbr6 rule1 -srcPort 50
```

[Top](#)

unset ns pbr6

Synopsis

```
unset ns pbr6 <name> [-srcIPv6] [-srcPort] [-destIPv6] [-destPort] [-srcMac] [-protocol]
[-interface] [-vlan] [-msr] [-monitor] [-nextHop] [-nextHopVlan]
```

Description

Resets the attributes of the specified PBR6. Attributes for which a default value is available revert to their default values. Refer to the set ns pbr6 command for descriptions of the parameters..Refer to the set ns pbr6 command for meanings of the arguments.

Example

```
unset ns pbr6 rule1 -srcPort
```

[Top](#)**enable ns pbr6****Synopsis**

```
enable ns pbr6 <name> ...
```

Description

Enables a PBR6. To commit this operation, you must apply the PBR6s. After you apply the PBR6s, the NetScaler appliance compares outgoing packets to the enabled PBR6.

Parameters**name**

Name of PBR6 that you want to enable.

Example

```
enable ns pbr6 rule1
```

[Top](#)**disable ns pbr6****Synopsis**

```
disable ns pbr6 <name> ...
```

Description

Disables a PBR6. To commit this operation, you must apply the PBR6s. After you apply the PBR6s, the NetScaler appliance does not compare outgoing packets to the disabled PBR6s.

Parameters**name**

Name of PBR6 that you want to disable.

Example

```
disable ns pbr6 rule1
```

[Top](#)

stat ns pbr6

Synopsis

```
stat ns pbr6 [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile  
<input_filename>] [-clearstats ( basic | full )]
```

Description

Displays statistics related to the PBR6s. To display statistics of all the PBR6s, run the command without any parameters. To display statistics of a particular PBR6, specify the name of the PBR6.

Parameters

name

Name of the PBR6 whose statistics you want the NetScaler appliance to display.

clearstats

Clear the statistics / counters Possible values: basic, full

Example

```
stat pbr6
```

[Top](#)

show ns pbr6

Synopsis

```
show ns pbr6 [<name>] [-detail]
```

Description

Displays settings related to the PBR6s. To display settings of all the PBR6s, run the command without any parameters. To display settings of a particular PBR6, specify the name of the PBR6.

Parameters

name

Name of the PBR6 whose settings you want the NetScaler appliance to display.

detail

To get a detailed view.

Example

```
show ns pbr6 rule1
1)      Name: r1                      Action:
DENY
      srcIPv6 = 2001::1
      destIPv6
```



```

srcMac:
Protocol:
Vlan:
Interface:
Active Status: ENABLED           Applied
Status: NOTAPPLIED
Priority: 10                     Hits: 0
Nexthop:

```

[Top](#)

clear ns pbr6

Synopsis

clear ns pbr6

Description

Removes all PBR6s from the NetScaler appliance. This operation does not require an explicit apply.

Example

```
clear ns pbr6
```

[Top](#)

apply ns pbr6

Synopsis

apply ns pbr6

Description

Updates the PBR6's memory tree (lookup table), adding any new PBR6 and applying any modifications to the existing PBR6s. The lookup table includes the configuration of all the extended PBR6s on the NetScaler appliance. The NetScaler appliance uses the lookup table (not the configuration file) to filter the outgoing IPv6 packets.

Example

```
apply ns pbr6
```

[Top](#)

ns trafficDomain

[[add](#) | [rm](#) | [clear](#) | [bind](#) | [unbind](#) | [enable](#) | [disable](#) | [show](#) | [stat](#)]

add ns trafficDomain

Synopsis

add ns trafficDomain <td> [-aliasName <string>]

Description

Configure Traffic Domain on the system.

Parameters

td

Traffic Domain Id. Minimum value: 1 Maximum value: 4094

aliasName

Name of traffic domain being added.

Example

```
add ns trafficDomain 1 -aliasName td1
```

[Top](#)

rm ns trafficDomain

Synopsis

rm ns trafficDomain <td>

Description

Remove Traffic Domain configured.

Parameters

td

Traffic Domain Id. Minimum value: 1 Maximum value: 4094

Example

```
rm ns trafficDomain 1
```

[Top](#)

clear ns trafficDomain

Synopsis

clear ns trafficDomain <td>

Description

Remove Traffic Domain configuration.

Parameters

td

Traffic Domain Id. Minimum value: 1 Maximum value: 4094

[Top](#)

bind ns trafficDomain

Synopsis

`bind ns trafficDomain <td> [-vlan <positive_integer>] [-bridgegroup <positive_integer>]`

Description

bind vlan or bridgegroup entities with traffic domain.

Parameters

td

Traffic Domain Id. Minimum value: 1 Maximum value: 4094

vlan

Names of all member vlans. Minimum value: 1 Maximum value: 4094

bridgegroup

bridge group. Minimum value: 1 Maximum value: 1000

Example

```
bind ns trafficDomain 1 -vlan 2
```

[Top](#)

unbind ns trafficDomain

Synopsis

`unbind ns trafficDomain <td> [-vlan <positive_integer>] [-bridgegroup <positive_integer>]`

Description

Unbind vlan or bridgegroup entities from traffic domain

Parameters

td

Traffic Domain Id. Minimum value: 1 Maximum value: 4094

vlan

Names of all member vlans. Minimum value: 1 Maximum value: 4094

bridgegroup

bridge group. Minimum value: 1 Maximum value: 1000

Example

```
unbind ns trafficDomain 1 -vlan 2
```

[Top](#)

enable ns trafficDomain

Synopsis

enable ns trafficDomain <td> [-state (ENABLED | DISABLED)]

Description

Enable TrafficDomain.

Parameters

td

Traffic Domain Id. Minimum value: 1 Maximum value: 4094

state

The state of TrafficDmain. Possible values: ENABLED, DISABLED Default value: ENABLED

Example

```
enable ns trafficdomain 1
```

[Top](#)

disable ns trafficDomain

Synopsis

disable ns trafficDomain <td> [-state (ENABLED | DISABLED)]

Description

Disable TrafficDomain.

Parameters

td

Traffic Domain Id. Minimum value: 1 Maximum value: 4094

state

The state of TrafficDmain. Possible values: ENABLED, DISABLED Default value: ENABLED

Example

```
disable ns trafficdomain 1
```

[Top](#)**show ns trafficDomain****Synopsis**

```
show ns trafficDomain [<td>]
```

Description

Display Traffic Domain configuration.

Parameters**td**

Traffic Domain Id. Minimum value: 1 Maximum value: 4094

Example

An example of the output of the show trafficDomain command is as follows:

```
1)      Td: 1
        Alias Name:      State: ENABLED
        Vlans : 50

2)      Td: 2
        Alias Name:      State: ENABLED
        Vlans : 2
        Bridge Group : 1

Done
```

[Top](#)**stat ns trafficDomain****Synopsis**

```
stat ns trafficDomain [<td>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile
<input_filename>] [-clearstats ( basic | full )]
```

Description

Display statistics for Traffic Domains(s).

Parameters**td**

An integer specifying the Traffic Domain ID. Possible values: 1 through 4094.
Minimum value: 1 Maximum value: 4094

clearstats

Clear the statistics / counters Possible values: basic, full

Example

```
stat ns trafficdomain 1
```

[Top](#)

ns consoleloginprompt

[[set](#) | [unset](#) | [show](#)]

set ns consoleloginprompt

Synopsis

set ns consoleloginprompt <promptString>

Parameters

promptString

Console login prompt string

Example

```
set ns consoleloginprompt <prompt_string>
```

[Top](#)

unset ns consoleloginprompt

Synopsis

unset ns consoleloginprompt -promptString

Description

Use this command to remove ns consoleloginprompt settings. Refer to the set ns consoleloginprompt command for meanings of the arguments.

[Top](#)

show ns consoleloginprompt

Synopsis

show ns consoleloginprompt

Parameters

promptString

Console login prompt string

Example

```
get ns consoleloginprompt
```

[Top](#)

ns timer

[[add](#) | [rm](#) | [set](#) | [unset](#) | [bind](#) | [unbind](#) | [show](#) | [rename](#)]

add ns timer

Synopsis

```
add ns timer <name> (-interval <integer> [<unit>]) [-comment <string>]
```

Description

Create a Timer.

Parameters**name**

Timer name.

interval

The frequency at which the policies bound to this timer are invoked. The minimum value is 20 msec. The maximum value is 20940 in seconds and 349 in minutes Default value: 5 Minimum value: 1 Maximum value: 20940000

comment

Comments associated with this timer.

Example

```
add timer policy timer -comment "Timer that would  
be invoked at interval 10 sec apart."
```

[Top](#)

rm ns timer

Synopsis

```
rm ns timer <name>
```

Description

Remove a Timer.

Parameters

name

Timer name.

Example

```
rm ns timer timer
```

[Top](#)

set ns timer

Synopsis

set ns timer <name> [-interval <integer>] [<unit>] [-comment <string>]

Description

Set a argument values for existing timer.

Parameters

name

Timer name.

interval

The frequency at which the policies bound to this timer are invoked. The minimum value is 20 msec. The maximum value is 20940 in seconds and 349 in minutes Default value: 5 Minimum value: 1 Maximum value: 20940000

unit

Timer interval unit Possible values: SEC, MIN Default value: NSTMUNT_SEC

comment

Comments associated with this timer.

Example

```
set ns timer timer -comment "Timer that would be
invoked at interval 20 sec apart."
```

[Top](#)

unset ns timer

Synopsis

unset ns timer <name> [-interval <integer>] [<unit>] [-comment <string>]

Description

Unset comment for existing timer..Refer to the set ns timer command for meanings of the arguments.

Example

```
unset ns timer timer -comment
```

[Top](#)

bind ns timer

Synopsis

```
bind ns timer <name> -policyName <string> -priority <positive_integer> [-
gotoPriorityExpression <expression>] [-vServer <string>] [-sampleSize
<positive_integer>] [-threshold <positive_integer>]
```

Description

Defines the binding relation among timer, and timer policy.

Parameters

name

Timer name.

policyName

The timer policy associated with the timer.

Example

```
i)    bind ns timer timer_trigger -policyName
timer_pol -priority 1
ii)   bind ns timer timer_trigger -policyName
timer_pol -priority 1
```

[Top](#)

unbind ns timer

Synopsis

```
unbind ns timer <name> -policyName <string>
```

Description

Unbind entities from timer

Parameters

name

Timer name.

policyName

The timer policy associated with the timer.

Example

```
unbind ns timer timer -policyName timer_pol
```

[Top](#)

show ns timer

Synopsis

show ns timer [<name>]

Description

Display the Timer entities.

Parameters

name

Timer name.

[Top](#)

rename ns timer

Synopsis

rename ns timer <name>@ <newName>@

Description

Rename a timer.

Parameters

name

The name of the timer.

newName

The new name of the timer.

Example

```
rename ns timer oldname newname
```

[Top](#)

ns aptlicense

[[show](#) | [update](#)]

show ns aptlicense

Synopsis

show ns aptlicense <serialNo>

Parameters

serialNo

Hardware Serial Number/License Activation Code(LAC)

Example

```
show ns aptlicense <hw-no/lac>
```

[Top](#)

update ns aptlicense

Synopsis

update ns aptlicense <id> <sessionId> <bindType> <countAvailable> [<licenseDir>]

Parameters

id

License ID

sessionId

Session ID

bindType

Bind type

countAvailable

Count

licenseDir

License Directory

Example

```
update ns aptlicense key1 sessionId#  HOSTNAME 1
```

[Top](#)

NTP Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [ntp server](#)

- ♦ [ntp sync](#)
- ♦ [ntp status](#)
- ♦ [ntp param](#)

ntp server

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add ntp server

Synopsis

```
add ntp server (<serverIP> | <serverName>) [-minpoll <positive_integer>] [-maxpoll  
<positive_integer>] [-autokey | -key <positive_integer>]
```

Description

Adds an NTP server to the appliance. This server can be used to synchronize the time on the appliance to the network time.

Parameters

serverIP

IP address of the NTP server.

serverName

Fully qualified domain name of the NTP server.

minpoll

Minimum time after which the NTP server must poll the NTP messages. In seconds, expressed as a power of 2. Default value: NS_NTP_MINPOLL_DEFAULT_VALUE
Minimum value: 4 Maximum value: 17

maxpoll

Maximum time after which the NTP server must poll the NTP messages. In seconds, expressed as a power of 2. Default value: NS_NTP_MAXPOLL_DEFAULT_VALUE
Minimum value: 4 Maximum value: 17

autokey

Use the Autokey protocol for key management for this server, with the cryptographic values (for example, symmetric key, host and public certificate files, and sign key) generated by the ntp-keygen utility. To require authentication for communication with the server, you must set either the value of this parameter or the key parameter.

key

Key to use for encrypting authentication fields. All packets sent to and received from the server must include authentication fields encrypted by using this key. To require authentication for communication with the server, you must set either the value of this parameter or the autokey parameter. Minimum value: 1 Maximum value: 65534

[Top](#)

rm ntp server

Synopsis

rm ntp server (<serverIP> | <serverName>)

Description

Removes an NTP server. You can specify the server by IP address or by name.

Parameters

serverIP

IP address of the NTP server to be removed.

serverName

Name of the NTP server to be removed.

[Top](#)

set ntp server

Synopsis

set ntp server (<serverIP> | <serverName>) [-minpoll <positive_integer>] [-maxpoll <positive_integer>] [-preferredNtpServer (YES | NO)] [-autokey | -key <positive_integer>]

Description

Modifies the specified attributes of an NTP server.

Parameters

serverIP

IP address of the NTP server to be modified.

serverName

Name of the NTP server to be modified.

minpoll

Minimum time after which the NTP server must poll the NTP messages. In seconds, expressed as a power of 2. Default value: NS_NTP_MINPOLL_DEFAULT_VALUE
Minimum value: 4 Maximum value: 17

maxpoll

Maximum time after which the NTP server must poll the NTP messages. In seconds, expressed as a power of 2. Default value: NS_NTP_MAXPOLL_DEFAULT_VALUE
Minimum value: 4 Maximum value: 17

preferredNtpServer

Preferred NTP server. The NetScaler appliance chooses this NTP server for time synchronization among a set of correctly operating hosts. Possible values: YES, NO
Default value: NO

autokey

Use the Autokey protocol for key management for this server, with the cryptographic values (for example, symmetric key, host and public certificate files, and sign key)

generated by the ntp-keygen utility. To require authentication for communication with the server, you must set either the value of this parameter or the key parameter.

key

Key to use for encrypting authentication fields. All packets sent to and received from the server must include authentication fields encrypted by using this key. To require authentication for communication with the server, you must set either the value of this parameter or the autokey parameter. Minimum value: 1 Maximum value: 65534

[Top](#)

unset ntp server

Synopsis

```
unset ntp server [<serverIP>] [<serverName>] [-minpoll] [-maxpoll] [-preferredNtpServer] [-autokey] [-key]
```

Description

Use this command to remove ntp server settings. Refer to the set ntp server command for meanings of the arguments.

[Top](#)

show ntp server

Synopsis

```
show ntp server [<serverIP> | <serverName>]
```

Description

Displays information about an NTP server. You can specify the server by IP address or by name.

Parameters

serverIP

IP address of the NTP server about which to display information.

serverName

Name of the NTP server about which to display information.

[Top](#)

ntp sync

[[enable](#) | [disable](#) | [show](#)]

enable ntp sync

Synopsis

```
enable ntp sync
```

Description

Enables NTP synchronization. When NTP synchronization is enabled, the NTP daemon is spawned for time synchronization.

[Top](#)

disable ntp sync

Synopsis

disable ntp sync

Description

Disables NTP synchronization.

[Top](#)

show ntp sync

Synopsis

show ntp sync

Description

Displays the status of the NTP synchronization.

[Top](#)

ntp status

show ntp status

Synopsis

show ntp status

Description

Displays the NTP status on the appliance.

ntp param

[[set](#) | [unset](#) | [show](#)]

set ntp param

Synopsis

set ntp param [-authentication (YES | NO)] [-trustedkey <positive_integer> ...] [-autokeyLogsec <positive_integer>] [-revokeLogsec <positive_integer>]

Description

Modifies the values for NTP parameters on the NetScaler appliance.

Parameters

authentication

Apply NTP authentication, which enables the NTP client (NetScaler) to verify that the server is in fact known and trusted. Possible values: YES, NO Default value: YES

trustedkey

Key identifiers that are trusted for server authentication with symmetric key cryptography in the keys file. Minimum value: 1 Maximum value: 65534

autokeyLogsec

Autokey protocol requires the keys to be refreshed periodically. This parameter specifies the interval between regenerations of new session keys. In seconds, expressed as a power of 2. Default value: 12 Maximum value: 32

revokeLogsec

Interval between re-randomizations of the autokey seeds to prevent brute-force attacks on the autokey algorithms. Default value: 16 Maximum value: 32

[Top](#)

unset ntp param

Synopsis

```
unset ntp param [-authentication] [-trustedkey] [-autokeyLogsec] [-revokeLogsec]
```

Description

Use this command to remove ntp param settings. Refer to the set ntp param command for meanings of the arguments.

[Top](#)

show ntp param

Synopsis

```
show ntp param
```

Description

Displays information about the NTP parameters.

[Top](#)

Policy Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [policy expression](#)
- ♦ [policy map](#)
- ♦ [policy patset](#)
- ♦ [policy dataset](#)

- ♦ [policy httpCallout](#)
- ♦ [policy stringmap](#)

policy expression

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add policy expression

Synopsis

add policy expression <name> <value> [-comment <string>] [-clientSecurityMessage <string>]

Description

Creates a classic or default syntax named expression, which can be used in multiple policies. For example, you can create the following named expressions, ExpressionA and ExpressionB: ExpressionA: http.req.body(100).contains("A") ExpressionB: http.req.body(100).contains("B") You could then create an expression of the form: <ExpressionA || ExpressionB>

Parameters

name

Unique name for the expression. Not case sensitive. Must begin with an ASCII letter or underscore (_) character, and must consist only of ASCII alphanumeric or underscore characters. Must not begin with 're' or 'xp' or be a word reserved for use as a default syntax expression qualifier prefix (such as HTTP) or enumeration value (such as ASCII). Must not be the name of an existing named expression, pattern set, dataset, stringmap, or HTTP callout.

value

Expression string. For example: http.req.body(100).contains("this").

description

Description for the expression.

comment

Any comments associated with the expression. Displayed upon viewing the policy expression.

clientSecurityMessage

Message to display if the expression fails. Allowed for classic end-point check expressions only.

[Top](#)

rm policy expression

Synopsis

rm policy expression <name> ...

Description

Removes a named policy expression. If the expression is used by a policy or filter, you must remove the policy or filter before removing the expression.

Parameters

name

Name of the policy expression to be removed.

[Top](#)

set policy expression

Synopsis

```
set policy expression <name> [<value>] [-comment <string>] [-clientSecurityMessage <string>]
```

Description

Modifies the attributes of a named policy expression.

Parameters

name

Name of the policy expression to be modified.

value

The expression string.

description

Description for the expression.

comment

Any comments associated with the expression. Displayed upon viewing the policy expression.

clientSecurityMessage

The client security message that will be displayed on failure of this expression. Only relevant for end point check expressions.

[Top](#)

unset policy expression

Synopsis

```
unset policy expression <name> [-comment] [-clientSecurityMessage]
```

Description

Use this command to remove policy expression settings. Refer to the set policy expression command for meanings of the arguments.

[Top](#)

show policy expression

Synopsis

show policy expression [<name> | -type (CLASSIC | ADVANCED)]

Description

Displays information about the available named policy expressions.

Parameters

name

Name of the policy expression to display. If a name is not provided, information about all policy expressions is shown.

type

Type of expression. Can be a classic or default syntax (advanced) expression. Possible values: CLASSIC, ADVANCED

[Top](#)

policy map

[[add](#) | [rm](#) | [show](#)]

add policy map

Synopsis

add policy map <mapPolicyName> -sd <string> [-su <string>] [-td <string>] [-tu <string>]

Description

Creates a policy to map a publicly known domain name to a target domain name for a reverse proxy virtual server used by the cache redirection feature. Optionally, you can also specify a source and target URL. The map policy can be associated with a reverse proxy cache redirection virtual server by using the 'bind cr vserver' command. There can be only one default map policy for a domain.

Parameters

mapPolicyName

Name for the map policy. Must begin with a letter, number, or the underscore (_) character and must consist only of letters, numbers, and the hash (#), period (.), colon (:), space (), at (@), equals (=), hyphen (-), and underscore (_) characters. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my map" or 'my map').

sd

Publicly known source domain name. This is the domain name with which a client request arrives at a reverse proxy virtual server for cache redirection. If you specify a source domain, you must specify a target domain.

su

Source URL. Specify all or part of the source URL, in the following format: /[[prefix] [*]] [.suffix].

td

Target domain name sent to the server. The source domain name is replaced with this domain name.

tu

Target URL. Specify the target URL in the following format: /[[prefix] [*]][.suffix].

Example

Example 1

The following example creates a default map policy (map1) for the source domain www.a.com. Any client requests with this source domain in the host header is changed to www.real_a.com.

```
add policy map map2 -sd www.a.com -td  
www.real_a.com
```

Example 2

This example shows how to create a URL map policy (map2) if you want to translate /sports.html in the incoming request to /news.html in addition to mapping the source domain www.a.com to www.real_a.com in the outgoing request.

```
add policy map map2 -sd www.a.com  
-td www.real_a.com -su /sports.html  
-tu /news.html
```

These type of map policies, called "URL map policies," have the following restrictions:

- 1 URL map policies belonging to www.a.com cannot be added without first adding a default map policy as described in Example 1.

- 1 If a source suffix has been specified for URL map policy, a destination suffix must also be specified.

- 1 If an exact URL has been specified as the source, then the target URL should also be exact URL.

- 1 If there is a source prefix in the URL, there must be also a destination prefix in the URL.

[Top](#)

rm policy map

Synopsis

```
rm policy map <mapPolicyName>
```

Description

Removes a map policy. Before removing the map policy, you must unbind the map policy from the reverse proxy virtual server.

Parameters

mapPolicyName

Name of the policy map to remove.

[Top](#)

show policy map

Synopsis

show policy map [<mapPolicyName>]

Description

Displays information about the available policy maps.

Parameters

mapPolicyName

Name of the policy map to display. If a name is not provided, information of all configured policy maps is shown.

[Top](#)

policy patset

[[add](#) | [rm](#) | [bind](#) | [unbind](#) | [show](#)]

add policy patset

Synopsis

add policy patset <name> [-indexType (Auto-generated | User-defined)]

Description

Adds a pattern set. A pattern set contains a name and one or more string patterns. Pattern sets can be used in default syntax expressions to match a set of strings. For example, HTTP.REQ.URL.EQUALS_ANY("test_urls"), where test_urls is a pattern set containing URL strings. Pattern sets can also be used in the search parameter of a rewrite action. Each string pattern is assigned an index that enables you to select the associated string from the set.

Parameters

name

Unique name of the pattern set. Not case sensitive. Must begin with an ASCII letter or underscore (_) character and must contain only alphanumeric and underscore characters. Must not be the name of an existing named expression, pattern set, dataset, string map, or HTTP callout.

indexType

Index type.

Example

```
add policy patset pat1
```

[Top](#)

rm policy patset

Synopsis

```
rm policy patset <name>
```

Description

Removes a pattern set. If the pattern set is used by an expression in another object, such as a policy, you must remove the object before removing the pattern set.

Parameters

name

Name of the pattern set to remove.

Example

```
rm policy patset pat1
```

[Top](#)

bind policy patset

Synopsis

```
bind policy patset <name> <string> [-index <positive_integer>] [-charset ( ASCII | UTF_8 )]
```

Description

Binds a string to a pattern set.

Parameters

name

Name of the pattern set to which to bind the string.

string

String of characters that constitutes a pattern. For more information about the characters that can be used, refer to the character set parameter. Note: Minimum length for pattern sets used in rewrite actions of type REPLACE_ALL, DELETE_ALL, INSERT_AFTER_ALL, and INSERT_BEFORE_ALL, is three characters.

Example

```
bind policy patset pat1 bar -index 2
```

[Top](#)

unbind policy patset

Synopsis

unbind policy patset <name> <string> ...

Description

Unbinds a string from a pattern set.

Parameters**name**

Name of the pattern set from which to unbind a string.

string

String of characters to unbind from the pattern set.

Example

```
unbind policy patset pat1 bar xyz
```

[Top](#)

show policy patset

Synopsis

show policy patset [<name>]

Description

Displays the list of pattern sets configured on the appliance.

Parameters**name**

Name of the pattern set for which to display the detailed information. If a name is not provided, a list of all pattern sets configured on the appliance is shown.

Example

```
show policy patset pat1
```

[Top](#)

policy dataset

[[add](#) | [rm](#) | [bind](#) | [unbind](#) | [show](#)]

add policy dataset

Synopsis

add policy dataset <name> <type> [-indexType (Auto-generated | User-defined)]

Description

Adds a policy dataset to the appliance.

Parameters

name

Name of the dataset. Must not exceed 127 characters.

type

Type of value to bind to the dataset. Possible values: ipv4, number, ipv6

indexType

Index type.

Example

```
add policy dataset ts1 -type IPV4
```

[Top](#)

rm policy dataset

Synopsis

rm policy dataset <name>

Description

Removes a dataset from the appliance.

Parameters

name

Name of the dataset to remove.

Example

```
rm policy dataset pat1
```

[Top](#)

bind policy dataset

Synopsis

bind policy dataset <name> <value> [-index <positive_integer>]

Description

Binds a value of the specified type to the dataset. If the first value is bound by using an index label, the other bind statements to that set should also provide an index.

Parameters

name

Name of the dataset to which to bind the value.

value

Value of the specified type that is associated with the dataset.

Example

```
bind policy dataset ts1 192.168.20.1 -index 2
```

[Top](#)

unbind policy dataset

Synopsis

unbind policy dataset <name> <value>

Description

Unbind string(s) from a dataset.

Parameters

name

Name of the dataset from which to unbind the value.

value

Value to unbind from the dataset.

Example

```
unbind policy dataset pat1 bar xyz
```

[Top](#)

show policy dataset

Synopsis

show policy dataset [<name>]

Description

Display the configured dataset(s).

Parameters

name

Name of the dataset. Must not exceed 127 characters.

Example

```
show policy dataset set1
```

[Top](#)

policy httpCallout

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add policy httpCallout

Synopsis

add policy httpCallout <name>

Description

Adds a default syntax expression element that, when evaluated, sends an HTTP request to a specified service and receives an HTTP response from the service. Can be used to obtain additional information for use in evaluating policy rules and other expressions. This command only creates the HTTP callout. Use the 'set policy httpCallout' command to configure it.

Parameters

name

Name for the HTTP callout. Not case sensitive. Must begin with an ASCII letter or underscore (_) character, and must consist only of ASCII alphanumeric or underscore characters. Must not begin with 're' or 'xp' or be a word reserved for use as a default syntax expression qualifier prefix (such as HTTP) or enumeration value (such as ASCII). Must not be the name of an existing named expression, pattern set, dataset, stringmap, or HTTP callout.

Example

```
add policy httpcallout h1
```

[Top](#)

rm policy httpCallout

Synopsis

```
rm policy httpCallout <name>
```

Description

Removes an HTTP callout. You cannot remove an HTTP callout that is used in any part of policy, action, or expression.

Parameters

name

Name of the HTTP callout to remove.

Example

```
rm policy httpcallout h1
```

[Top](#)

set policy httpCallout

Synopsis

```
set policy httpCallout <name> [-IPAddress <ip_addr|ipv6_addr>] [-port <port>] [-vServer <string>] [-returnType <returnType>] [-httpMethod ( GET | POST )] [-hostExpr <string>] [-urlStemExpr <string>] [-headers <name(value)> ...] [-parameters <name(value)> ...] [-bodyExpr <string>] [-fullReqExpr <string>] [-scheme ( http | https )] [-resultExpr <string>] [-cacheForSecs <secs>]
```

Description

Configures an HTTP callout element. You can then invoke the HTTP callout from other policies and functions (for example, actions) that use default syntax expressions. The expression prefix SYS.HTTP_CALLOUT invokes an HTTP callout. You can construct the HTTP callout request in one of two ways: * Specify individual parts of the request by using the HTTP method, host expression, URL stem expression, and header parameters. These parts are evaluated at run time and concatenated to build the request. * Specify the entire HTTP request in a single expression.

Parameters

name

Name of the HTTP callout to configure.

IPAddress

IP Address of the server (callout agent) to which the callout is sent. Can be an IPv4 or IPv6 address. Mutually exclusive with the Virtual Server parameter. Therefore, you cannot set the <IP Address, Port> and the Virtual Server in the same HTTP callout.

port

Server port to which the HTTP callout agent is mapped. Mutually exclusive with the Virtual Server parameter. Therefore, you cannot set the <IP Address, Port> and the Virtual Server in the same HTTP callout.

vServer

Name of the load balancing, content switching, or cache redirection virtual server (the callout agent) to which the HTTP callout is sent. The service type of the virtual server must be HTTP. Mutually exclusive with the IP address and port parameters. Therefore, you cannot set the <IP Address, Port> and the Virtual Server in the same HTTP callout.

returnType

Type of data that the target callout agent returns in response to the callout. Available settings function as follows: * TEXT - Treat the returned value as a text string. * NUM - Treat the returned value as a number. * BOOL - Treat the returned value as a Boolean value. Note: You cannot change the return type after it is set. Possible values: BOOL, NUM, TEXT

httpMethod

Method used in the HTTP request that this callout sends. Mutually exclusive with the full HTTP request expression. Possible values: GET, POST

hostExpr

Default Syntax string expression to configure the Host header. Can contain a literal value (for example, 10.101.10.11) or a derived value (for example, http.req.header("Host")). The literal value can be an IP address or a fully qualified domain name. Mutually exclusive with the full HTTP request expression.

urlStemExpr

Default Syntax string expression for generating the URL stem. Can contain a literal string (for example, "/mysite/index.html") or an expression that derives the value (for example, http.req.url). Mutually exclusive with the full HTTP request expression.

headers

One or more headers to insert into the HTTP request. Each header is specified as "name(expr)", where expr is a default syntax expression that is evaluated at runtime to provide the value for the named header. You can configure a maximum of eight headers for an HTTP callout. Mutually exclusive with the full HTTP request expression.

parameters

One or more query parameters to insert into the HTTP request URL (for a GET request) or into the request body (for a POST request). Each parameter is specified as "name(expr)", where expr is an default syntax expression that is evaluated at run time to provide the value for the named parameter (name=value). The parameter values are URL encoded. Mutually exclusive with the full HTTP request expression.

bodyExpr

An advanced string expression for generating the body of the request. The expression can contain a literal string or an expression that derives the value (for example, client.ip.src). Mutually exclusive with -fullReqExpr.

fullReqExpr

Exact HTTP request, in the form of a default syntax expression, which the NetScaler appliance sends to the callout agent. If you set this parameter, you must not include HTTP method, host expression, URL stem expression, headers, or parameters. The request expression is constrained by the feature for which the callout is used. For example, an HTTP.RES expression cannot be used in a request-time policy bank or in a TCP content switching policy bank. The NetScaler appliance does not check the validity of this request. You must manually validate the request.

scheme

Type of scheme for the callout server. Possible values: http, https

resultExpr

Expression that extracts the callout results from the response sent by the HTTP callout agent. Must be a response based expression, that is, it must begin with HTTP.RES. The operations in this expression must match the return type. For example, if you configure a return type of TEXT, the result expression must be a text based expression. If the return type is NUM, the result expression (resultExpr) must return a numeric value, as in the following example: http.res.body(10000).length.

cacheForSecs

Duration, in seconds, for which the callout response is cached. The cached responses are stored in an integrated caching content group named "calloutContentGroup". If no duration is configured, the callout responses will not be cached unless normal caching configuration is used to cache them. This parameter takes precedence over any normal caching configuration that would otherwise apply to these responses. Note that the calloutContentGroup definition may not be modified or removed nor may it be used with other cache policies. Minimum value: 1 Maximum value: 31536000

Example

```
set policy httpcallout h1 -vServer v1
```

[Top](#)

unset policy httpCallout**Synopsis**

```
unset policy httpCallout <name> [-IPAddress] [-port] [-vServer] [-httpMethod] [-hostExpr] [-urlStemExpr] [-headers] [-parameters] [-bodyExpr] [-fullReqExpr] [-resultExpr] [-cacheForSecs]
```

Description

Use this command to remove policy httpCallout settings. Refer to the set policy httpCallout command for meanings of the arguments.

[Top](#)

show policy httpCallout

Synopsis

show policy httpCallout [<name>]

Description

Displays information about the configured HTTP callouts.

Parameters

name

Name of the HTTP callout to display. If a name is not provided, information about all configured HTTP callouts is shown.

Example

```
show policy httpcallout h1
```

[Top](#)

policy stringmap

[[add](#) | [rm](#) | [set](#) | [unset](#) | [bind](#) | [unbind](#) | [show](#)]

add policy stringmap

Synopsis

add policy stringmap <name> [-comment <string>]

Description

Creates a string map. You must use the 'bind policy stringmap' command to bind strings to this string map.

Parameters

name

Unique name for the string map. Not case sensitive. Must begin with an ASCII letter or underscore (_) character, and must consist only of ASCII alphanumeric or underscore characters. Must not begin with 're' or 'xp' or be a word reserved for use as a default syntax expression qualifier prefix (such as HTTP) or enumeration value (such as ASCII). Must not be the name of an existing named expression, pattern set, dataset, string map, or HTTP callout.

comment

Comments associated with the string map.

Example

```
i)      add stringmap custom_stringmap
.       This creates a new string map with name
custom_stringmap.
```

[Top](#)**rm policy stringmap****Synopsis**

rm policy stringmap <name>

Description

Removes a string map. String maps can be removed only if not used in any part of policy, action, or expression.

Parameters

name

Name of the string map to remove.

Example

```
i)      rm stringmap custom_stringmap
.       This removes a string map whose name is
custom_stringmap
```

[Top](#)**set policy stringmap****Synopsis**

set policy stringmap <name> -comment <string>

Description

Modifies the attributes of an existing string map.

Parameters

name

Name of the string map to be modified.

comment

Comments associated with the string map.

Example

```
i)      set stringmap custom_stringmap -comment
"custom string map is for URLs."
.      This updates the comment associated with the
string map whose name is custom_stringmap
```

[Top](#)

unset policy stringmap

Synopsis

unset policy stringmap <name> -comment

Description

Use this command to remove policy stringmap settings. Refer to the set policy stringmap command for meanings of the arguments.

[Top](#)

bind policy stringmap

Synopsis

bind policy stringmap <name> <key> <value>

Description

Binds a key and its associated value to a string map. If the key already exists and has a different value, the old value is overwritten with the new value.

Parameters

name

Name of the string map to which to bind the key-value pair.

key

Character string constituting the key to be bound to the string map. The key is matched against the data processed by the operation that uses the string map. The default character set is ASCII. UTF-8 characters can be included if the character set is UTF-8. UTF-8 characters can be entered directly (if the UI supports it) or can be encoded as a sequence of hexadecimal bytes '\xNN'. For example, the UTF-8 character 'u' can be encoded as '\xC3\xBC'.

Example

```
bind stringmap custom_stringmap "key-string"
"value-string"
.      This adds the key "key-string" and its
associated value "value-string" to the string map
whose name is custom_stringmap.
```


[Top](#)

unbind policy stringmap

Synopsis

unbind policy stringmap <name> <key>

Description

Removes a key from the string map.

Parameters

name

Name of the string map from which to remove a key.

key

Key to remove from the string map.

Example

```
unbind stringmap custom_stringmap key1
. This removes the key "key1" and its
associated value from the string map whose name is
custom_stringmap.
```

[Top](#)

show policy stringmap

Synopsis

show policy stringmap [<name>]

Description

Displays a list of available string maps.

Parameters

name

Name of the string map to display. If a name is not provided, a list of all the configured string maps is shown.

Example

```
show stringmap custom_stringmap
. Displays all the key-value pairs of a string map
whose name is custom-stringmap
```

[Top](#)

PQ Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [pq](#)
- ♦ [pq policy](#)
- ♦ [pq stats](#)

pq

stat pq

Synopsis

```
stat pq [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-clearstats ( basic | full )]
```

Description

Displays statistics of priority queuing.

Parameters

clearstats

Clear the statistics / counters Possible values: basic, full

pq policy

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#) | [stat](#)]

add pq policy

Synopsis

```
add pq policy <policyName> -rule <expression> -priority <positive_integer> [-weight <positive_integer>] [-qDepth <positive_integer> | -polqDepth <positive_integer>]
```

Description

Adds a priority queuing policy to the appliance. Note: To use the priority queuing policy on a virtual server, the virtual server must have priority queuing enabled and the priority queuing policy must be bound to the load balancing virtual server. To enable priority queuing on the virtual server and to bind the policy, use the `set lb vserver` and `bind lb vserver` commands.

Parameters

policyName

Name for the priority queuing policy. Must begin with a letter, number, or the underscore symbol (`_`). Other characters allowed, after the first character, are the hyphen (`-`), period (`.`) hash (`#`), space (), at (`@`), equals (`=`), and colon (`:`) characters.

rule

Expression or name of a named expression, against which the request is evaluated. The priority queuing policy is applied if the rule evaluates to true. Note: * On the command line interface, if the expression includes blank spaces, the entire expression must be enclosed in double quotation marks. * If the expression itself includes double quotation marks, you must escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you will not have to escape the double quotation marks. * Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>"

priority

Priority for queuing the request. If server resources are not available for a request that matches the configured rule, this option specifies a priority for queuing the request until the server resources are available again. Enter the value of positive_integer as 1, 2 or 3. The highest priority level is 1 and the lowest priority value is 3. Minimum value: 1 Maximum value: 3

weight

Weight of the priority. Each priority is assigned a weight according to which it is served when server resources are available. The weight for a higher priority request must be set higher than that of a lower priority request. To prevent delays for low-priority requests across multiple priority levels, you can configure weighted queuing for serving requests. The default weights for the priorities are: * Gold - Priority 1 - Weight 3 * Silver - Priority 2 - Weight 2 * Bronze - Priority 3 - Weight 1 Specify the weights as 0 through 101. A weight of 0 indicates that the particular priority level should be served only when there are no requests in any of the priority queues. A weight of 101 specifies a weight of infinity. This means that this priority level is served irrespective of the number of clients waiting in other priority queues. Maximum value: 101

qDepth

Queue depth threshold value. When the queue size (number of requests in the queue) on the virtual server to which this policy is bound, increases to the specified qDepth value, subsequent requests are dropped to the lowest priority level. Maximum value: 4294967294

polqDepth

Policy queue depth threshold value. When the policy queue size (number of requests in all the queues belonging to this policy) increases to the specified polqDepth value, subsequent requests are dropped to the lowest priority level. Maximum value: 4294967294

[Top](#)

rm pq policy

Synopsis

rm pq policy <policyName> ...

Description

Removes a priority queuing policy from the appliance.

Parameters

policyName

Name of the priority queuing policy to be removed.

[Top](#)

set pq policy

Synopsis

```
set pq policy <policyName> [-weight <positive_integer>] [-qDepth <positive_integer> |  
-polqDepth <positive_integer>]
```

Description

Modifies the attributes of a priority queuing policy.

Parameters

policyName

Name of the priority queuing policy to be modified.

weight

Weight of the priority. Each priority is assigned a weight according to which it is served when server resources are available. The weight for a higher priority request must be set higher than that of a lower priority request. To prevent delays for low-priority requests across multiple priority levels, you can configure weighted queuing for serving requests. The default weights for the priorities are: * Gold - Priority 1 - Weight 3 * Silver - Priority 2 - Weight 2 * Bronze - Priority 3 - Weight 1 Specify the weights as 0 through 101. A weight of 0 indicates that the particular priority level should be served only when there are no requests in any of the priority queues. A weight of 101 specifies a weight of infinity. This means that this priority level is served irrespective of the number of clients waiting in other priority queues. Maximum value: 101

qDepth

Queue depth threshold value. When the queue size (number of requests in the queue) on the virtual server to which this policy is bound, increases to the specified qDepth value, subsequent requests are dropped to the lowest priority level. Maximum value: 4294967294

polqDepth

Policy queue depth threshold value. When the policy queue size (number of requests in all the queues belonging to this policy) increases to the specified polqDepth value, subsequent requests are dropped to the lowest priority level. Maximum value: 4294967294

[Top](#)

unset pq policy

Synopsis

unset pq policy <policyName> [-weight] [-qDepth] [-polqDepth]

Description

Use this command to remove pq policy settings. Refer to the set pq policy command for meanings of the arguments.

[Top](#)

show pq policy

Synopsis

show pq policy [<policyName>]

Description

Displays information about the priority queuing policy.

Parameters

policyName

Name of the priority queuing policy about which to display information. If a name is not provided, information about all priority queuing policies is shown.

[Top](#)

stat pq policy

Synopsis

stat pq policy [<policyName>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-clearstats (basic | full)]

Description

Displays statistics of the priority queuing policy.

Parameters

policyName

Name of the priority queuing policy whose statistics must be displayed. If a name is not provided, statistics of all priority queuing policies are shown.

clearstats

Clear the statistics / counters Possible values: basic, full

[Top](#)

pq stats

show pq stats

Synopsis

show pq stats - alias for 'stat pq'

Description

show pq stats is an alias for stat pq

Protocol Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [protocol tcp](#)
- ♦ [protocol http](#)
- ♦ [protocol icmp](#)
- ♦ [protocol ipv6](#)
- ♦ [protocol icmpv6](#)
- ♦ [protocol ip](#)
- ♦ [protocol udp](#)
- ♦ [protocol httpBand](#)

protocol tcp

stat protocol tcp

Synopsis

stat protocol tcp [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-clearstats (basic | full)]

Description

Displays statistics of the TCP protocol.

Parameters

clearstats

Clear the statistics / counters Possible values: basic, full

protocol http

stat protocol http

Synopsis

stat protocol http [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-clearstats (basic | full)]

Description

Displays statistics of the HTTP protocol.

Parameters**clearstats**

Clear the statistics / counters Possible values: basic, full

protocol icmp

stat protocol icmp

Synopsis

```
stat protocol icmp [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile  
<input_filename>] [-clearstats ( basic | full )]
```

Description

Displays statistics of the ICMP protocol.

Parameters**clearstats**

Clear the statistics / counters Possible values: basic, full

protocol ipv6

stat protocol ipv6

Synopsis

```
stat protocol ipv6 [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile  
<input_filename>] [-clearstats ( basic | full )]
```

Description

Displays statistics of the IPv6 protocol.

Parameters**clearstats**

Clear the statistics / counters Possible values: basic, full

protocol icmpv6

stat protocol icmpv6

Synopsis

```
stat protocol icmpv6 [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile  
<input_filename>] [-clearstats ( basic | full )]
```

Description

Displays statistics of the ICMPv6 protocol.

Parameters

clearstats

Clear the statistics / counters Possible values: basic, full

protocol ip

stat protocol ip

Synopsis

```
stat protocol ip [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile  
<input_filename>] [-clearstats ( basic | full )]
```

Description

Displays statistics of the IP protocol.

Parameters

clearstats

Clear the statistics / counters Possible values: basic, full

protocol udp

stat protocol udp

Synopsis

```
stat protocol udp [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile  
<input_filename>] [-clearstats ( basic | full )]
```

Description

Displays statistics of the UDP protocol.

Parameters

clearstats

Clear the statistics / counters Possible values: basic, full

protocol httpBand

[[set](#) | [unset](#) | [show](#)]

set protocol httpBand

Synopsis

```
set protocol httpBand [-reqBandSize <integer>] [-respBandSize <integer>]
```


Description

Sets the band size for HTTP request/response band statistics.

Parameters

reqBandSize

Band size, in bytes, for HTTP request band statistics. For example, if you specify a band size of 100 bytes, statistics will be maintained and displayed for the following size ranges: 0 - 99 bytes 100 - 199 bytes 200 - 299 bytes and so on. Default value: 100
Minimum value: 50

respBandSize

Band size, in bytes, for HTTP response band statistics. For example, if you specify a band size of 100 bytes, statistics will be maintained and displayed for the following size ranges: 0 - 99 bytes 100 - 199 bytes 200 - 299 bytes and so on. Default value: 1024
Minimum value: 50

Example

```
set protocol httpBand -reqBandSize 200 -  
respBandSize 2048
```

[Top](#)

unset protocol httpBand

Synopsis

unset protocol httpBand [-reqBandSize] [-respBandSize]

Description

Use this command to remove protocol httpBand settings. Refer to the set protocol httpBand command for meanings of the arguments.

[Top](#)

show protocol httpBand

Synopsis

show protocol httpBand -type (REQUEST | RESPONSE)

Description

Displays statistics of the HTTP request/response band.

Parameters

type

Type of statistics to display. Possible values: REQUEST, RESPONSE

[Top](#)

QOS Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [qos](#)
- ♦ [qos stats](#)

qos

stat qos

Synopsis

```
stat qos [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]  
[-clearstats ( basic | full )]
```

Description

Display QoS statistics.

Parameters

clearstats

Clear the statistics / counters Possible values: basic, full

qos stats

show qos stats

Synopsis

show qos stats - alias for 'stat qos'

Description

show qos stats is an alias for stat qos

Responder Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [responder policy](#)
- ♦ [responder action](#)
- ♦ [responder policylabel](#)
- ♦ [responder global](#)
- ♦ [responder param](#)
- ♦ [responder htmlpage](#)

responder policy

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#) | [rename](#) | [stat](#)]

add responder policy

Synopsis

add responder policy <name> <rule> <action> [<undefAction>] [-comment <string>] [-logAction <string>] [-appflowAction <string>]

Description

Creates a responder policy, which specifies requests that the NetScaler appliance intercepts and responds to directly instead of forwarding them to a protected server.

Parameters

name

Name for the responder policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.), pound (#), space (), at (@), equals (=), colon (:), and underscore characters. Can be changed after the responder policy is added. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my responder policy" or 'my responder policy').

rule

Default syntax expression that the policy uses to determine whether to respond to the specified request.

action

Name of the responder action to perform if the request matches this responder policy.

undefAction

Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Available settings function as follows: * NOOP - Send the request to the protected server instead of responding to it. * RESET - Reset the request and notify the user's browser, so that the user can resend the request. * DROP - Drop the request without sending a response to the user.

comment

Any type of information about this responder policy.

logAction

Name of the messagelog action to use for requests that match this policy.

appflowAction

AppFlow action to invoke for requests that match this policy.

Example

```
i) add responder policy pol9 "HTTP.REQ.HEADER(\
\"header\\").CONTAINS(\\\"qh3\\")" act_respondwith
```

[Top](#)

rm responder policy

Synopsis

rm responder policy <name>

Description

Removes the specified responder policy.

Parameters

name

Name of the responder policy to remove.

Example

```
rm responder policy pol9
```

[Top](#)

set responder policy

Synopsis

set responder policy <name> [-rule <expression>] [-action <string>] [-undefAction <string>] [-comment <string>] [-logAction <string>] [-appflowAction <string>]

Description

Modifies the rule or action portion of the specified responder policy.

Parameters

name

Name of the responder policy.

rule

Default syntax expression that the policy uses to determine whether to respond to the specified request.

action

Name of the responder action to perform if the request matches this responder policy.

undefAction

Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Available settings function as follows: *

NOOP - Send the request to the protected server instead of responding to it. * RESET - Reset the request and notify the user's browser, so that the user can resend the request. * DROP - Drop the request without sending a response to the user.

comment

Any type of information about this responder policy.

logAction

Name of the messagelog action to use for requests that match this policy.

appflowAction

AppFlow action to invoke for requests that match this policy.

Example

```
set responder policy pol9 -rule "HTTP.REQ.HEADER(\
\"header\\\") .CONTAINS(\\\"qh2\\\") "
```

[Top](#)

unset responder policy**Synopsis**

```
unset responder policy <name> [-undefAction] [-comment] [-logAction] [-
appflowAction]
```

Description

Removes the settings of an existing responder policy. Attributes for which a default value is available revert to their default values. See the set responder policy command for descriptions of the parameters..Refer to the set responder policy command for meanings of the arguments.

Example

```
unset responder policy respol9 -undefAction
```

[Top](#)

show responder policy**Synopsis**

```
show responder policy [<name>] show responder policy stats - alias for 'stat responder
policy'
```

Description

Displays the current settings for the specified responder policy. If no policy name is specified, displays a list of all responder policies currently configured on the NetScaler appliance, with abbreviated settings.

Parameters

name

Name of the responder policy for which to display settings.

Example

```
show responder policy
```

[Top](#)

rename responder policy

Synopsis

```
rename responder policy <name>@ <newName>@
```

Description

Renames the specified responder policy.

Parameters

name

Existing name of the responder policy.

newName

New name for the responder policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space (), at (@), equals (=), colon (:), and underscore characters. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my responder policy" or 'my responder policy').

Example

```
rename responder policy oldname newname
```

[Top](#)

stat responder policy

Synopsis

```
stat responder policy [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-clearstats ( basic | full )]
```

Description

Displays statistics for all responder policies currently configured on the NetScaler appliance, or detailed statistics for the specified policy.

Parameters

name

Name of the responder policy for which to show detailed statistics.

clearstats

Clear the statistics / counters Possible values: basic, full

[Top](#)

responder action

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#) | [rename](#)]

add responder action

Synopsis

add responder action <name> <type> (<target> | <htmlpage>) [-bypassSafetyCheck (YES | NO)] [-comment <string>]

Description

Creates a responder action, which specifies how to respond to a request.

Parameters

name

Name for the responder action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space (), at (@), equals (=), colon (:), and underscore characters. Can be changed after the responder policy is added. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my responder action" or 'my responder action').

type

Type of responder action. Available settings function as follows: * respondwith <target> - Respond to the request with the expression specified as the target. * respondwithhtmlpage - Respond to the request with the uploaded HTML page object specified as the target. * redirect - Redirect the request to the URL specified as the target. * sqlresponse_ok - Send an SQL OK response. * sqlresponse_error - Send an SQL ERROR response. Possible values: noop, respondwith, redirect, respondwithhtmlpage, sqlresponse_ok, sqlresponse_error

target

Expression specifying what to respond with. Typically a URL for redirect policies or a default-syntax expression. In addition to NetScaler default-syntax expressions that refer to information in the request, a stringbuilder expression can contain text and HTML, and simple escape codes that define new lines and paragraphs. Enclose each stringbuilder expression element (either a NetScaler default-syntax expression or a string) in double quotation marks. Use the plus (+) character to join the elements. Examples: 1) Respondwith expression that sends an HTTP 1.1 200 OK response: "HTTP/1.1 200 OK\r\n\r\n" 2) Redirect expression that redirects user to the specified web host and appends the request URL to the redirect. "http://backupsite2.com" +

HTTP.REQ.URL 3) Respondwith expression that sends an HTTP 1.1 404 Not Found response with the request URL included in the response: "HTTP/1.1 404 Not Found\r\n\r\n"+ "HTTP.REQ.URL.HTTP_URL_SAFE" + "does not exist on the web server." The following requirement applies only to the NetScaler CLI: Enclose the entire expression in single quotation marks. (NetScaler default expression elements should be included inside the single quotation marks for the entire expression, but do not need to be enclosed in double quotation marks.)

htmlpage

For respondwithhtmlpage policies, name of the HTML page object to use as the response. You must first import the page object.

bypassSafetyCheck

Bypass the safety check, allowing potentially unsafe expressions. An unsafe expression in a response is one that contains references to request elements that might not be present in all requests. If a response refers to a missing request element, an empty string is used instead. Possible values: YES, NO Default value: NO

comment

Comment. Any type of information about this responder action.

Example

```
1) add responder action act1 respondwith "\"HTTP/
1.1 200 OK\\r\\n\\r\\n\\\"
2) add responder action resp respondwithhtmlpage
my-responder-page,
3) add responder action redir_action redirect
'"http://backupsite2.com" + HTTP.REQ.URL' -
bypassSafetyCheck YES
```

[Top](#)

rm responder action

Synopsis

rm responder action <name>

Description

Removes the specified responder action.

Parameters

name

Name of the responder action to remove.

Example

```
rm responder action act_before
```


[Top](#)

set responder action

Synopsis

```
set responder action <name> [-target <string> [-bypassSafetyCheck ( YES | NO )]] [-htmlpage <string>] [-comment <string>]
```

Description

Modifies the specified parameters of a responder action.

Parameters

name

Name of the responder action to be modified.

target

Expression specifying what to respond with. Typically a URL for redirect policies or a default-syntax expression. In addition to NetScaler default-syntax expressions that refer to information in the request, a stringbuilder expression can contain text and HTML, and simple escape codes that define new lines and paragraphs. Enclose each stringbuilder expression element (either a NetScaler default-syntax expression or a string) in double quotation marks. Use the plus (+) character to join the elements. Examples: 1) Respondwith expression that sends an HTTP 1.1 200 OK response: "HTTP/1.1 200 OK\r\n\r\n" 2) Redirect expression that redirects user to the specified web host and appends the request URL to the redirect. "http://backupsite2.com" + HTTP.REQ.URL 3) Respondwith expression that sends an HTTP 1.1 404 Not Found response with the request URL included in the response: "HTTP/1.1 404 Not Found\r\n\r\n" + "HTTP.REQ.URL.HTTP_URL_SAFE" + "does not exist on the web server." The following requirement applies only to the NetScaler CLI: Enclose the entire expression in single quotation marks. (NetScaler default expression elements should be included inside the single quotation marks for the entire expression, but do not need to be enclosed in double quotation marks.)

htmlpage

For respondwithhtmlpage policies, name of the HTML page object to use as the response. You must first import the page object.

comment

Comment. Any type of information about this responder action.

Example

```
1. set responder action act_responder -target
   'HTTP.REQ.HEADER(MYURL)' -bypassSafetyCheck YES/,
2. set responder action act_responder -htmlpage my-
   local-file
```

[Top](#)

unset responder action

Synopsis

unset responder action <name> -comment

Description

Use this command to remove responder action settings. Refer to the set responder action command for meanings of the arguments.

[Top](#)

show responder action

Synopsis

show responder action [<name>]

Description

Displays the current settings for the specified responder action. If no action name is provided, displays a list of all responder actions currently configured on the NetScaler appliance, with abbreviated settings.

Parameters

name

Name of the responder action.

Example

```
1. show responder action
2. show responder action act_insert
```

[Top](#)

rename responder action

Synopsis

rename responder action <name>@ <newName>@

Description

Renames a responder action.

Parameters

name

Existing name of the responder action.

newName

New name for the responder action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space (), at (@), equals (=), colon (:), and underscore characters. The following requirement applies only to the NetScaler CLI: If the name

includes one or more spaces, enclose the name in double or single quotation marks (for example, "my responder action" or my responder action').

Example

```
rename responder action oldname newname
```

[Top](#)

responder policylabel

[[add](#) | [rm](#) | [bind](#) | [unbind](#) | [show](#) | [stat](#) | [rename](#)]

add responder policylabel

Synopsis

```
add responder policylabel <labelName> [-policylabeltype <policylabeltype>]
```

Description

Creates a user-defined responder policy label, to which you can bind policies. A policy label is a tool for evaluating a set of policies in a specified order. By using a policy label, you can configure the responder feature to choose the next policy, invoke a different policy label, or terminate policy evaluation completely by looking at whether the previous policy evaluated to TRUE or FALSE.

Parameters

labelName

Name for the responder policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space (), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the responder policy label is added. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my responder policy label" or my responder policy label').

policylabeltype

Type of responses sent by the policies bound to this policy label. Types are: * HTTP - HTTP responses. * OTHERTCP - NON-HTTP TCP responses. * SIP_UDP - SIP responses. * MYSQL - SQL responses in MySQL format. * MSSQL - SQL responses in Microsoft SQL format. Possible values: HTTP, OTHERTCP, SIP_UDP, MYSQL, MSSQL Default value: NS_PLTMAP_RSP_REQ

Example

```
add responder policylabel resp_lab
```

[Top](#)

rm responder policylabel

Synopsis

rm responder policylabel <labelName>

Description

Removes a responder policy label.

Parameters

labelName

Name of the responder policy label to remove.

Example

```
rm responder policylabel resp_lab
```

[Top](#)

bind responder policylabel

Synopsis

bind responder policylabel <labelName> <policyName> <priority>
[<gotoPriorityExpression>] [-invoke (<labelType> <labelName>)]

Description

Binds the specified responder policy to the specified policy label.

Parameters

labelName

Name of the responder policy label to which to bind the policy.

policyName

Name of the policy to bind to the responder policy label.

Example

```
i)      bind responder policylabel resp_lab pol_resp
1 2
ii)     bind responder policylabel resp_lab
pol_resp 1 2 -invoke vserver CURRENT
```

[Top](#)

unbind responder policylabel

Synopsis

unbind responder policylabel <labelName> <policyName> [-priority <positive_integer>]

Description

Unbinds the specified responder policy from the specified policy label.

Parameters

labelName

Name for the responder policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space (), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the responder policy label is added. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my responder policy label" or my responder policy label').

policyName

The name of the policy to be unbound.

priority

Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

```
unbind responder policylabel resp_lab pol_resp
```

[Top](#)

show responder policylabel

Synopsis

show responder policylabel [<labelName>]

Description

Displays the current settings for the specified responder policy label. If no policy label is specified, displays a list of all responder policy labels currently configured on the NetScaler appliance, with abbreviated settings.

Parameters

labelName

Name of the responder policy label.

Example

```
i) show responder policylabel resp_lab
ii) show responder policylabel
```

[Top](#)

stat responder policylabel

Synopsis

```
stat responder policylabel [<labelName>] [-detail] [-fullValues] [-ntimes  
<positive_integer>] [-logFile <input_filename>] [-clearstats ( basic | full )]
```

Description

Displays statistics for the specified responder policy label. If no policy label name is provided, displays abbreviated statistics for all responder policy labels currently configured on the NetScaler appliance.

Parameters

labelName

Name of the responder policy label.

clearstats

Clear the statistics / counters Possible values: basic, full

[Top](#)

rename responder policylabel

Synopsis

```
rename responder policylabel <labelName>@ <newName>@
```

Description

Renames the specified responder policy label.

Parameters

labelName

Current name of the responder policy label.

newName

New name for the responder policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space (), at (@), equals (=), colon (:), and underscore characters.

Example

```
rename responder policylabel oldname newname
```

[Top](#)

responder global

[[bind](#) | [unbind](#) | [show](#)]

bind responder global

Synopsis

```
bind responder global <policyName> <priority> [<gotoPriorityExpression>] [-type  
<type>] [-invoke (<labelType> <labelName>)]
```

Description

Activates the specified responder policy for all requests sent to the NetScaler appliance.

Parameters

policyName

Name of the responder policy to activate. If you want to create the policy as well as activate it, specify a name for the responder policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space (), at (@), equals (=), colon (:), and underscore characters. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my responder policy" or 'my responder policy').

Example

```
i)      bind responder global pol9 9
```

[Top](#)

unbind responder global

Synopsis

```
unbind responder global <policyName> [-type <type>] [-priority <positive_integer>]
```

Description

Unbind the specified responder policy from responder global.

Parameters

policyName

Name of the policy to unbind.

priority

Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

```
unbind responder global pol9
```

[Top](#)

show responder global

Synopsis

show responder global [-type <type>]

Description

Displays the list of policies bound to the specified responder global bind point. If no bind point is specified, displays a list of all policies bound to responder global.

Parameters

type

Specifies the bind point whose policies you want to display. Available settings function as follows: * REQ_OVERRIDE - Request override. Binds the policy to the priority request queue. * REQ_DEFAULT - Binds the policy to the default request queue. * OTHERTCP_REQ_OVERRIDE - Binds the policy to the non-HTTP TCP priority request queue. * OTHERTCP_REQ_DEFAULT - Binds the policy to the non-HTTP TCP default request queue.. * SIPUDP_REQ_OVERRIDE - Binds the policy to the SIP UDP priority response queue.. * SIPUDP_REQ_DEFAULT - Binds the policy to the SIP UDP default response queue. * MSSQL_REQ_OVERRIDE - Binds the policy to the Microsoft SQL priority response queue.. * MSSQL_REQ_DEFAULT - Binds the policy to the Microsoft SQL default response queue. * MYSQL_REQ_OVERRIDE - Binds the policy to the MySQL priority response queue. * MYSQL_REQ_DEFAULT - Binds the policy to the MySQL default response queue. Possible values: REQ_OVERRIDE, REQ_DEFAULT, OVERRIDE, DEFAULT, OTHERTCP_REQ_OVERRIDE, OTHERTCP_REQ_DEFAULT, SIPUDP_REQ_OVERRIDE, SIPUDP_REQ_DEFAULT, MSSQL_REQ_OVERRIDE, MSSQL_REQ_DEFAULT, MYSQL_REQ_OVERRIDE, MYSQL_REQ_DEFAULT

Example

```
show responder global
```

[Top](#)

responder param

[[set](#) | [unset](#) | [show](#)]

set responder param

Synopsis

set responder param -undefAction <string>

Description

Sets the default responder undefined action. If an UNDEF event is triggered during policy evaluation and if no undefAction is specified for the current policy, this value is used.

Parameters

undefAction

Action to perform when policy evaluation creates an UNDEF condition. Available settings function as follows: * NOOP - Send the request to the protected server. * RESET - Reset the request and notify the user's browser, so that the user can resend the request. * DROP - Drop the request without sending a response to the user. Default value: "NOOP"

Example

```
set responder param -undefAction RESET
```

[Top](#)

unset responder param

Synopsis

```
unset responder param -undefAction
```

Description

Resets the global undefAction to NOOP..Refer to the set responder param command for meanings of the arguments.

Example

```
unset responder param -undefAction
```

[Top](#)

show responder param

Synopsis

```
show responder param
```

Description

Displays the default responder undefAction.

Example

```
show responder param
```

[Top](#)

responder htmlpage

[[import](#) | [rm](#) | [update](#) | [show](#)]

import responder htmlpage

Synopsis

```
import responder htmlpage [<src>] <name> [-comment <string>] [-overwrite]
```

Description

Imports the specified HTML page to the NetScaler appliance, assigns it the specified name, and stores it in the list of Responder HTML page objects.

Parameters

src

Local path to and name of, or URL \(protocol, host, path, and file name\) for, the file in which to store the imported HTML page. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

name

Name to assign to the HTML page object on the NetScaler appliance.

comment

Any comments to preserve information about the HTML page object.

overwrite

Overwrites the existing file

Example

```
import responder htmlpage http://www.example.com/
page.html my-responder-page
```

[Top](#)

rm responder htmlpage

Synopsis

```
rm responder htmlpage <name>
```

Description

Removes the specified HTML page object.

Parameters

name

Name of the HTML page object to remove.

Example

```
rm responder htmlpage <name>
```

[Top](#)

update responder htmlpage

Synopsis

```
update responder htmlpage <name>
```

Description

Updates the specified HTML page object from the source.

Parameters**name**

Name to assign to the HTML page object on the NetScaler appliance.

Example

```
update responder htmlpage my-responder-page
```

[Top](#)

show responder htmlpage

Synopsis

```
show responder htmlpage [<name>]
```

Description

Displays the specified HTML page object. If no HTML page object is specified, lists all HTML page objects on the NetScaler appliance.

Parameters**name**

Name of the HTML page object to display.

Example

```
show responder htmlpage
```

[Top](#)

Rewrite Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [rewrite policy](#)
- ♦ [rewrite action](#)
- ♦ [rewrite policylabel](#)
- ♦ [rewrite global](#)
- ♦ [rewrite param](#)

rewrite policy

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#) | [stat](#) | [rename](#)]

add rewrite policy

Synopsis

```
add rewrite policy <name> <rule> <action> [<undefAction>] [-comment <string>] [-logAction <string>]
```

Description

Creates a rewrite policy, which specifies which requests or responses to rewrite.

Parameters

name

Name for the rewrite policy. Must begin with a letter, number, or the underscore character (`_`), and must contain only letters, numbers, and the hyphen (`-`), period (`.`) hash (`#`), space (), at (`@`), equals (`=`), colon (`:`), and underscore characters. Can be changed after the rewrite policy is added. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my rewrite policy" or 'my rewrite policy').

rule

Expression against which traffic is evaluated. Written in default syntax. Note: Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the `+` operator. For example, you can create a 500-character string as follows: "`<string of 255 characters>`" + "`<string of 245 characters>`" (Classic expressions are not supported in the cluster build.) The following requirements apply only to the NetScaler CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the `\` character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action

Name of the rewrite action to perform if the request or response matches this rewrite policy.

undefAction

Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Available settings function as follows: * NOREWRITE - Send the request to the protected server without rewriting. * RESET - Reset the request and notify the user's browser, so that the user can resend the request. * DROP - Drop the request without sending a response to the user.

comment

Any comments to preserve information about this rewrite policy.

logAction

Name of messagelog action to use when a request matches this policy.

Example

```
i)      add rewrite policy pol9 "HTTP.REQ.HEADER(\
\"header\").CONTAINS(\"qh3\")" act_insert
ii)     add rewrite policy pol9 "HTTP.REQ.HEADER(\
\"header\").CONTAINS(\"qh3\")" act_insert
NOREWRITE
iii)    add rewrite policy pol9 "HTTP.REQ.HEADER(\
\"header\").CONTAINS(\"qh3\")" act_insert RESET
iii)    add rewrite policy pol9 "HTTP.REQ.HEADER(\
\"header\").CONTAINS(\"qh3\")" act_insert DROP
```

[Top](#)

rm rewrite policy**Synopsis**

rm rewrite policy <name>

Description

Removes the specified rewrite policy.

Parameters**name**

Name of the rewrite policy to be removed.

Example

```
rm rewrite policy pol9
```

[Top](#)

set rewrite policy

Synopsis

```
set rewrite policy <name> [-rule <expression>] [-action <string>] [-undefAction  
<string>] [-comment <string>] [-logAction <string>]
```

Description

Modifies the specified parameters of a rewrite policy.

Parameters

name

Name of the rewrite policy to modify.

rule

Expression against which traffic is evaluated. Written in default syntax. Note: Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>" (Classic expressions are not supported in the cluster build.) The following requirements apply only to the NetScaler CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action

Name of the rewrite action to perform if the request or response matches this rewrite policy.

undefAction

Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Available settings function as follows: * NOREWRITE - Send the request to the protected server without rewriting. * RESET - Reset the request and notify the user's browser, so that the user can resend the request. * DROP - Drop the request without sending a response to the user.

comment

Any comments to preserve information about this rewrite policy.

logAction

Name of message log action to use when a request matches this policy.

Example

```
set rewrite policy pol9 -rule "HTTP.REQ.HEADER(\  
\"header\\\")\".CONTAINS(\\\"qh2\\\") "
```

[Top](#)

unset rewrite policy

Synopsis

unset rewrite policy <name> [-undefAction] [-comment] [-logAction]

Description

Removes the settings of an existing rewrite policy. Attributes for which a default value is available revert to their default values. See the set rewrite policy command for a description of the parameters..Refer to the set rewrite policy command for meanings of the arguments.

Example

```
unset rewrite policy pol9 -undefAction
```

[Top](#)

show rewrite policy

Synopsis

show rewrite policy [<name>] show rewrite policy stats - alias for 'stat rewrite policy'

Description

Displays the current settings for the specified rewrite policy. If no policy name is provided, displays a list of all rewrite policies currently configured on the NetScaler appliance.

Parameters

name

Name of the rewrite policy.

Example

```
show rewrite policy
```

[Top](#)

stat rewrite policy

Synopsis

stat rewrite policy [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-clearstats (basic | full)]

Description

Displays statistics for the specified rewrite policy. If no policy name is specified, displays abbreviated statistics for all rewrite policies currently configured on the NetScaler appliance.

Parameters

name

Name of the rewrite policy.

clearstats

Clear the statistics / counters Possible values: basic, full

Example

```
stat rewrite policy
```

[Top](#)

rename rewrite policy

Synopsis

rename rewrite policy <name>@ <newName>@

Description

Renames the specified rewrite policy. You must restart the NetScaler appliance to put new name in effect.

Parameters

name

Existing name of the rewrite policy.

newName

New name for the rewrite policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space (), at (@), equals (=), colon (:), and underscore characters. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my rewrite policy" or 'my rewrite policy').

Example

```
rename rewrite policy oldname newname
```

[Top](#)

rewrite action

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#) | [rename](#)]

add rewrite action

Synopsis

```
add rewrite action <name> <type> <target> [<stringBuilderExpr>] [-pattern
<expression> | -search <expression>] [-bypassSafetyCheck ( YES | NO )] [-refineSearch
<string>] [-comment <string>]
```

Description

Creates a rewrite action, which specifies exactly what modifications to make to a request or response before forwarding that request or response to the protected web server or to the user. In addition to user-defined actions, the rewrite feature has the following three built-in actions: * NOREWRITE - Sends the request or response to the user without rewriting it. * RESET - Resets the connection and notifies the user's browser, so that the user can resend the request. * DROP - Drops the connection without sending a response to the user. One of the following three flow types is implicitly associated with every action: * Request - Action applies to the request. * Response - Action applies to the response. * Neutral - Action applies to both requests and responses.

Parameters

name

Name for the user-defined rewrite action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space (), at (@), equals (=), colon (:), and underscore characters. Can be changed after the rewrite policy is added. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my rewrite action" or 'my rewrite action').

type

Type of user-defined rewrite action. The information that you provide for, and the effect of, each type are as follows: * REPLACE <target> <string_builder_expr>. Replaces the string with the string-builder expression. * REPLACE_ALL <target> <string_builder_expr1> -(pattern|search) <string_builder_expr2>. In the request or response specified by <target>, replaces all occurrences of the string defined by <string_builder_expr1> with the string defined by <string_builder_expr2>. You can use a PCRE-format pattern or the search facility to find the strings to be replaced. * REPLACE_HTTP_RES <string_builder_expr>. Replaces the complete HTTP response with the string defined by the string-builder expression. * REPLACE_SIP_RES <target> - Replaces the complete SIP response with the string specified by <target>. * INSERT_HTTP_HEADER <header_string_builder_expr> <contents_string_builder_expr>. Inserts the HTTP header specified by <header_string_builder_expr> and header contents specified by <contents_string_builder_expr>. * DELETE_HTTP_HEADER <target>. Deletes the HTTP header specified by <target>. * CORRUPT_HTTP_HEADER <target>. Replaces the header name of all occurrences of the HTTP header specified by <target> with a corrupted name, so that it will not be recognized by the receiver Example: MY_HEADER is changed to MHEY_ADER. * INSERT_BEFORE

<string_builder_expr1> <string_builder_expr1>. Finds the string specified in <string_builder_expr1> and inserts the string in <string_builder_expr2> before it. * INSERT_BEFORE_ALL <target> <string_builder_expr1> -(pattern|search) <string_builder_expr2>. In the request or response specified by <target>, locates all occurrences of the string specified in <string_builder_expr1> and inserts the string specified in <string_builder_expr2> before each. You can use a PCRE-format pattern or the search facility to find the strings. * INSERT_AFTER <string_builder_expr1> <string_builder_expr2>. Finds the string specified in <string_builder_expr1>, and inserts the string specified in <string_builder_expr2> after it. * INSERT_AFTER_ALL <target> <string_builder_expr1> -(pattern|search) <string_builder_expr>. In the request or response specified by <target>, locates all occurrences of the string specified by <string_builder_expr1> and inserts the string specified by <string_builder_expr2> after each. You can use a PCRE-format pattern or the search facility to find the strings. * DELETE <target>. Finds and deletes the specified target. * DELETE_ALL <target> -(pattern|search) <string_builder_expr>. In the request or response specified by <target>, locates and deletes all occurrences of the string specified by <string_builder_expr>. You can use a PCRE-format pattern or the search facility to find the strings. Possible values: noop, delete, insert_http_header, delete_http_header, corrupt_http_header, insert_before, insert_after, replace, replace_http_res, delete_all, replace_all, insert_before_all, insert_after_all, clientless_vpn_encode, clientless_vpn_encode_all, clientless_vpn_decode, clientless_vpn_decode_all, insert_sip_header, delete_sip_header, corrupt_sip_header, replace_sip_res

target

Default syntax expression that specifies which part of the request or response to rewrite.

stringBuilderExpr

Default syntax expression that specifies the content to insert into the request or response at the specified location, or that replaces the specified string.

pattern

Pattern that is used to match multiple strings in the request or response. The pattern may be a string literal (without quotes) or a PCRE-format regular expression with a delimiter that consists of any printable ASCII non-alphanumeric character except for the underscore (`_`) and space () that is not otherwise used in the expression. Example: `re-https?://|HTTPS?://~` The preceding regular expression can use the tilde (`~`) as the delimiter because that character does not appear in the regular expression itself. Used in the INSERT_BEFORE_ALL, INSERT_AFTER_ALL, REPLACE_ALL, and DELETE_ALL action types.

search

Search facility that is used to match multiple strings in the request or response. Used in the INSERT_BEFORE_ALL, INSERT_AFTER_ALL, REPLACE_ALL, and DELETE_ALL action types. The following search types are supported: * Text ("text(string)") - A literal string. Example: `-search text("hello")` * Regular expression ("regex(re<delimiter>regular exp<delimiter>)") - Pattern that is used to match multiple strings in the request or response. The pattern may be a string literal (without quotes) or a PCRE-format regular expression with a delimiter that consists of any printable ASCII non-alphanumeric character except for the underscore (`_`) and space () that is not otherwise used in the expression. Example: `-search`

regex(re~^hello~) The preceding regular expression can use the tilde (~) as the delimiter because that character does not appear in the regular expression itself. * **XPath** ("xpath(xp<delimiter>xpath expression<delimiter>)") - An XPath expression. Example: -search xpath(xp%/a/b%) * **JSON** ("xpath_json(xp<delimiter>xpath expression<delimiter>)") - An XPath JSON expression. Example: -search xpath_json(xp%/a/b%) **NOTE:** JSON searches use the same syntax as XPath searches, but operate on JSON files instead of standard XML files. * **Patset** ("patset(patset)") - A predefined pattern set. Example: -search patset("patset1")

bypassSafetyCheck

Bypass the safety check and allow unsafe expressions. An unsafe expression is one that contains references to message elements that might not be present in all messages. If an expression refers to a missing request element, an empty string is used instead. Possible values: YES, NO Default value: NO

refineSearch

Specify additional criteria to refine the results of the search. Always starts with the "extend(m,n)" operation, where 'm' specifies number of bytes to the left of selected data and 'n' specifies number of bytes to the right of selected data. You can use refineSearch only on body expressions, and for the INSERT_BEFORE_ALL, INSERT_AFTER_ALL, REPLACE_ALL, and DELETE_ALL action types.

comment

Comment. Can be used to preserve information about this rewrite action.

Example

```
i)    add rewrite action act_insert
INSERT_HTTP_HEADER change_req "\\\"no change\\\""
.    This Adds to http header
will add the header change_req: no change.
ii)   add rewrite action act_replace REPLACE
"HTTP.REQ.URL.PREFIX(1)" "HTTP.REQ.URL.PREFIX(1)+\
\"citrix/\\\"" -bypassSafetyCheck YES
.    If HTTP.REQ.URL.PREFIX(1) is / the result
would be /citrix/
iii)  add rewrite action act_before
INSERT_BEFORE "HTTP.REQ.HEADER(\\\"host\
\").VALUE(0)" "\\\"india\\\""
.    If HTTP.REQ.HEADER(\\\"host\").VALUE(0) is
netscaler.com the result would be
indianetscaler.com
iv)   add rewrite action act_after INSERT_AFTER
"HTTP.REQ.HEADER(\\\"host\
\").TYPECAST_LIST_T(' ').GET(0)" "\\\"-india\\\""
.    If HTTP.REQ.HEADER(\\\"host\").VALUE(0) is
support.netscaler.com then the result would be
support-india.netscaler.com
v)    add rewrite action act_delete DELETE
"HTTP.REQ.HEADER(\\\"host\").VALUE(0)"
will leave the Host header looking like "HOST: ".
vi)   add rewrite action act_delete_header
DELETE_HTTP_HEADER Host
will delete the Host header. If Host header occurs
```

```
more than once all occurrence of the header will
be deleted.
vii)      add rewrite action act_corrupt_header
CORRUPT_HTTP_HEADER Host
will corrupt the Host header. If Host header
occurs more than once all occurrence of the header
will be corrupted.
```

[Top](#)

rm rewrite action

Synopsis

```
rm rewrite action <name>
```

Description

Removes a rewrite action.

Parameters

name

Name of the rewrite action to remove.

Example

```
rm rewrite action act_before
```

[Top](#)

set rewrite action

Synopsis

```
set rewrite action <name> [-target <string>] [-stringBuilderExpr <string>] [-pattern
<expression> | -search <expression>] [-bypassSafetyCheck ( YES | NO )] [-refineSearch
<string>] [-comment <string>]
```

Description

Modifies the specified parameters of a rewrite action.

Parameters

name

Name of the rewrite action to modify.

target

Expression that specifies which part of the connection to rewrite.

stringBuilderExpr

Default syntax expression that specifies the content to insert into the request or response at the specified location, or that replaces the specified string.

pattern

Pattern that is used to match multiple strings in the request or response. The pattern may be a string literal (without quotes) or a PCRE-format regular expression with a delimiter that consists of any printable ASCII non-alphanumeric character except for the underscore (`_`) and space () that is not otherwise used in the expression.

Example: `re~https?://|HTTPS?://~` The preceding regular expression can use the tilde (`~`) as the delimiter because that character does not appear in the regular expression itself. Used in the `INSERT_BEFORE_ALL`, `INSERT_AFTER_ALL`, `REPLACE_ALL`, and `DELETE_ALL` action types.

search

Search facility that is used to match multiple strings in the request or response. Used in the `INSERT_BEFORE_ALL`, `INSERT_AFTER_ALL`, `REPLACE_ALL`, and `DELETE_ALL` action types. The following search types are supported: * Text (`"text(string)"`) - A literal string. Example: `-search text("hello")` * Regular expression

(`"regex(re<delimiter>regular exp<delimiter>)"`) - Pattern that is used to match multiple strings in the request or response. The pattern may be a string literal (without quotes) or a PCRE-format regular expression with a delimiter that consists of any printable ASCII non-alphanumeric character except for the underscore (`_`) and space () that is not otherwise used in the expression. Example: `-search`

`regex(re~^hello~)` The preceding regular expression can use the tilde (`~`) as the delimiter because that character does not appear in the regular expression itself. * XPath (`"xpath(xp<delimiter>xpath expression<delimiter>)"`) - An XPath expression.

Example: `-search xpath(xp%/a/b%)` * JSON (`"xpath_json(xp<delimiter>xpath expression<delimiter>)"`) - An XPath JSON expression. Example: `-search xpath_json(xp%/a/b%)` NOTE: JSON searches use the same syntax as XPath searches, but operate on JSON files instead of standard XML files. * Patset (`"patset(patset)"`) - A predefined pattern set. Example: `-search patset("patset1")`

bypassSafetyCheck

Bypass the safety check and allow unsafe expressions. An unsafe expression is one that contains references to message elements that might not be present in all messages. If an expression refers to a missing request element, an empty string is used instead. Possible values: YES, NO Default value: NO

refineSearch

Specify additional criteria to refine the results of the search. Always starts with the `"extend(m,n)"` operation, where 'm' specifies number of bytes to the left of selected data and 'n' specifies number of bytes to the right of selected data. You can use `refineSearch` only on body expressions, and for the `INSERT_BEFORE_ALL`, `INSERT_AFTER_ALL`, `REPLACE_ALL`, and `DELETE_ALL` action types.

comment

Comment. Can be used to preserve information about this rewrite action.

Example

```
set rewrite action rwact1 -target
"HTTP.REQ.HEADER(\\\"MyHdr\\\")" -stringBuilderExpr
"HTTP.REQ.URL.MARK_SAFE"
```

[Top](#)

unset rewrite action

Synopsis

```
unset rewrite action <name> [-stringBuilderExpr] [-refineSearch] [-comment]
```

Description

Use this command to remove rewrite action settings. Refer to the set rewrite action command for meanings of the arguments.

[Top](#)

show rewrite action

Synopsis

```
show rewrite action [<name>]
```

Description

Displays the current settings for the specified rewrite action. If no rewrite action name is provided, displays a list of all rewrite actions currently configured on the NetScaler appliance.

Parameters

name

Name of the rewrite action.

Example

```
1. show rewrite action
   2. show rewrite action act_insert
```

[Top](#)

rename rewrite action

Synopsis

```
rename rewrite action <name>@ <newName>@
```

Description

Renames a rewrite action.

Parameters

name

Existing name of the rewrite action.

newName

New name for the rewrite action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space (), at (@), equals (=), colon (:), and underscore

characters. Can be changed after the rewrite policy is added. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my rewrite action" or 'my rewrite action').

Example

```
rename rewrite action oldname newname
```

[Top](#)

rewrite policylabel

[[add](#) | [rm](#) | [bind](#) | [unbind](#) | [show](#) | [stat](#) | [rename](#)]

add rewrite policylabel

Synopsis

add rewrite policylabel <labelName> <transform>

Description

Creates a user-defined rewrite policy label.

Parameters

labelName

Name for the rewrite policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space (), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the rewrite policy label is added. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my rewrite policy label" or 'my rewrite policy label').

transform

Types of transformations allowed by the policies bound to the label. For Rewrite, the following types are supported: * http_req - HTTP requests * http_res - HTTP responses * othertcp_req - Non-HTTP TCP requests * othertcp_res - Non-HTTP TCP responses * url - URLs * text - Text strings * clientless_vpn_req - NetScaler clientless VPN requests * clientless_vpn_res - NetScaler clientless VPN responses * sipudp_req - SIP requests * sipudp_res - SIP responses Possible values: http_req, http_res, othertcp_req, othertcp_res, url, text, clientless_vpn_req, clientless_vpn_res, sipudp_req, sipudp_res

Example

```
add rewrite policylabel trans_http_url http_req
```

[Top](#)

rm rewrite policylabel

Synopsis

rm rewrite policylabel <labelName>

Description

Removes the specified rewrite policy label.

Parameters

labelName

Name of the rewrite policy label to remove.

Example

```
rm rewrite policylabel trans_http_url
```

[Top](#)

bind rewrite policylabel

Synopsis

bind rewrite policylabel <labelName> <policyName> <priority>
[<gotoPriorityExpression>] [-invoke (<labelType> <labelName>)]

Description

Binds the specified rewrite policy to the specified policy label.

Parameters

labelName

Name of the rewrite policy label to which to bind the policy.

policyName

Name of the rewrite policy to bind to the policy label.

Example

```
i)      bind rewrite policylabel trans_http_url  
pol_1 1 2 -invoke reqvserver CURRENT  
ii)     bind rewrite policylabel trans_http_url  
pol_2 2
```

[Top](#)

unbind rewrite policylabel

Synopsis

unbind rewrite policylabel <labelName> <policyName> [-priority <positive_integer>]

Description

Unbinds the specified rewrite policy from the specified policy label. See the bind rewrite policylabel command for a description of the parameters.

Parameters

labelName

Name for the rewrite policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space (), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the rewrite policy label is added. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my rewrite policy label" or 'my rewrite policy label').

policyName

Name of the rewrite policy to bind to the policy label.

priority

Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

```
unbind rewrite policylabel trans_http_url pol_1
```

[Top](#)

show rewrite policylabel

Synopsis

show rewrite policylabel [<labelName>]

Description

Displays the current settings for the specified rewrite policy label. If no policy label is specified, displays a list of all rewrite policy labels currently configured on the NetScaler appliance.

Parameters

labelName

Name of the rewrite policy label.

Example

```
i)      show rewrite policylabel trans_http_url
ii)     show rewrite policylabel
```

[Top](#)

stat rewrite policylabel

Synopsis

```
stat rewrite policylabel [<labelName>] [-detail] [-fullValues] [-ntimes
<positive_integer>] [-logFile <input_filename>] [-clearstats ( basic | full )]
```

Description

Displays statistics for the specified rewrite policy label. If no policy label name is provided, displays abbreviated statistics for all rewrite policy labels currently configured on the NetScaler appliance.

Parameters

labelName

Name of the rewrite policy label.

clearstats

Clear the statistics / counters Possible values: basic, full

[Top](#)

rename rewrite policylabel

Synopsis

```
rename rewrite policylabel <labelName>@ <newName>@
```

Description

Renames a rewrite policy label.

Parameters

labelName

Current name of the policy label.

newName

New name for the rewrite policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space (), at (@), equals (=), colon (:), and underscore characters. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy label" or 'my policy label').

Example

```
rename rewrite policylabel oldname newname
```

[Top](#)

rewrite global

[[bind](#) | [unbind](#) | [show](#)]

bind rewrite global

Synopsis

```
bind rewrite global <policyName> <priority> [<gotoPriorityExpression>] [-type <type>]
[-invoke (<labelType> <labelName>)]
```

Description

Activates the specified rewrite policy globally.

Parameters**policyName**

Name of the rewrite policy to activate.

Example

```
i)    bind rewrite global pol9 9
      ii)    bind rewrite global pol9 9 120
      iii)   bind rewrite global pol9 9
"HTTP.REQ.HEADER(\"qh3\
\").TYPECAST_NUM_T(DECIMAL) "
```

[Top](#)

unbind rewrite global

Synopsis

```
unbind rewrite global <policyName> [-type <type>] [-priority <positive_integer>]
```

Description

Unbinds the specified rewrite policy from rewrite global. See the bind rewrite global command for a description of the parameters.

Parameters**policyName**

Name of the rewrite policy to deactivate.

priority

Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

```
unbind rewrite global pol9
```

[Top](#)**show rewrite global****Synopsis**

show rewrite global [-type <type>]

Description

Displays the list of policies bound to the specified rewrite global policy bank. If no policy bank is specified, displays a list of all policies bound to rewrite global.

Parameters**type**

The bindpoint to which to policy is bound. Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT, OTHERTCP_REQ_OVERRIDE, OTHERTCP_REQ_DEFAULT, OTHERTCP_RES_OVERRIDE, OTHERTCP_RES_DEFAULT, SIPUDP_REQ_OVERRIDE, SIPUDP_REQ_DEFAULT, SIPUDP_RES_OVERRIDE, SIPUDP_RES_DEFAULT

Example

```
show rewrite global
```

[Top](#)**rewrite param**

[[set](#) | [unset](#) | [show](#)]

set rewrite param**Synopsis**

set rewrite param -undefAction <string>

Description

Sets the default rewrite undefined action. If an UNDEF event is triggered during policy evaluation and if no undefAction is specified for the current policy, this value is used.

Parameters

undefAction

Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Available settings function as follows: * NOOP - Send the request to the protected server instead of responding to it. * RESET - Reset the request and notify the user's browser, so that the user can resend the request. * DROP - Drop the request without sending a response to the user. Default value: "NOREWRITE"

Example

```
set rewrite param -undefAction RESET
```

[Top](#)

unset rewrite param

Synopsis

```
unset rewrite param -undefAction
```

Description

Resets the global undefAction to NOREWRITE..Refer to the set rewrite param command for meanings of the arguments.

Example

```
unset rewrite param -undefAction
```

[Top](#)

show rewrite param

Synopsis

```
show rewrite param
```

Description

Displays the default rewrite undefAction.

Example

```
show rewrite param
```

[Top](#)

Router Commands

vttysh

Synopsis

vttysh

Description

Enters into the Virtual Teletype Shell (VTYSH) prompt, at which you can configure all the dynamic routing protocols. The NetScaler dynamic routing suite is based on ZebOS, the commercial version of GNU Zebra.

SC Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [sc](#)
- ♦ [sc policy](#)
- ♦ [sc stats](#)
- ♦ [sc parameter](#)

SC

stat sc

Synopsis

stat sc [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-clearstats (basic | full)]

Description

Displays SureConnect statistics.

Parameters

clearstats

Clear the statistics / counters Possible values: basic, full

sc policy

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#) | [stat](#)]

add sc policy

Synopsis

```
add sc policy <name> [-url <URL> | -rule <expression>] [-delay <usecs>] [-maxConn
<positive_integer>] [-action <action> (<altContentSvcName> <altContentPath>)]
```

Description

Creates a new SureConnect policy.

Parameters

name

Name for the policy. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

url

URL against which to match incoming client request.

rule

Expression against which the traffic is evaluated. Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>". The following requirements apply only to the NetScaler CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

delay

Delay threshold, in microseconds, for requests that match the policy's URL or rule. If the delay statistics gathered for the matching request exceed the specified delay, SureConnect is triggered for that request. Minimum value: 1 Maximum value: 599999999

maxConn

Maximum number of concurrent connections that can be open for requests that match the policy's URL or rule. Minimum value: 1 Maximum value: 4294967294

action

Action to be taken when the delay or maximum-connections threshold is reached. Available settings function as follows: ACS - Serve content from an alternative content service. NS - Serve alternative content from the NetScaler appliance. NO ACTION - Serve no alternative content. However, delay statistics are still collected for the configured URLs, and, if the Maximum Client Connections parameter is set, the number of connections is limited to the value specified by that parameter. (However, alternative content is not served even if the maxConn threshold is met). Possible values: ACS, NS, NOACTION

altContentSvcName

Name of the alternative content service to be used in the ACS action.

altContentPath

Path to the alternative content service to be used in the ACS action.

Example

```
add sc policy scpol_ns -delay 1000000 -url /
delay.asp -action NS

add policy expression exp_acs "url == /mc_acs.asp"
add service svc_acs 10.110.100.253 http 80
add scpolicy scpol_acs -maxconn 10 -rule exp_acs -
action ACS svc_acs /altcont.htm
```

[Top](#)

rm sc policy

Synopsis

rm sc policy <name>

Description

Removes the specified SureConnect policy.

Parameters

name

Name of the policy to be removed.

Example

```
rm sc policy scpol_ns
rm sc policy scpol_acs
```

[Top](#)

set sc policy

Synopsis

set sc policy <name> [-url <URL> | -rule <expression>] [-delay <usecs>] [-maxConn <positive_integer>] [-action <action> (<altContentSvcName> <altContentPath>)]

Description

Modifies the specified settings of a SureConnect policy.

Parameters

name

Name of the policy to be modified.

url

URL against which to match requests. URLs take precedence over rules in SureConnect policies.

rule

Expression against which the traffic is evaluated. Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>". The following requirements apply only to the NetScaler CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

delay

Delay threshold, in microseconds, for requests that match the policy's URL or rule. If the delay statistics gathered for the matching request exceed the specified delay, SureConnect is triggered for that request. Minimum value: 1 Maximum value: 599999999

maxConn

Maximum number of concurrent connections that can be open for the configured URL or rule. Minimum value: 1 Maximum value: 4294967294

action

Action to be taken when the delay or maximum-connections threshold is reached. Available settings function as follows: ACS - Serve content from an alternative content service. NS - Serve alternative content from the NetScaler appliance. NO ACTION - Serve no alternative content. However, delay statistics are still collected for the configured URLs, and, if the Maximum Client Connections parameter is set, the number of connections is limited to the value specified by that parameter. (However, alternative content is not served even if the maxConn threshold is met). Possible values: ACS, NS, NOACTION

Example

```
set sc policy scpol_ns -delay 2000000
set sc policy scpol_acs -maxconn 100
```

[Top](#)**unset sc policy****Synopsis**

```
unset sc policy <name> [-delay] [-maxConn]
```

Description

Use this command to remove sc policy settings. Refer to the set sc policy command for meanings of the arguments.

[Top](#)

show sc policy

Synopsis

show sc policy [<name>]

Description

Displays information about the SureConnect policies.

Parameters

name

Name of a policy about which to display detailed information. To display information about all the SureConnect policies, do not set this parameter.

Example

```
> show sc policy
    2 monitored Sure Connect Policies:
1)   Name: scpol_ns
     RULE: expl
     Delay: 1000000 microsecs
     Alternate Content from NS
2)   Name: scpol_acs
     RULE: exp_acs
     Max Conn: 10
     Alternate Content from ACS,
svc_acs      /delay/alcont.htm
Done
```

[Top](#)

stat sc policy

Synopsis

stat sc policy [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-clearstats (basic | full)]

Description

Displays statistics about SureConnect policies.

Parameters

name

Name of the policy about which to display statistics. To display statistics about all SureConnect policies, do not set this parameter.

clearstats

Clear the statistics / counters Possible values: basic, full

[Top](#)

sc stats

show sc stats**Synopsis**

show sc stats - alias for 'stat sc'

Description

show sc stats is an alias for stat sc

sc parameter

[[set](#) | [unset](#) | [show](#)]

set sc parameter**Synopsis**

set sc parameter [-sessionLife <secs>] [-vsr <input_filename>]

Description

Sets the parameters for displaying SureConnect information.

Parameters**sessionLife**

Time, in seconds, between the first time and the next time the SureConnect alternative content window is displayed. The alternative content window is displayed only once during a session for the same browser accessing a configured URL, so this parameter determines the length of a session. Default value: 300 Minimum value: 1 Maximum value: 4294967294

vsr

File containing the customized response to be displayed when the ACTION in the SureConnect policy is set to NS. Default value: "DEFAULT"

Example

```
set sc parameter -sessionlife 200 -vsr /etc/vsr.htm
```

[Top](#)

unset sc parameter

Synopsis

unset sc parameter [-sessionLife] [-vsr]

Description

Use this command to remove sc parameter settings. Refer to the set sc parameter command for meanings of the arguments.

[Top](#)

show sc parameter

Synopsis

show sc parameter

Description

Displays the values of the session life and vsr filename parameters.

Example

```
> show sc parameter
  Sure Connect Parameters:
  Sessionlife: 300
  Vsr: DEFAULT
Done
```

[Top](#)

SNMP Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [snmp](#)
- ♦ [snmp community](#)
- ♦ [snmp manager](#)
- ♦ [snmp trap](#)
- ♦ [snmp group](#)
- ♦ [snmp view](#)
- ♦ [snmp user](#)
- ♦ [snmp oid](#)
- ♦ [snmp stats](#)
- ♦ [snmp alarm](#)

- ♦ [snmp mib](#)
- ♦ [snmp engineId](#)
- ♦ [snmp option](#)

snmp

stat snmp

Synopsis

```
stat snmp [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile
<input_filename>] [-clearstats ( basic | full )]
```

Description

Display the statistics related to SNMP.

Parameters

clearstats

Clear the statistics / counters Possible values: basic, full

Example

```
stat snmp
```

snmp community

[[add](#) | [rm](#) | [show](#)]

add snmp community

Synopsis

```
add snmp community <communityName> <permissions>
```

Description

Creates an SNMP community, which is a password (string) used to authenticate SNMP queries from SNMP managers. You can associate it with any of the following SNMP query types: GET, GET NEXT, ALL, GET BULK. You can associate one or more community strings with each query type. For example, if you associate two community strings, such as Example and Test, with the query type GET NEXT, the NetScaler appliance considers only those GET NEXT SNMP query packets that contain Example or Test as the community string.

Parameters

communityName

The SNMP community string. Can consist of 1 to 31 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), space (), at sign (@), equals (=), colon (:), and underscore (_) characters. The following requirement applies only to the NetScaler CLI: If the string includes one or more

spaces, enclose the name in double or single quotation marks (for example, "my string" or 'my string').

permissions

The SNMP V1 or V2 query-type privilege that you want to associate with this SNMP community. Possible values: GET, GET_NEXT, GET_BULK, SET, ALL

Example

```
add snmp community public ALL
add snmp community a#12ab GET_BULK
```

[Top](#)

rm snmp community

Synopsis

rm snmp community <communityName>

Description

Removes an SNMP community from the NetScaler appliance. After you remove the SNMP community, the appliance does not respond to any SNMP queries that contain that community string.

Parameters

communityName

The name of the SNMP community.

Example

```
rm snmp community public
```

[Top](#)

show snmp community

Synopsis

show snmp community [<communityName>]

Description

Displays the SNMP v1 or v2 query-type privileges (such as GET, GET NEXT, ALL, or GET BULK) that have been set for all SNMP communities or for the specified SNMP community. To display the settings of all the SNMP communities, run the command without any parameters. To display the settings of a particular SNMP community, specify the name of the SNMP community.

Parameters

communityName

The name of the SNMP community whose SNMP v1 or v2 query type privilege setting, such as GET, GET NEXT, ALL, or GET BULK, you want the NetScaler appliance to display.

Example

```
show snmp community
```

[Top](#)

snmp manager

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add snmp manager

Synopsis

add snmp manager <IPAddress> ... [-netmask <netmask>] [-domainResolveRetry <integer>]

Description

Specifies an SNMP manager to query the NetScaler appliance. The added manager complies with SNMP V1, V2, and V3. If you specify one or more SNMP managers, the appliance does not accept SNMP queries from any hosts except the specified SNMP managers. You can specify up to a maximum of 100 IP based SNMP managers or networks and a maximum of 5 host-name based SNMP managers.

Parameters

IPAddress

IP address of the SNMP manager. Can be an IPv4 or IPv6 address. You can instead specify an IPv4 network address or IPv6 network prefix if you want the NetScaler appliance to respond to SNMP queries from any device on the specified network. Alternatively, instead of an IPv4 address, you can specify a host name that has been assigned to an SNMP manager. If you do so, you must add a DNS name server that resolves the host name of the SNMP manager to its IP address. Note: The NetScaler appliance does not support host names for SNMP managers that have IPv6 addresses.

netmask

Subnet mask associated with an IPv4 network address. If the IP address specifies the address or host name of a specific host, accept the default value of 255.255.255.255. Default value: 0xFFFFFFFF

domainResolveRetry

Amount of time, in seconds, for which the NetScaler appliance waits before sending another DNS query to resolve the host name of the SNMP manager if the last query failed. This parameter is valid for host-name based SNMP managers only. After a

query succeeds, the TTL determines the wait time. Minimum value: 5 Maximum value: 20939

Example

```
add snmp manager 192.168.1.20 192.168.2.42
add snmp manager 192.168.2.16 -netmask
255.255.255.240
add snmp manager hostnamemanager.com
```

[Top](#)

rm snmp manager

Synopsis

```
rm snmp manager <IPAddress> ... [-netmask <netmask>]
```

Description

Removes an SNMP manager from the list of managers that are allowed to access the NetScaler appliance.

Parameters

IPAddress

IPv4 or IPv6 address (or IPv4 host name) of the SNMP manager, or the IPv4 network address or IPv6 network prefix of the SNMP managers.

netmask

Subnet mask associated with an IPv4 SNMP manager entry. For a specific host, the subnet mask is 255.255.255.255. Default value: 0xFFFFFFFF

Example

```
rm snmp manager 192.168.1.20
rm snmp manager 192.168.2.16 -netmask
255.255.255.240
rm snmp manager hostnamemanager.com
```

[Top](#)

set snmp manager

Synopsis

```
set snmp manager <IPAddress> [-netmask <netmask>] [-domainResolveRetry <integer>]
```

Description

Modifies the Domain Resolve Retry parameter of any host-name based SNMP manager configured on the NetScaler appliance.

Parameters

IPAddress

Host name of the SNMP manager for which you want to modify the Domain Resolve Retry parameter.

netmask

Subnet mask associated with an IPv4 network address. If the IP address specifies the address or host name of a specific host, accept the default value of 255.255.255.255. Default value: 0xFFFFFFFF

domainResolveRetry

Amount of time, in seconds, for which the NetScaler appliance waits before sending another DNS query to resolve the host name of the SNMP manager if the last query failed. This parameter is valid for host-name based SNMP managers only. After a query succeeds, the TTL determines the wait time. Minimum value: 5 Maximum value: 20939

Example

```
set snmp manager www.example.com -  
domainResolveRetry 7
```

[Top](#)

unset snmp manager

Synopsis

```
unset snmp manager <IPAddress> -netmask <netmask> -domainResolveRetry
```

Description

Use this command to remove snmp manager settings. Refer to the set snmp manager command for meanings of the arguments.

[Top](#)

show snmp manager

Synopsis

```
show snmp manager [<IPAddress> [-netmask <netmask>]]
```

Description

Displays configuration information about all SNMP managers on the NetScaler appliance, or detailed information about the specified manager.

Parameters

IPAddress

IPv4 or IPv6 address (or IPv4 host name) of the SNMP manager, or the IPv4 network address or IPv6 network prefix of the SNMP managers, about which to display information.

Example

```
show snmp manager
```

[Top](#)

snmp trap

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add snmp trap

Synopsis

```
add snmp trap <trapClass> <trapDestination> ... [-version ( V1 | V2 )] [-destPort <port>]
[-communityName <string>] [-srcIP <ip_addr|ipv6_addr>] [-severity <severity>]
```

Description

Adds an SNMP trap listener. You can configure the NetScaler appliance to generate asynchronous events (trap messages) to report abnormal conditions. The trap messages are sent to a remote device (trap listener) to help administrators monitor the appliance and respond promptly to any issues.

Parameters

trapClass

Type of trap messages that the NetScaler appliance sends to the trap listener: Generic or the enterprise-specific messages defined in the MIB file. Possible values: generic, specific

trapDestination

IPv4 or the IPv6 address of the trap listener to which the NetScaler appliance is to send SNMP trap messages.

version

SNMP version, which determines the format of trap messages sent to the trap listener. This setting must match the setting on the trap listener. Otherwise, the listener drops the trap messages. Possible values: V1, V2 Default value: TRAP_VERSION_2

destPort

UDP port at which the trap listener listens for trap messages. This setting must match the setting on the trap listener. Otherwise, the listener drops the trap messages. Default value: 162 Minimum value: 1 Maximum value: 65534

communityName

Password (string) sent with the trap messages, so that the trap listener can authenticate them. Can include 1 to 31 uppercase or lowercase letters, numbers, and hyphen (-), period (.) pound (#), space (), at (@), equals (=), colon (:), and underscore (_) characters. You must specify the same community string on the trap listener device. Otherwise, the trap listener drops the trap messages. The following requirement applies only to the NetScaler CLI: If the string includes one or more

spaces, enclose the name in double or single quotation marks (for example, "my string" or 'my string'). Default value: "public"

srcIP

IPv4 or IPv6 address that the NetScaler appliance inserts as the source IP address in all SNMP trap messages that it sends to this trap listener. By default this is the appliance's NSIP or NSIP6 address, but you can specify an IPv4 MIP or SNIP address or a SNIP6 address.

severity

Severity level at or above which the NetScaler appliance sends trap messages to this trap listener. The severity levels, in increasing order of severity, are Informational, Warning, Minor, Major, Critical. This parameter can be set for trap listeners of type SPECIFIC only. The default is to send all levels of trap messages. Important: Trap messages are not assigned severity levels unless you specify severity levels when configuring SNMP alarms. Possible values: Critical, Major, Minor, Warning, Informational Default value: SNMP_SEV_UNKNOWN

[Top](#)

rm snmp trap**Synopsis**

```
rm snmp trap <trapClass> <trapDestination> ...
```

Description

Removes a trap listener entry from the NetScaler appliance.

Parameters**trapClass**

Trap type specified in the trap listener entry that you want to remove. Possible values: generic, specific

trapDestination

IP address of the trap listener specified in the trap listener entry that you want to remove.

[Top](#)

set snmp trap**Synopsis**

```
set snmp trap <trapClass> <trapDestination> [-destPort <port>] [-version ( V1 | V2 )] [-communityName <string>] [-srcIP <ip_addr|ipv6_addr>] [-severity <severity>]
```

Description

Modifies the specified parameters in a trap-listener entry.

Parameters

trapClass

Type of trap specified in the trap-listener entry. Because this parameter is used for identifying the trap listener entry, it cannot be modified after the entry has been created. Possible values: generic, specific

trapDestination

IPv4 or the IPv6 address of the trap listener to which the NetScaler appliance is to send SNMP trap messages.

destPort

UDP port at which the trap listener listens for trap messages. This setting must match the setting on the trap listener. Otherwise, the listener drops the trap messages. Default value: 162 Minimum value: 1 Maximum value: 65534

version

SNMP version, which determines the format of trap messages sent to the trap listener. This setting must match the setting on the trap listener. Otherwise, the listener drops the trap messages. Possible values: V1, V2 Default value: TRAP_VERSION_2

communityName

Password (string) sent with the trap messages, so that the trap listener can authenticate them. Can include 1 to 31 uppercase or lowercase letters, numbers, and hyphen (-), period (.) pound (#), space (), at (@), equals (=), colon (:), and underscore (_) characters. You must specify the same community string on the trap listener device. Otherwise, the trap listener drops the trap messages. The following requirement applies only to the NetScaler CLI: If the string includes one or more spaces, enclose the name in double or single quotation marks (for example, "my string" or 'my string'). Default value: "public"

srcIP

IPv4 or IPv6 address that the NetScaler appliance inserts as the source IP address in all SNMP trap messages that it sends to this trap listener. By default this is the appliance's NSIP or NSIP6 address, but you can specify an IPv4 MIP or SNIP address or a SNIP6 address.

severity

Severity level at or above which the NetScaler appliance sends trap messages to this trap listener. The severity levels, in increasing order of severity, are Informational, Warning, Minor, Major, Critical. This parameter can be set for trap listeners of type SPECIFIC only. The default is to send all levels of trap messages. Important: Trap messages are not assigned severity levels unless you specify severity levels when configuring SNMP alarms. Possible values: Critical, Major, Minor, Warning, Informational Default value: SNMP_SEV_UNKNOWN

Example

```
set snmp trap generic 192.168.3.4 -version V1
```

[Top](#)

unset snmp trap

Synopsis

```
unset snmp trap <trapClass> <trapDestination> [-destPort] [-version] [-communityName] [-srcIP] [-severity]
```

Description

Resets the specified parameters to their default settings in a trap-listener entry. Refer to the set snmp trap command for meanings of the arguments.

Example

```
unset snmp trap generic 192.168.3.4 -version
```

[Top](#)

show snmp trap

Synopsis

```
show snmp trap [<trapClass> <trapDestination>]
```

Description

Displays the settings of all trap listeners or of the specified trap listener. To display the settings of all the trap listeners, run the command without any parameters. To display the settings of a particular trap listener, specify the trapClass (Trap Type) and trapDestination (IP Address) of the trap listener.

Parameters

trapClass

Trap type specified in the trap listener entry. Possible values: generic, specific

Example

```
show snmp trap
```

[Top](#)

snmp group

[[add](#) | [rm](#) | [set](#) | [show](#)]

add snmp group

Synopsis

```
add snmp group <name> <securityLevel> -readViewName <string>
```

Description

Adds an SNMPv3 user group on the NetScaler appliance. SNMPv3 groups are logical aggregations of SNMPv3 users. SNMPv3 groups are used to implement access control and define the security levels for the users. You can add a maximum of 1000 SNMPv3 groups to the NetScaler appliance.

Parameters

name

Name for the SNMPv3 group. Can consist of 1 to 31 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), space (), at sign (@), equals (=), colon (:), and underscore (_) characters. You should choose a name that helps identify the SNMPv3 group. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose it in double or single quotation marks (for example, "my name" or 'my name').

securityLevel

Security level required for communication between the NetScaler appliance and the SNMPv3 users who belong to the group. Specify one of the following options: noAuthNoPriv. Require neither authentication nor encryption. authNoPriv. Require authentication but no encryption. authPriv. Require authentication and encryption. Note: If you specify authentication, you must specify an encryption algorithm when you assign an SNMPv3 user to the group. If you also specify encryption, you must assign both an authentication and an encryption algorithm for each group member. Possible values: noAuthNoPriv, authNoPriv, authPriv

readViewName

Name of the configured SNMPv3 view that you want to bind to this SNMPv3 group. An SNMPv3 user bound to this group can access the subtrees that are bound to this SNMPv3 view as type INCLUDED, but cannot access the ones that are type EXCLUDED. If the NetScaler appliance has multiple SNMPv3 view entries with the same name, all such entries are associated with the SNMPv3 group.

[Top](#)

rm snmp group

Synopsis

```
rm snmp group <name> <securityLevel>
```

Description

Removes an SNMPv3 group entry from the NetScaler appliance. The appliance can have multiple SNMPv3 groups with the same name, differentiated by the securityLevel (Security level) parameter setting. Therefore, to identify an SNMPv3 group entry that you want to remove, you have to specify both the name and security level of the SNMPv3 group.

Parameters

name

Name of the SNMPv3 group.

securityLevel

Security level of the SNMPv3 group. Possible values: noAuthNoPriv, authNoPriv, authPriv

[Top](#)

set snmp group**Synopsis**

```
set snmp group <name> <securityLevel> -readViewName <string>
```

Description

Modifies the specified parameters of an SNMPv3 group entry on the NetScaler appliance.

Parameters**name**

The name specified in the SNMPv3 group entry that you want to modify. This parameter cannot be modified.

securityLevel

Security level required for communication between the NetScaler appliance and the SNMPv3 users who belong to the group. Specify one of the following options: noAuthNoPriv. Require neither authentication nor encryption. authNoPriv. Require authentication but no encryption. authPriv. Require authentication and encryption. Note: If you specify authentication, you must specify an encryption algorithm when you assign an SNMPv3 user to the group. If you also specify encryption, you must assign both an authentication and an encryption algorithm for each group member. Possible values: noAuthNoPriv, authNoPriv, authPriv

readViewName

Name of the configured SNMPv3 view that you want to bind to this SNMPv3 group. An SNMPv3 user bound to this group can access the subtrees that are bound to this SNMPv3 view as type INCLUDED, but cannot access the ones that are type EXCLUDED. If the NetScaler appliance has multiple SNMPv3 view entries with the same name, all such entries are associated with the SNMPv3 group.

[Top](#)

show snmp group**Synopsis**

```
show snmp group [<name> <securityLevel>]
```

Description

Displays the settings of all SNMPv3 groups or of the specified SNMPv3 group. To display the settings of all SNMPv3 groups, run the command without any parameters. To display the settings of a particular SNMPv3 group, specify the name of the SNMPv3 group and securityLevel (Security level). The NetScaler appliance can have multiple SNMPv3 groups with the same name, differentiated by the securityLevel (Security level) parameter setting.

Parameters

name

Name of the SNMPv3 group whose details you want the NetScaler appliance to display.

securityLevel

Security level of the SNMPv3 group whose details you want the NetScaler appliance to display. Possible values: noAuthNoPriv, authNoPriv, authPriv

[Top](#)

snmp view

[[add](#) | [rm](#) | [set](#) | [show](#)]

add snmp view

Synopsis

add snmp view <name> <subtree> -type (included | excluded)

Description

Adds an SNMPv3 view. Used to implement access control for the SNMPv3 user, SNMPv3 views restrict user access to specific portions of the MIB. The NetScaler appliance can have multiple SNMPv3 views with the same name, differentiated by subtree parameter settings. You can add a maximum of 1000 SNMPv3 views.

Parameters

name

Name for the SNMPv3 view. Can consist of 1 to 31 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), space (), at sign (@), equals (=), colon (:), and underscore (_) characters. You should choose a name that helps identify the SNMPv3 view. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose it in double or single quotation marks (for example, "my view" or 'my view').

subtree

A particular branch (subtree) of the MIB tree that you want to associate with this SNMPv3 view. You must specify the subtree as an SNMP OID.

type

Include or exclude the subtree, specified by the subtree parameter, in or from this view. This setting can be useful when you have included a subtree, such as A, in an SNMPv3 view and you want to exclude a specific subtree of A, such as B, from the SNMPv3 view. Possible values: included, excluded

[Top](#)

rm snmp view

Synopsis

rm snmp view <name> <subtree>

Description

Removes an SNMPv3 view entry from the NetScaler appliance. The appliance can have multiple SNMPv3 views with the same name, differentiated by the subtree parameter setting. Therefore, to identify an SNMPv3 group subtree that you want to remove, you have to specify both the name and subtree of the SNMPv3 view.

Parameters

name

Name of the SNMPv3 view. Note: If multiple views have the same name, specify the subtree to identify the view to be removed.

subtree

A MIB subtree of the SNMPv3 view.

[Top](#)

set snmp view

Synopsis

```
set snmp view <name> <subtree> -type ( included | excluded )
```

Description

Modifies the type (Type) parameter of an SNMPv3 view configured on the NetScaler appliance.

Parameters

name

The name specified in the SNMPv3 view entry. This parameter cannot be modified.

subtree

A MIB subtree of the SNMPv3 view entry. This parameter cannot be modified.

type

Include or exclude the subtree, specified by the subtree parameter, in or from this view. This setting can be useful when you have included a subtree, such as A, in an SNMPv3 view and you want to exclude a specific subtree of A, such as B, from the SNMPv3 view. Possible values: included, excluded

[Top](#)

show snmp view

Synopsis

```
show snmp view [<name> [<subtree>]]
```

Description

Displays the settings of all SNMPv3 views or of the specified SNMPv3 view. To display the settings of all the SNMPv3 views, run the command without any parameters. To display the settings of a particular SNMPv3 view, specify the name of the SNMPv3 view and subtree (the associated subtree of the MIB). The NetScaler appliance can have

multiple SNMPv3 views with the same name, differentiated by the subtree parameter settings.

Parameters

name

Name of the SNMPv3 view.

[Top](#)

snmp user

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add snmp user

Synopsis

```
add snmp user <name> -group <string> [-authType ( MD5 | SHA ) {-authPasswd } [-privType ( DES | AES ) {-privPasswd }]]
```

Description

Adds an SNMPv3 user who can send SNMP queries to the NetScaler appliance. You can add a maximum of 1000 SNMPv3 users.

Parameters

name

Name for the SNMPv3 user. Can consist of 1 to 31 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), space (), at sign (@), equals (=), colon (:), and underscore (_) characters. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose it in double or single quotation marks (for example, "my user" or 'my user').

group

Name of the configured SNMPv3 group to which to bind this SNMPv3 user. The access rights (bound SNMPv3 views) and security level set for this group are assigned to this user.

authType

Authentication algorithm used by the NetScaler appliance and the SNMPv3 user for authenticating the communication between them. You must specify the same authentication algorithm when you configure the SNMPv3 user in the SNMP manager. Possible values: MD5, SHA

privType

Encryption algorithm used by the NetScaler appliance and the SNMPv3 user for encrypting the communication between them. You must specify the same encryption algorithm when you configure the SNMPv3 user in the SNMP manager. Possible values: DES, AES

[Top](#)

rm snmp user

Synopsis

rm snmp user <name>

Description

Removes an SNMPv3 user entry from the NetScaler appliance.

Parameters

name

Name of the SNMPv3 user.

[Top](#)

set snmp user

Synopsis

set snmp user <name> [-group <string>] [-authType (MD5 | SHA) {-authPasswd }}] [-privType (DES | AES) {-privPasswd }}]

Description

Modifies the specified parameters of an SNMPv3 user entry on the NetScaler appliance.

Parameters

name

Name specified in the SNMPv3 user entry that you want to modify. Because this parameter is used for identifying the SNMPv3 user entry, it cannot be modified after the entry has been created.

group

Name of the configured SNMPv3 group to which to bind this SNMPv3 user. The access rights (bound SNMPv3 views) and security level set for this group are assigned to this user.

authType

Authentication algorithm used by the NetScaler appliance and the SNMPv3 user for authenticating the communication between them. You must specify the same authentication algorithm when you configure the SNMPv3 user in the SNMP manager. Possible values: MD5, SHA

privType

Encryption algorithm used by the NetScaler appliance and the SNMPv3 user for encrypting the communication between them. You must specify the same encryption algorithm when you configure the SNMPv3 user in the SNMP manager. Possible values: DES, AES

[Top](#)

unset snmp user

Synopsis

unset snmp user <name> (-authType | -privType) [-authPasswd] [-privPasswd]

Description

Resets the specified parameters of an SNMPv3 user entry to their default settings..Refer to the set snmp user command for meanings of the arguments.

[Top](#)

show snmp user

Synopsis

show snmp user [<name>]

Description

Displays the settings of all SNMPv3 users or of the specified SNMPv3 user. To display the settings of all the SNMPv3 users, run the command without any parameters. To display the settings of a particular SNMPv3 user, specify the name of the SNMPv3 user.

Parameters

name

Name of the SNMPv3 user whose details you want the NetScaler appliance to display.

[Top](#)

snmp oid

show snmp oid

Synopsis

show snmp oid <entityType> [<name>]

Description

Displays the corresponding SNMP OIDs for the virtual servers, services, and service groups configured on the NetScaler appliance. To display the SNMP OID of all entities of a particular type, such as virtual servers, run the command with only that entity type specified. To display the SNMP of a particular entity, specify the entity type and the entity name.

Parameters

entityType

The type of entity whose SNMP OIDs you want to displayType of entity whose SNMP OIDs you want the NetScaler appliance to display. Possible values: VSERVER, SERVICE, SERVICEGROUP

name

Name of the entity whose SNMP OID you want the NetScaler appliance to display.

Example

```
show snmp oid VSERVER vs1
```

snmp stats

show snmp stats

Synopsis

show snmp stats - alias for 'stat snmp'

Description

show snmp stats is an alias for stat snmp Displays the statistics related to SNMP.

snmp alarm

[[set](#) | [unset](#) | [enable](#) | [disable](#) | [show](#)]

set snmp alarm

Synopsis

set snmp alarm <trapName> [-thresholdValue <positive_integer> [-normalValue <positive_integer>]] [-time <secs>] [-state <state>] [-severity <severity>] [-logging (ENABLED | DISABLED)]

Description

Configures an SNMP alarm. You must enable and configure alarms to generate enterprise-specific trap messages. The NetScaler appliance sends these trap messages only to trap listeners of type (class) SPECIFIC. The SNMP alarms are either event based or threshold based. The NetScaler appliance supports the following user configurable alarms: HA-STATE-CHANGE: Change to primary/secondary CPU-USAGE: Individual CPU usage AVERAGE-CPU: Average CPU usage MGMT-CPU: Management CPU usage ENTITY-STATE: Entity state change SYNFLOOD: Global unacknowledged SYN count MEMORY: Memory usage VSERVER-REQRATE: Vserver specific request rate SERVICE-REQRATE: Service specific request rate ENTITY-RXRATE: Entity specific Rx bytes per sec ENTITY-TXRATE: Entity specific Tx bytes per sec ENTITY-SYNFLOOD: Entity specific unacknowledged SYN count CONFIG-CHANGE: System configuration changed SERVICE-MAXCLIENTS: Service hit max-client limit CONFIG-SAVE: System configuration was saved SERVICEGROUP-MEMBER-REQRATE: Request rate on a service group member SERVICEGROUP-MEMBER-MAXCLIENTS: Service group member hits max-client MONITOR-RTO-THRESHOLD: Monitor probe response timeout LOGIN-FAILURE: GUI/CLI/API login failure SSL-CERT-EXPIRY: Certificate expiry FAN-SPEED-LOW: Low fan speed VOLTAGE-LOW: Low voltage VOLTAGE-HIGH: High Voltage TEMPERATURE-HIGH: High temperature CPU-TEMPERATURE-HIGH: High CPU temperature POWER-SUPPLY-FAILURE: Power supply failure DISK-USAGE-HIGH: High disk usage INTERFACE-THROUGHPUT-LOW: Low Interface throughput MON_PROBE_FAILED: Monitor probe failure HA-VERSION-MISMATCH: HA netscaler's OS version mismatch HA-SYNC-FAILURE: HA config synchronization failure

HA-NO-HEARTBEATS: No HA hearbeats HA-BAD-SECONDARY-STATE: Secondary state DOWN/UNKNOWN/STAY SECONDARY INTERFACE-BW-USAGE: System aggregate BW usage RATE-LIMIT-THRESHOLD-EXCEEDED: Client exceed rate-limit threshold ENTITY-NAME-CHANGE: Entity name change HA-PROP-FAILURE: HA config propagation failure IP-CONFLICT: IP conflict PF-RL-RATE-THRESHOLD: Platform rate limit in Mbps PF-RL-PPS-THRESHOLD: Platform packets per second limit PF-RL-RATE-PKTS-DROPPED: Packet Drops due to platform rate limit PF-RL-PPS-PKTS-DROPPED: Packet Drops due to platform packet per sec limit APPFW-START-URL: AppFirewall Start URL violation APPFW-DENY-URL: AppFirewall Deny URL violation APPFW-REFERER-HEADER: AppFirewall Referer Header violation APPFW-CSRF-TAG: AppFirewall CSRF Tag violation APPFW-COOKIE: AppFirewall Cookie violation APPFW-FIELD-CONSISTENCY: AppFirewall Field Consistency violation APPFW-BUFFER-OVERFLOW: AppFirewall Buffer Overflow violation APPFW-FIELD-FORMAT: AppFirewall Field Format violation APPFW-SAFE-COMMERCE: AppFirewall Safe Commerce violation APPFW-SAFE-OBJECT: AppFirewall Safe Object violation APPFW-POLICY-HIT: AppFirewall Policy Hit APPFW-VIOLATIONS-TYPE: AppFirewall Content Type violation APPFW-XSS: AppFirewall Cross Site Scripting violation APPFW-XML-XSS: AppFirewall XML Cross Site Scripting violation APPFW-SQL: AppFirewall SQL violation APPFW-XML-SQL: AppFirewall XML SQL violation APPFW-XML-ATTACHMENT: AppFirewall XML Attachment violation APPFW-XML-DOS: AppFirewall XML DoS violation APPFW-XML-VALIDATION: AppFirewall XML Validation violation APPFW-XML-WSI: AppFirewall XML WSI violation APPFW-XML-SCHEMA-COMPILE: AppFirewall XML Schema Compile violation APPFW-XML-SOAP-FAULT: AppFirewall XML Soap Fault violation DNSKEY-EXPIRY: DNSKEY expiry DATASTREAM-RATE-LIMIT-HIT: DataStream Rate Limit Hit HA-LICENSE-MISMATCH: HA netscaler's license mismatch SSL-CARD-FAILED: SSL Card Failed SSL-CARD-NORMAL: SSL Card Normal WARM-RESTART-EVENT: Warm Restart Event Occurred HARD-DISK-DRIVE-ERRORS: Hard Disk Drive Errors COMPACT-FLASH-ERRORS: Compact Flash Errors CALLHOME-UPLOAD-EVENT: Attempt to upload Show Tech Support Archive 1024KEY-EXCHANGE-RATE: 1024 Key Exchange Rate 2048KEY-EXCHANGE-RATE: 2048 Key Exchange Rate 4096KEY-EXCHANGE-RATE: 4096 Key Exchange Rate SSL-CUR-SESSION-INUSE: SSL Current Sessions In Use CLUSTER-NODE-HEALTH: Cluster Node Health State Change CLUSTER-NODE-QUORUM: Cluster Node View has Quorum CLUSTER-VERSION-MISMATCH: Cluster Node Version Mismatch CLUSTER-CCO-CHANGE: Cluster Configuration Coordinator Change CLUSTER-OVS-CHANGE: Cluster Operational View Set Change CLUSTER-SYNC-FAILURE: Cluster Config Synchronization Failure CLUSTER-PROP-FAILURE: Cluster Config Propagation Failure HA-STICKY-PRIMARY: Fixed primary state owing to max HA flips INBAND-PROTOCOL-VERSION-MISMATCH: Inband protocol mismatch between BR and QoSd SSL-CHIP-REINIT: SSL Chip Reinit VRID-STATE-CHANGE: VRID State Change For the purposes of this command, entity includes vservers and services.

Parameters

trapName

Name of the SNMP alarm. This parameter is required for identifying the SNMP alarm and cannot be modified. Possible values: CPU-USAGE, AVERAGE-CPU, MEMORY, MGMT-CPU-USAGE, SYNFLOOD, VSERVER-REQRATE, SERVICE-REQRATE, ENTITY-RXRATE, ENTITY-TXRATE, ENTITY-SYNFLOOD, SERVICE-MAXCLIENTS, HA-STATE-CHANGE, ENTITY-STATE, CONFIG-CHANGE, CONFIG-SAVE, SERVICEGROUP-MEMBER-REQRATE, SERVICEGROUP-MEMBER-MAXCLIENTS, MONITOR-RTO-THRESHOLD, LOGIN-FAILURE, SSL-CERT-EXPIRY, FAN-SPEED-LOW, VOLTAGE-LOW, VOLTAGE-HIGH, TEMPERATURE-HIGH, CPU-TEMPERATURE-HIGH, POWER-SUPPLY-FAILURE, DISK-USAGE-HIGH, INTERFACE-THROUGHPUT-LOW, MON_PROBE_FAILED, HA-VERSION-MISMATCH, HA-

SYNC-FAILURE, HA-NO-HEARTBEATS, HA-BAD-SECONDARY-STATE, INTERFACE-BW-USAGE, RATE-LIMIT-THRESHOLD-EXCEEDED, ENTITY-NAME-CHANGE, HA-PROP-FAILURE, IP-CONFLICT, PF-RL-RATE-THRESHOLD, PF-RL-PPS-THRESHOLD, PF-RL-RATE-PKTS-DROPPED, PF-RL-PPS-PKTS-DROPPED, APPFW-START-URL, APPFW-DENY-URL, APPFW-VIOLATIONS-TYPE, APPFW-REFERER-HEADER, APPFW-CSRF-TAG, APPFW-COOKIE, APPFW-FIELD-CONSISTENCY, APPFW-BUFFER-OVERFLOW, APPFW-FIELD-FORMAT, APPFW-SAFE-COMMERCE, APPFW-SAFE-OBJECT, APPFW-POLICY-HIT, APPFW-XSS, APPFW-XML-XSS, APPFW-SQL, APPFW-XML-SQL, APPFW-XML-ATTACHMENT, APPFW-XML-DOS, APPFW-XML-VALIDATION, APPFW-XML-WSI, APPFW-XML-SCHEMA-COMPILE, APPFW-XML-SOAP-FAULT, DNSKEY-EXPIRY, DATASTREAM-RATE-LIMIT-HIT, HA-LICENSE-MISMATCH, SSL-CARD-FAILED, SSL-CARD-NORMAL, WARM-RESTART-EVENT, HARD-DISK-DRIVE-ERRORS, COMPACT-FLASH-ERRORS, CALLHOME-UPLOAD-EVENT, 1024KEY-EXCHANGE-RATE, 2048KEY-EXCHANGE-RATE, 4096KEY-EXCHANGE-RATE, SSL-CUR-SESSION-INUSE, CLUSTER-NODE-HEALTH, CLUSTER-NODE-QUORUM, CLUSTER-VERSION-MISMATCH, CLUSTER-CCO-CHANGE, CLUSTER-OVS-CHANGE, CLUSTER-SYNC-FAILURE, CLUSTER-PROP-FAILURE, HA-STICKY-PRIMARY, INBAND-PROTOCOL-VERSION-MISMATCH, SSL-CHIP-REINIT, VRID-STATE-CHANGE

thresholdValue

Value for the high threshold. The NetScaler appliance generates an SNMP trap message when the value of the attribute associated with the alarm is greater than or equal to the specified high threshold value. Minimum value: 1

time

Interval, in seconds, at which the NetScaler appliance generates SNMP trap messages when the conditions specified in the SNMP alarm are met. Can be specified for the following alarms: SYNFLOOD, HA-VERSION-MISMATCH, HA-SYNC-FAILURE, HA-NO-HEARTBEATS, HA-BAD-SECONDARY-STATE, HA-PROP-FAILURE, IP-CONFLICT, and APPFW. Default value: 1

state

Current state of the SNMP alarm. The NetScaler appliance generates trap messages only for SNMP alarms that are enabled. Some alarms are enabled by default, but you can disable them. Possible values: ENABLED, DISABLED, UNSET Default value: ENABLED

severity

Severity level assigned to trap messages generated by this alarm. The severity levels are, in increasing order of severity, Informational, Warning, Minor, Major, and Critical. This parameter is useful when you want the NetScaler appliance to send trap messages to a trap listener on the basis of severity level. Trap messages with a severity level lower than the specified level (in the trap listener entry) are not sent. Possible values: Critical, Major, Minor, Warning, Informational Default value: SNMP_SEV_UNKNOWN

logging

Logging status of the alarm. When logging is enabled, the NetScaler appliance logs every trap message that is generated for this alarm. Possible values: ENABLED, DISABLED Default value: ENABLED

Example

```
set snmp alarm VSERVER-REQRATE -thresholdValue
10000 -normalValue 100
```

[Top](#)

unset snmp alarm

Synopsis

```
unset snmp alarm <trapName> [-thresholdValue] [-normalValue] [-time] [-state] [-severity] [-logging]
```

Description

Resets the specified parameters of an SNMP alarm to their default settings..Refer to the set snmp alarm command for meanings of the arguments.

Example

```
unset snmp alarm VSERVER-REQRATE
```

[Top](#)

enable snmp alarm

Synopsis

```
enable snmp alarm <trapName> ...
```

Description

Enables or disables an SNMP alarm. The NetScaler appliance looks for conditions specified in the enabled SNMP alarms. When the condition in any enabled SNMP alarm is met, the appliance generates an SNMP trap message. It does not look for conditions specified in disabled SNMP alarms and therefore does not generate an SNMP trap message when the condition in any disabled SNMP alarm is met. Some alarms are enabled by default, but you can disable them.

Parameters**trapName**

Name of the SNMP alarm. This parameter is required for identifying the SNMP alarm. Possible values: CPU-USAGE, AVERAGE-CPU, MEMORY, MGMT-CPU-USAGE, SYNFLOOD, VSERVER-REQRATE, SERVICE-REQRATE, ENTITY-RXRATE, ENTITY-TXRATE, ENTITY-SYNFLOOD, SERVICE-MAXCLIENTS, HA-STATE-CHANGE, ENTITY-STATE, CONFIG-CHANGE, CONFIG-SAVE, SERVICEGROUP-MEMBER-REQRATE, SERVICEGROUP-MEMBER-MAXCLIENTS, MONITOR-RTO-THRESHOLD, LOGIN-FAILURE, SSL-CERT-EXPIRY, FAN-SPEED-LOW, VOLTAGE-LOW, VOLTAGE-HIGH, TEMPERATURE-HIGH, CPU-TEMPERATURE-HIGH, POWER-SUPPLY-FAILURE, DISK-USAGE-HIGH, INTERFACE-THROUGHPUT-LOW, MON_PROBE_FAILED, HA-VERSION-MISMATCH, HA-SYNC-FAILURE, HA-NO-HEARTBEATS, HA-BAD-SECONDARY-STATE, INTERFACE-BW-USAGE, RATE-LIMIT-THRESHOLD-

EXCEEDED, ENTITY-NAME-CHANGE, HA-PROP-FAILURE, IP-CONFLICT, PF-RL-RATE-THRESHOLD, PF-RL-PPS-THRESHOLD, PF-RL-RATE-PKTS-DROPPED, PF-RL-PPS-PKTS-DROPPED, APPFW-START-URL, APPFW-DENY-URL, APPFW-VIOLATIONS-TYPE, APPFW-REFERER-HEADER, APPFW-CSRF-TAG, APPFW-COOKIE, APPFW-FIELD-CONSISTENCY, APPFW-BUFFER-OVERFLOW, APPFW-FIELD-FORMAT, APPFW-SAFE-COMMERCE, APPFW-SAFE-OBJECT, APPFW-POLICY-HIT, APPFW-XSS, APPFW-XML-XSS, APPFW-SQL, APPFW-XML-SQL, APPFW-XML-ATTACHMENT, APPFW-XML-DOS, APPFW-XML-VALIDATION, APPFW-XML-WSI, APPFW-XML-SCHEMA-COMPILE, APPFW-XML-SOAP-FAULT, DNSKEY-EXPIRY, DATASTREAM-RATE-LIMIT-HIT, HA-LICENSE-MISMATCH, SSL-CARD-FAILED, SSL-CARD-NORMAL, WARM-RESTART-EVENT, HARD-DISK-DRIVE-ERRORS, COMPACT-FLASH-ERRORS, CALLHOME-UPLOAD-EVENT, 1024KEY-EXCHANGE-RATE, 2048KEY-EXCHANGE-RATE, 4096KEY-EXCHANGE-RATE, SSL-CUR-SESSION-INUSE, CLUSTER-NODE-HEALTH, CLUSTER-NODE-QUORUM, CLUSTER-VERSION-MISMATCH, CLUSTER-CCO-CHANGE, CLUSTER-OVS-CHANGE, CLUSTER-SYNC-FAILURE, CLUSTER-PROP-FAILURE, HA-STICKY-PRIMARY, INBAND-PROTOCOL-VERSION-MISMATCH, SSL-CHIP-REINIT, VRID-STATE-CHANGE

Example

```
enable snmp alarm VSERVER-REQRATE
enable snmp alarm CPU SYNFLOOD
```

[Top](#)

disable snmp alarm

Synopsis

disable snmp alarm <trapName> ...

Description

Disables an SNMP alarm. The NetScaler appliance does not generate trap messages for SNMP alarms that are disabled. Some alarms are enabled by default, but you can disable them.

Parameters

trapName

Name of the SNMP alarm. This parameter is required for identifying the SNMP alarm. Possible values: CPU-USAGE, AVERAGE-CPU, MEMORY, MGMT-CPU-USAGE, SYNFLOOD, VSERVER-REQRATE, SERVICE-REQRATE, ENTITY-RXRATE, ENTITY-TXRATE, ENTITY-SYNFLOOD, SERVICE-MAXCLIENTS, HA-STATE-CHANGE, ENTITY-STATE, CONFIG-CHANGE, CONFIG-SAVE, SERVICEGROUP-MEMBER-REQRATE, SERVICEGROUP-MEMBER-MAXCLIENTS, MONITOR-RTO-THRESHOLD, LOGIN-FAILURE, SSL-CERT-EXPIRY, FAN-SPEED-LOW, VOLTAGE-LOW, VOLTAGE-HIGH, TEMPERATURE-HIGH, CPU-TEMPERATURE-HIGH, POWER-SUPPLY-FAILURE, DISK-USAGE-HIGH, INTERFACE-THROUGHPUT-LOW, MON_PROBE_FAILED, HA-VERSION-MISMATCH, HA-SYNC-FAILURE, HA-NO-HEARTBEATS, HA-BAD-SECONDARY-STATE, INTERFACE-BW-USAGE, RATE-LIMIT-THRESHOLD-EXCEEDED, ENTITY-NAME-CHANGE, HA-PROP-FAILURE, IP-CONFLICT, PF-RL-RATE-THRESHOLD, PF-RL-PPS-THRESHOLD, PF-RL-RATE-PKTS-DROPPED, PF-RL-PPS-PKTS-DROPPED, APPFW-START-URL, APPFW-DENY-URL, APPFW-VIOLATIONS-TYPE, APPFW-

REFERER-HEADER, APPFW-CSRF-TAG, APPFW-COOKIE, APPFW-FIELD-CONSISTENCY, APPFW-BUFFER-OVERFLOW, APPFW-FIELD-FORMAT, APPFW-SAFE-COMMERCE, APPFW-SAFE-OBJECT, APPFW-POLICY-HIT, APPFW-XSS, APPFW-XML-XSS, APPFW-SQL, APPFW-XML-SQL, APPFW-XML-ATTACHMENT, APPFW-XML-DOS, APPFW-XML-VALIDATION, APPFW-XML-WSI, APPFW-XML-SCHEMA-COMPILER, APPFW-XML-SOAP-FAULT, DNSKEY-EXPIRY, DATASTREAM-RATE-LIMIT-HIT, HA-LICENSE-MISMATCH, SSL-CARD-FAILED, SSL-CARD-NORMAL, WARM-RESTART-EVENT, HARD-DISK-DRIVE-ERRORS, COMPACT-FLASH-ERRORS, CALLHOME-UPLOAD-EVENT, 1024KEY-EXCHANGE-RATE, 2048KEY-EXCHANGE-RATE, 4096KEY-EXCHANGE-RATE, SSL-CUR-SESSION-INUSE, CLUSTER-NODE-HEALTH, CLUSTER-NODE-QUORUM, CLUSTER-VERSION-MISMATCH, CLUSTER-CCO-CHANGE, CLUSTER-OVS-CHANGE, CLUSTER-SYNC-FAILURE, CLUSTER-PROP-FAILURE, HA-STICKY-PRIMARY, INBAND-PROTOCOL-VERSION-MISMATCH, SSL-CHIP-REINIT, VRID-STATE-CHANGE

Example

```
disable snmp alarm VSERVER-REQRATE
disable snmp alarm CPU SYNFLOOD
```

[Top](#)

show snmp alarm

Synopsis

show snmp alarm [<trapName>]

Description

Displays the settings of all SNMP alarms or of the specified SNMP alarm. To display the settings of all the SNMP alarms, run the command without any parameters. To display the settings of a particular SNMP alarm, specify the trapName (Alarm name) of the SNMP alarm.

Parameters

trapName

Name of the SNMP alarm whose details you want the NetScaler appliance to display. Possible values: CPU-USAGE, AVERAGE-CPU, MEMORY, MGMT-CPU-USAGE, SYNFLOOD, VSERVER-REQRATE, SERVICE-REQRATE, ENTITY-RXRATE, ENTITY-TXRATE, ENTITY-SYNFLOOD, SERVICE-MAXCLIENTS, HA-STATE-CHANGE, ENTITY-STATE, CONFIG-CHANGE, CONFIG-SAVE, SERVICEGROUP-MEMBER-REQRATE, SERVICEGROUP-MEMBER-MAXCLIENTS, MONITOR-RTO-THRESHOLD, LOGIN-FAILURE, SSL-CERT-EXPIRY, FAN-SPEED-LOW, VOLTAGE-LOW, VOLTAGE-HIGH, TEMPERATURE-HIGH, CPU-TEMPERATURE-HIGH, POWER-SUPPLY-FAILURE, DISK-USAGE-HIGH, INTERFACE-THROUGHPUT-LOW, MON_PROBE_FAILED, HA-VERSION-MISMATCH, HA-SYNC-FAILURE, HA-NO-HEARTBEATS, HA-BAD-SECONDARY-STATE, INTERFACE-BW-USAGE, RATE-LIMIT-THRESHOLD-EXCEEDED, ENTITY-NAME-CHANGE, HA-PROP-FAILURE, IP-CONFLICT, PF-RL-RATE-THRESHOLD, PF-RL-PPS-THRESHOLD, PF-RL-RATE-PKTS-DROPPED, PF-RL-PPS-PKTS-DROPPED, APPFW-START-URL, APPFW-DENY-URL, APPFW-VIOLATIONS-TYPE, APPFW-REFERER-HEADER, APPFW-CSRF-TAG, APPFW-COOKIE, APPFW-FIELD-CONSISTENCY, APPFW-BUFFER-OVERFLOW, APPFW-FIELD-FORMAT, APPFW-SAFE-COMMERCE, APPFW-

SAFE-OBJECT, APPFW-POLICY-HIT, APPFW-XSS, APPFW-XML-XSS, APPFW-SQL, APPFW-XML-SQL, APPFW-XML-ATTACHMENT, APPFW-XML-DOS, APPFW-XML-VALIDATION, APPFW-XML-WSI, APPFW-XML-SCHEMA-COMPILER, APPFW-XML-SOAP-FAULT, DNSKEY-EXPIRY, DATASTREAM-RATE-LIMIT-HIT, HA-LICENSE-MISMATCH, SSL-CARD-FAILED, SSL-CARD-NORMAL, WARM-RESTART-EVENT, HARD-DISK-DRIVE-ERRORS, COMPACT-FLASH-ERRORS, CALLHOME-UPLOAD-EVENT, 1024KEY-EXCHANGE-RATE, 2048KEY-EXCHANGE-RATE, 4096KEY-EXCHANGE-RATE, SSL-CUR-SESSION-INUSE, CLUSTER-NODE-HEALTH, CLUSTER-NODE-QUORUM, CLUSTER-VERSION-MISMATCH, CLUSTER-CCO-CHANGE, CLUSTER-OVS-CHANGE, CLUSTER-SYNC-FAILURE, CLUSTER-PROP-FAILURE, HA-STICKY-PRIMARY, INBAND-PROTOCOL-VERSION-MISMATCH, SSL-CHIP-REINIT, VRID-STATE-CHANGE

[Top](#)

snmp mib

[[set](#) | [unset](#) | [show](#)]

set snmp mib

Synopsis

```
set snmp mib [-contact <string>] [-name <string>] [-location <string>] [-customID <string>]
```

Description

Configures the SNMP agent of the NetScaler appliance with information that identifies the appliance, such as the name of the administrator for this NetScaler appliance, a name for the appliance, and the location of the appliance. SNMP managers can query the NetScaler appliance for this information.

Parameters

contact

Name of the administrator for this NetScaler appliance. Along with the name, you can include information on how to contact this person, such as a phone number or an email address. Can consist of 1 to 127 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), space (), at sign (@), equals (=), colon (:), and underscore (_) characters. The following requirement applies only to the NetScaler CLI: If the information includes one or more spaces, enclose it in double or single quotation marks (for example, "my contact" or 'my contact'). Default value: "WebMaster (default)"

name

Name for this NetScaler appliance. Can consist of 1 to 127 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), space (), at sign (@), equals (=), colon (:), and underscore (_) characters. You should choose a name that helps identify the NetScaler appliance. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose it in double or single quotation marks (for example, "my name" or 'my name'). Default value: "NetScaler"

location

Physical location of the NetScaler appliance. For example, you can specify building name, lab number, and rack number. Can consist of 1 to 127 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), space (), at sign (@), equals (=), colon (:), and underscore (_) characters. The following requirement applies only to the NetScaler CLI: If the location includes one or more spaces, enclose it in double or single quotation marks (for example, "my location" or 'my location'). Default value: "POP (default)"

customID

Custom identification number for the NetScaler appliance. Can consist of 1 to 127 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), space (), at sign (@), equals (=), colon (:), and underscore (_) characters. You should choose a custom identification that helps identify the NetScaler appliance. The following requirement applies only to the NetScaler CLI: If the ID includes one or more spaces, enclose it in double or single quotation marks (for example, "my ID" or 'my ID'). Default value: "Default"

[Top](#)**unset snmp mib****Synopsis**

```
unset snmp mib [-contact] [-name] [-location] [-customID]
```

Description

Use this command to remove snmp mib settings. Refer to the set snmp mib command for meanings of the arguments.

[Top](#)**show snmp mib****Synopsis**

```
show snmp mib
```

Description

Displays the information that has been configured on the SNMP agent for the purpose of identifying the NetScaler appliance, such as the name of the appliance, administrator, and location.

Example

```
show snmp mib
```

[Top](#)**snmp engineId**

[[set](#) | [unset](#) | [show](#)]

set snmp engineid

Synopsis

set snmp engineid <engineID> [-ownerNode <positive_integer>]

Description

Modifies the SNMPv3 engine identification (ID) on the NetScaler appliance. Caution: Changing the ID of the SNMPv3 engine invalidates the current SNMP users. You have to reconfigure the SNMP users in the SNMP managers. The SNMPv3 engine has an identification (ID) that uniquely identifies it on the appliance and is used in the communication between the SNMPv3 user and the SNMPv3 engine. The engine ID is preconfigured by Citrix and is based on the MAC address of one of its interfaces. Overriding the engine ID is not necessary, but you can change it.

Parameters

engineID

A hexadecimal value of at least 10 characters, uniquely identifying the engineid

ownerNode

ID of the cluster node for which you are setting the engineid Default value: -1
Maximum value: 31

[Top](#)

unset snmp engineid

Synopsis

unset snmp engineid [-ownerNode <positive_integer>]

Description

Resets the SNMPv3 engine identification (ID) on the NetScaler appliance to its default value. The NetScaler appliance derives the engine ID from the MAC address of one of its interfaces. Caution: Changing the ID of the SNMPv3 engine invalidates the current SNMP users. You have to reconfigure the SNMP users in the SNMP managers..Refer to the set snmp engineid command for meanings of the arguments.

[Top](#)

show snmp engineid

Synopsis

show snmp engineid [-ownerNode <positive_integer>]

Description

Displays the ID of the SNMPv3 engine of the NetScaler appliance.

Parameters

ownerNode

ID of the cluster node for which you are setting the engineid Default value: -1
Maximum value: 31

[Top](#)

snmp option

[[set](#) | [unset](#) | [show](#)]

set snmp option

Synopsis

```
set snmp option [-snmpset ( ENABLED | DISABLED )] [-snmpTrapLogging ( ENABLED |
DISABLED )]
```

Description

Enables or disables SNMP options for SNMP SET and SNMP trap logging.

Parameters

snmpset

Accept SNMP SET requests sent to the NetScaler appliance, and allow SNMP managers to write values to MIB objects that are configured for write access. Possible values: ENABLED, DISABLED Default value: DISABLED

snmpTrapLogging

Log any SNMP trap events (for SNMP alarms in which logging is enabled) even if no trap listeners are configured. With the default setting, SNMP trap events are logged if at least one trap listener is configured on the appliance. Possible values: ENABLED, DISABLED Default value: DISABLED

[Top](#)

unset snmp option

Synopsis

```
unset snmp option [-snmpset] [-snmpTrapLogging]
```

Description

Use this command to remove snmp option settings. Refer to the set snmp option command for meanings of the arguments.

[Top](#)

show snmp option

Synopsis

```
show snmp option
```

Description

Displays the settings for the following SNMP options: SNMP SET and SNMP trap Logging.

[Top](#)

SPILLOVER Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [spillover policy](#)
- ♦ [spillover action](#)

spillover policy

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#) | [rename](#) | [stat](#)]

add spillover policy

Synopsis

add spillover policy <name> -rule <expression> -action <string> [-comment <string>]

Description

Add a spillover policy. SPILLOVER policies that can be added are based on vserver expressions.

Parameters

name

Name of the spillover policy.

rule

Expression to be used by the spillover policy.

action

Action for the spillover policy. Action is created using add spillover action command

comment

Any comments that you might want to associate with the spillover policy.

Example

```
add spillover policy pol1 -rule
"SYS.VSERVER("abc").ACTIVESERVICES.LE(2) -action
act1
add spillover policy pol2 -rule
"SYS.VSERVER("abc").CONNECTIONS.GT(500) -action
act2"
```

[Top](#)

rm spillover policy

Synopsis

rm spillover policy <name>

Description

Removes a spillover policy.

Parameters

name

Name of the spillover policy.

[Top](#)

set spillover policy

Synopsis

set spillover policy <name> [-rule <expression>] [-action <string>] [-comment <string>]

Description

Used to change the expression or other parameters of an existing policy.

Parameters

name

Name of the spillover policy.

rule

Expression to be used by the spillover policy.

action

Action for the spillover policy. Action is created using add spillover action command

comment

Any comments that you might want to associate with the spillover policy.

Example

```
set spillover policy pol1 -rule
"SYS.VSERVER("abc").ACTIVESERVICES.LE(1) "
set spillover policy pol2 -action act4"
```

[Top](#)

unset spillover policy

Synopsis

unset spillover policy <name> -comment

Description

Use this command to remove spillover policy settings. Refer to the set spillover policy command for meanings of the arguments.

[Top](#)

show spillover policy

Synopsis

show spillover policy [<name>]

Description

Displaying the policy-related information.

Parameters

name

Name of the spillover policy.

[Top](#)

rename spillover policy

Synopsis

rename spillover policy <name>@ <newName>@

Description

Renames a spillover policy.

Parameters

name

Existing name of the policy.

newName

New name for the spillover policy. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Choose a name that reflects the function that the policy performs. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy').

Example

```
rename spillover policy oldname newname
```

[Top](#)

stat spillover policy

Synopsis

stat spillover policy [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-clearstats (basic | full)]

Description

Displays statistics for all spillover policies currently configured on the NetScaler appliance, or detailed statistics for the specified policy.

Parameters

name

Name of the spillover policy for which to show detailed statistics.

clearstats

Clear the statistics / counters Possible values: basic, full

[Top](#)

spillover action

[[add](#) | [rm](#) | [show](#) | [rename](#)]

add spillover action

Synopsis

add spillover action <name> -action SPILLOVER

Description

Creating spillover action

Parameters

name

Name of the spillover action.

action

Spillover action. Currently only type SPILLOVER is supported Possible values: SPILLOVER

[Top](#)

rm spillover action

Synopsis

rm spillover action <name>

Description

Removes a spillover policy.

Parameters

name

Name of the spillover action.

[Top](#)

show spillover action

Synopsis

show spillover action [<name>]

Description

Displaying spillover actions

Parameters

name

Name of the spillover action.

[Top](#)

rename spillover action

Synopsis

rename spillover action <name>@ <newName>@

Description

Renames a spillover action.

Parameters

name

Existing name of the action.

newName

New name for the spillover action. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Choose a name that can be correlated with the function that the action performs. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

Example

```
rename spillover policy oldname newname
```

[Top](#)

SSL Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [ssl](#)
- ♦ [ssl fipsKey](#)

- ♦ [ssl wrapkey](#)
- ♦ [ssl certKey](#)
- ♦ [ssl ciphersuite](#)
- ♦ [ssl cipher](#)
- ♦ [ssl crt](#)
- ♦ [ssl action](#)
- ♦ [ssl policy](#)
- ♦ [ssl policylabel](#)
- ♦ [ssl ocsponder](#)
- ♦ [ssl rsaKey](#)
- ♦ [ssl pkcs12](#)
- ♦ [ssl pkcs8](#)
- ♦ [ssl dhParam](#)
- ♦ [ssl dsaKey](#)
- ♦ [ssl certLink](#)
- ♦ [ssl certReq](#)
- ♦ [ssl cert](#)
- ♦ [ssl stats](#)
- ♦ [ssl parameter](#)
- ♦ [ssl fips](#)
- ♦ [ssl service](#)
- ♦ [ssl serviceGroup](#)
- ♦ [ssl vservice](#)
- ♦ [ssl fipsSIMTarget](#)
- ♦ [ssl fipsSIMSource](#)
- ♦ [ssl global](#)
- ♦ [ssl dtlsProfile](#)

ssl

stat ssl

Synopsis

```
stat ssl [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-clearstats ( basic | full )]
```

Description

Displays SSL statistics.

Parameters**clearstats**

Clear the statistics / counters Possible values: basic, full

ssl fipsKey

[[create](#) | [rm](#) | [show](#) | [import](#) | [export](#)]

create ssl fipsKey**Synopsis**

create ssl fipsKey <fipsKeyName> -modulus <positive_integer> [-exponent (3 | F4)]

Description

Generates a FIPS key within the Hardware Security Module (HSM) of the FIPS card.

Parameters**fipsKeyName**

Name for the FIPS key. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the FIPS key is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my fipskey" or 'my fipskey').

modulus

Modulus, in multiples of 64, of the FIPS key to be created. Minimum value: 1024
Maximum value: 4096

exponent

Exponent value for the FIPS key to be created. Available values function as follows:
3=3 (hexadecimal) F4=10001 (hexadecimal) Possible values: 3, F4 Default value: 3

Example

```
create fipskey fips1 -modulus 1024 -exp f4
```

[Top](#)

rm ssl fipsKey**Synopsis**

rm ssl fipsKey <fipsKeyName> ...

Description

Removes all the FIPS keys, or the specified FIPS key, from the appliance.

Parameters

fipsKeyName

Name of the FIPS key to remove.

Example

```
rm fipskey fips1
```

[Top](#)

show ssl fipsKey

Synopsis

show ssl fipsKey [<fipsKeyName>]

Description

Displays information about all the FIPS keys configured on the appliance, or displays detailed information about the specified FIPS key.

Parameters

fipsKeyName

Name of the FIPS key for which to show detailed information.

Example

```
1) An example of output of show ssl fipskey
command is as follows:
show fipskey
2 FIPS keys:
1)      FIPS Key Name: fips1
2)      FIPS Key Name: fips2

2) An example of output of show fipskey command
with FIPS key name specified is as follows:
show fipskey fips1
FIPS Key Name: fips1      Modulus: 1024    Public
Exponent: 3 (Hex: 0x3)
```

[Top](#)

import ssl fipsKey

Synopsis

```
import ssl fipsKey <fipsKeyName> -key <string> [-inform <inform>] [-wrapKeyName
<string>] [-iv <string>] [-exponent ( 3 | F4 )]
```

Description

Imports a FIPS key into the Hardware Security Module (HSM) of the FIPS card. Can import an existing FIPS key, or can import, as a FIPS key, an external private key, such as a key that was created on an Apache or IIS external Web server.

Parameters

fipsKeyName

Name for the FIPS key to be imported. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the FIPS key is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my fipskey" or 'my fipskey').

key

Name of and, optionally, path to the key file to be imported. /nsconfig/ssl/ is the default path.

inform

Input format of the key file. Available formats are: SIM - Secure Information Management; select when importing a FIPS key. If the external FIPS key is encrypted, first decrypt it, and then import it. PEM - Privacy Enhanced Mail; select when importing a non-FIPS key. Possible values: SIM, DER, PEM Default value: FORMAT_SIM

wrapKeyName

Name of the wrap key to use for importing the key. Required for importing a non-FIPS key.

iv

Initialization Vector (IV) to use for importing the key. Required for importing a non-FIPS key.

exponent

Exponent value for the FIPS key to be created. Available values function as follows: 3=3 (hexadecimal) F4=10001 (hexadecimal) Possible values: 3, F4 Default value: 3

Example

```
1)    import fipskey fips1 -key /nsconfig/ssl/
      fipskey.sim
      The above example imports a FIPS key stored in the
      file fipskey.sim in the system.
2)    import fipskey fips2 -key /nsconfig/ssl/
      key.der -inform DER -wrapKeyName wrapkey1 -iv
      wrap123
```

```
The above example imports a non-FIPS key stored in
the file key.der in the system.
```

[Top](#)

export ssl fipsKey

Synopsis

```
export ssl fipsKey <fipsKeyName> -key <string>
```

Description

Exports a FIPS key from one appliance to another or backs up a FIPS key in a secure manner. The exported key is secured by using a strong asymmetric key encryption method.

Parameters

fipsKeyName

Name of the FIPS key to export.

key

Name of and, optionally, path to the exported key file. /nsconfig/ssl/ is the default path.

Example

```
export fipskey fips1 -key /nsconfig/ssl/fips1.key
```

[Top](#)

ssl wrapkey

[[create](#) | [rm](#) | [show](#)]

create ssl wrapkey

Synopsis

```
create ssl wrapkey <wrapKeyName> {-password } {-salt }
```

Description

Generates a wrap key.

Parameters

wrapKeyName

Name for the wrap key. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the wrap key is created. The following requirement applies only to the

NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my key" or 'my key').

password

Password string for the wrap key.

salt

Salt string for the wrap key.

Example

```
create wrapkey wrap1 -password wrapkey123 -salt  
wrapsalt123
```

[Top](#)

rm ssl wrapkey

Synopsis

rm ssl wrapkey <wrapKeyName> ...

Description

Removes all the wrap keys, or the specified wrap key, from the appliance.

Parameters**wrapKeyName**

Name of the wrap key to remove.

Example

```
rm wrapkey wrap1
```

[Top](#)

show ssl wrapkey

Synopsis

show ssl wrapkey

Description

Display the wrap keys.

Example

```
An example of output of 'show wrapkey' command is  
as shown below:  
sh wrapkey
```

```

1 WRAP key:
1)   WRAP Key Name: wrap1

```

[Top](#)

ssl certKey

[[add](#) | [rm](#) | [set](#) | [unset](#) | [bind](#) | [unbind](#) | [link](#) | [unlink](#) | [show](#) | [update](#)]

add ssl certKey

Synopsis

```
add ssl certKey <certkeyName> -cert <string> [(-key <string> [-password]) | -fipsKey
<string>] [-inform ( DER | PEM )] [-expiryMonitor ( ENABLED | DISABLED ) [-
notificationPeriod <positive_integer>]] [-bundle ( YES | NO )]
```

Description

Adds a certificate-key pair to memory. After it is bound to a virtual server or service, it is used for processing SSL transactions. In a high-availability configuration, the path to the certificate and the optional private key must be the same on the primary and the secondary appliance. For a server certificate, a private key is required.

Parameters

certkeyName

Name for the certificate and private-key pair. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the certificate-key pair is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cert" or 'my cert').

cert

Name of and, optionally, path to the X509 certificate file that is used to form the certificate-key pair. The certificate file should be present on the appliance's hard-disk drive or solid-state drive. Storing a certificate in any location other than the default might cause inconsistency in a high availability setup. /nsconfig/ssl/ is the default path.

key

Name of and, optionally, path to the private-key file that is used to form the certificate-key pair. The certificate file should be present on the appliance's hard-disk drive or solid-state drive. Storing a certificate in any location other than the default might cause inconsistency in a high availability setup. /nsconfig/ssl/ is the default path.

fipsKey

Name of the FIPS key that was created inside the Hardware Security Module (HSM) of a FIPS appliance, or a key that was imported into the HSM.

inform

Input format of the certificate and the private-key files. The two formats supported by the appliance are: PEM - Privacy Enhanced Mail DER - Distinguished Encoding Rule
Possible values: DER, PEM Default value: FORMAT_PEM

passplain

Pass phrase used to encrypt the private-key. Required when adding an encrypted private-key in PEM format.

expiryMonitor

Issue an alert when the certificate is about to expire. Possible values: ENABLED, DISABLED

notificationPeriod

Time, in number of days, before certificate expiration, at which to generate an alert that the certificate is about to expire. Minimum value: 10 Maximum value: 100

bundle

Parse the certificate chain as a single file after linking the server certificate to its issuer's certificate within the file. Possible values: YES, NO Default value: NO

Example

```
1)    add ssl certkey siteAcertkey -cert /
nsconfig/ssl/cert.pem -key /nsconfig/ssl/pkey.pem
The above command loads a certificate and private
key file.
2)    add ssl certkey siteAcertkey -cert /
nsconfig/ssl/cert.pem -key /nsconfig/ssl/pkey.pem -
password
Password: *****
The above command loads a certificate and private
key file. Here the private key file is an
encrypted key.
3)    add ssl certkey fipscert -cert /nsconfig/ssl/
cert.pem -fipskey fips1024
The above command loads a certificate and
associates it with the corresponding FIPS key that
resides within the HSM.
```

[Top](#)

rm ssl certKey**Synopsis**

```
rm ssl certKey <certkeyName> ...
```

Description

Removes all the certificate-key pairs, or the specified certificate-key pair, from the appliance. The certificate-key pair is removed only if it is not referenced by any other object. The reference count is updated when the certificate-key pair is bound to an SSL virtual server or linked to another certificate-key pair.

Parameters

certkeyName

Name of the certificate-key pair to remove.

Example

```
1)      rm ssl certkey siteAcertkey
The above command removes the certificate-key pair
siteAcertkey from the system.
```

[Top](#)

set ssl certKey

Synopsis

```
set ssl certKey <certkeyName> [-expiryMonitor ( ENABLED | DISABLED ) [-
notificationPeriod <positive_integer>]]
```

Description

Modifies the specified attributes of a certificate-key pair.

Parameters

certkeyName

Name of the certificate-key pair to modify.

expiryMonitor

Issue an alert when the certificate is about to expire. Possible values: ENABLED, DISABLED

[Top](#)

unset ssl certKey

Synopsis

```
unset ssl certKey <certkeyName> [-expiryMonitor] [-notificationPeriod]
```

Description

Use this command to remove ssl certKey settings. Refer to the set ssl certKey command for meanings of the arguments.

[Top](#)

bind ssl certKey

Synopsis

```
bind ssl certKey [<certkeyName>] [-ocspResponder <string>] [-priority
<positive_integer>]
```

Description

Binds a certificate-key pair to an SSL virtual server or an SSL service.

Parameters

certkeyName

Name of the certificate-key pair.

ocspResponder

Name of the OCSP responder to be associated with the CA certificate.

vServerName

The name of the SSL virtual server name to which the certificate-key pair needs to be bound.

serviceName

The name of the SSL service to which the certificate-key pair needs to be bound. Use the `###add service###` command to create this service.

serviceGroupName

The name of the SSL service group to which the certificate-key pair needs to be bound. Use the "add servicegroup" command to create this service.

CA

If this option is specified, it indicates that the certificate-key pair being bound to the SSL virtual server is a CA certificate. If this option is not specified, the certificate-key pair is bound as a normal server certificate. Note: In case of a normal server certificate, the certificate-key pair should consist of both the certificate and the private-key.

Example

```
1)    bind ssl certkey cacert -ocspResponder
      ocsf_ca -priority 1
In the above example, the CA certificate cacert is
bound with the OCSP responder ocsf_ca with
priority 1, which is highest.
```

[Top](#)

unbind ssl certKey

Synopsis

`unbind ssl certKey <certkeyName> -ocspResponder <string>`

Description

Unbinds the specified certificate-key pair from the SSL virtual server or service.

Parameters

certkeyName

Name of the certificate-key pair to unbind.

ocspResponder

Name of the OCSP responder.

vServerName

The name of the SSL virtual server.

serviceName

The name of the SSL service

serviceGroupName

The name of the service group.

CA

The certificate-key pair being unbound is a Certificate Authority (CA) certificate. If you choose this option, the certificate-key pair is unbound from the list of CA certificates that were bound to the specified SSL virtual server or SSL service.

Example

```
1)      unbind ssl certkey sslvip siteAcertkey
In the above example, the server certificate
siteAcertkey is unbound from the SSL virtual
server.
2)      unbind ssl certkey sslvip CAcertkey -CA
In the above example, the CA certificate CAcertkey
is unbound from the SSL virtual server.
```

[Top](#)

link ssl certKey

Synopsis

link ssl certKey <certkeyName> <linkCertKeyName>

Description

Links a certificate-key pair to its Certificate Authority (CA) certificate-key pair.

Parameters

certkeyName

Name of the certificate-key pair to link to its issuer's certificate-key pair in the chain.

linkCertKeyName

Name of the Certificate Authority certificate-key pair to which to link a certificate-key pair.

Example

```
1)      link ssl certkey siteAcertkey CAcertkey
In the above example, the certificate-key
```

```
siteAcertkey is bound to its issuer certificate-  
key pair CAcertkey.
```

[Top](#)

unlink ssl certKey

Synopsis

```
unlink ssl certKey <certkeyName>
```

Description

Unlinks the certificate-key pair from its Certificate-Authority (CA) certificate-key pair.

Parameters

certkeyName

Name of the certificate-key pair to unlink.

Example

```
1)      unlink ssl certkey siteAcertkey  
The above example unlinks the certificate  
'siteAcertkey' from its Certificate-Authority (CA)  
certificate.
```

[Top](#)

show ssl certKey

Synopsis

```
show ssl certKey [<certkeyName>]
```

Description

Displays information about all the certificate-key pairs configured on the appliance, or displays detailed information about the specified certificate-key pair.

Parameters

certkeyName

Name of the certificate-key pair for which to show detailed information.

Example

```
1) An example of the output of the show ssl  
certkey command is shown below:  
   2 configured certkeys:  
1)   Name: siteAcertkey  
     Cert Path: /nsconfig/ssl/siteA-cert.pem  
     Key Path:  /nsconfig/ssl/siteA-key.pem  
     Format: PEM
```

```

        Status: Valid
2)    Name: cert1
        Cert Path: /nsconfig/ssl/server_cert.pem
        Key Path: /nsconfig/ssl/server_key.pem
        Format: PEM
        Status: Valid

2) An example of the output of the show ssl
certkey siteAcertkey command is shown below:
Name: siteAcertkey          Status: Valid
Version: 3
Serial Number: 02
Signature Algorithm: md5WithRSAEncryption
Issuer: /C=US/ST=CA/L=Santa Clara/O=siteA/OU=Tech
Validity
    Not Before: Nov 11 14:58:18 2001 GMT
    Not After: Aug 7 14:58:18 2004 GMT
Subject: /C=US/ST=CA/L=San Jose/O=CA/OU=Security
Public Key Algorithm: rsaEncryption
Public Key size: 1024

```

[Top](#)

update ssl certKey

Synopsis

```
update ssl certKey <certkeyName> [-cert <string>] [(-key <string> [-password]) | -
fipsKey <string>] [-inform ( DER | PEM )] [-noDomainCheck]
```

Description

Updates the certificate or private key in a certificate-key pair. In a high availability configuration, the path to the certificate and the optional private key must be the same on the primary and secondary nodes.

Parameters

certkeyName

Name of the certificate-key pair to update.

cert

Name of and, optionally, path to the X509 certificate file that is used to form the certificate-key pair. The certificate file should be present on the appliance's hard-disk drive or solid-state drive. Storing a certificate in any location other than the default might cause inconsistency in a high availability setup. /nsconfig/ssl/ is the default path.

key

Name of and, optionally, path to the private-key file that is used to form the certificate-key pair. The certificate file should be present on the appliance's hard-disk drive or solid-state drive. Storing a certificate in any location other than the default might cause inconsistency in a high availability setup. /nsconfig/ssl/ is the default path.

fipsKey

Name of the FIPS key that was created inside the Hardware Security Module (HSM) of a FIPS appliance, or a key that was imported into the HSM.

inform

Input format of the certificate and the private-key files. The two formats supported by the appliance are: PEM - Privacy Enhanced Mail DER - Distinguished Encoding Rule
Possible values: DER, PEM Default value: FORMAT_PEM

passplain

Pass phrase used to encrypt the private-key. Required when adding an encrypted private-key in PEM format.

noDomainCheck

Override the check for matching domain names during a certificate update operation.

Example

```
1)      update ssl certkey siteAcertkey -cert /
nsconfig/ssl/cert.pem -key /nsconfig/ssl/pkey.pem
The above command updates a certificate and
private key file.
2)      update ssl certkey siteAcertkey -cert /
nsconfig/ssl/cert.pem -key /nsconfig/ssl/pkey.pem -
password
Password: *****
The above command updates a certificate and
private key file. Here the private key file is an
encrypted key.
3)      update ssl certkey mydomaincert
The above command updates the certificate using
the same parameters (-cert path/-key path) that it
was added with.
```

[Top](#)

ssl ciphersuite

show ssl ciphersuite

Synopsis

```
show ssl ciphersuite [<cipherName>]
```

Description

Displays information about all the cipher suites configured on the appliance, or displays detailed information about the specified cipher-suite. A cipher suite comprises a protocol and the following algorithms: key exchange (Kx), authentication (Au), encryption (Enc), and message authentication code (Mac).

Parameters

cipherName

Name of the cipher suite for which to show detailed information.

Example

```
1) An example of the output of the show ssl cipher
SSL3-RC4-MD5 command is as follows:
Cipher Name: SSL3-RC4-MD5
Description: SSLv3 Kx=RSA      Au=RSA
Enc=RC4(128)  Mac=MD5
2) This example displays the details of individual
ciphers in the system predefined cipher-alias:
SSLv2 (the command show ssl cipher SSLv2 has been
entered):
8 configured cipher(s) in alias
1) Cipher Name: SSL2-RC4-MD5
   Description: SSLv2 Kx=RSA      Au=RSA
   Enc=RC4(128)  Mac=MD5
2) Cipher Name: SSL2-EXP-RC4-MD5
   Description: SSLv2 Kx=RSA(512) Au=RSA
   Enc=RC4(40)   Mac=MD5 export
3) Cipher Name: SSL2-RC2-CBC-MD5
   Description: SSLv2 Kx=RSA      Au=RSA
   Enc=RC2(128)  Mac=MD5
4) Cipher Name: SSL2-EXP-RC2-CBC-MD5
   Description: SSLv2 Kx=RSA(512) Au=RSA
   Enc=RC2(40)   Mac=MD5 export
5) Cipher Name: SSL2-DES-CBC-MD5
   Description: SSLv2 Kx=RSA      Au=RSA
   Enc=DES(56)   Mac=MD5
6) Cipher Name: SSL2-DES-CBC3-MD5
   Description: SSLv2 Kx=RSA      Au=RSA
   Enc=3DES(168) Mac=MD5
7) Cipher Name: SSL2-RC4-64-MD5
   Description: SSLv2 Kx=RSA      Au=RSA
   Enc=RC4(64)   Mac=MD5
```

ssl cipher

[[add](#) | [bind](#) | [show](#) | [rm](#) | [unbind](#)]

add ssl cipher

Synopsis

add ssl cipher <cipherGroupName>

Description

Creates a user-defined cipher group, which you can bind to an SSL virtual server instead of binding ciphers individually. Although you cannot modify a built-in cipher

group, you can add built-in cipher groups as well as individual ciphers to a user-defined cipher group.

Parameters

cipherGroupName

Name for the user-defined cipher group. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the cipher group is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my ciphergroup" or 'my ciphergroup').

cipherAliasName/cipherName/cipherGroupName

The individual cipher name(s), a user-defined cipher group, or a system predefined cipher alias that will be added to the predefined cipher alias that will be added to the group cipherGroupName. If a cipher alias or a cipher group is specified, all the individual ciphers in the cipher alias or group will be added to the user-defined cipher group.

Example

```
1)    add ssl cipher mygroup SSL2-RC4-MD5 SSL2-EXP-RC4-MD5
```

The above command creates a new cipher-group by the name: mygroup, with the two ciphers SSL2-RC4-MD5 and SSL2-EXP-RC4-MD5, as part of the cipher-group.

If a cipher-group by the name: mygroup already exists in system, then the two ciphers is added to the list of ciphers contained in the group.

```
2)    add ssl cipher mygroup HIGH MEDIUM
```

The above command creates a new cipher-group by the name: mygroup, with the ciphers from the cipher alias "HIGH" and "MEDIUM" as part of the cipher group.

If a cipher-group by the name, mygroup, already exists in system, then the ciphers from the two aliases is added to the list of ciphers contained in the group.

[Top](#)

bind ssl cipher

Synopsis

```
bind ssl cipher [<cipherGroupName>@] [-cipherName <string>]
```

Description

Adds ciphers to a user-defined cipher group. You can add an existing cipher group to a user-defined cipher group but you cannot modify a built-in cipher group.

Parameters

cipherGroupName

Name of the user-defined cipher group.

vServerName

The name of the SSL virtual server to which the cipher-suite is to be bound.

serviceName

The name of the SSL service name to which the cipher-suite is to be bound.

serviceGroupName

The name of the SSL service name to which the cipher-suite is to be bound.

cipherOperation

The operation that is performed when adding the cipher-suite. Possible cipher operations are: ADD - Appends the given cipher-suite to the existing one configured for the virtual server. REM - Removes the given cipher-suite from the existing one configured for the virtual server. ORD - Overrides the current configured cipher-suite for the virtual server with the given cipher-suite. Possible values: ADD, REM, ORD
Default value: 6

cipherAliasName/cipherName/cipherGroupName

A cipher-suite can consist of an individual cipher name, the system predefined cipher-alias name, or user defined cipher-group name.

cipherName

Name of the individual cipher, user-defined cipher group, or predefined (built-in) cipher alias to add to the cipher group.

Example

```
1)      bind ssl cipher sslvip ADD SSL3-RC4-SHA
The above example appends the cipher SSL3-RC4-SHA
to the cipher-suite already configured for the SSL
virtual server sslvip.
2)      bind ssl cipher sslvip REM NULL
The above example removes the ciphers identified
by the system's predefined cipher-alias -NULL from
the cipher-suite already configured for the SSL
virtual server sslvip.
3)      bind ssl cipher sslvip ORD HIGH
The above example overrides the existing cipher-
suite configured for the SSL virtual server with
ciphers, having HIGH encryption strength (ciphers
supporting 168-bit encryption).
```

Note: The individual ciphers contained in a system predefined cipher-alias can be viewed by using the

```
following command: show ssl cipher
<cipherAlaisName>
```

[Top](#)

show ssl cipher

Synopsis

```
show ssl cipher [<cipherGroupName>]
```

Description

Displays information about all the cipher groups defined on the appliance, or displays detailed information about the specified cipher group.

Parameters

cipherGroupName

Name of the cipher group for which to show detailed information.

Example

```
1) An example of the output of the show ssl cipher
SSL3-RC4-MD5 command is as follows:
Cipher Name: SSL3-RC4-MD5
Description: SSLv3 Kx=RSA      Au=RSA
Enc=RC4(128)  Mac=MD5
2) This example displays the details of individual
ciphers in the system predefined cipher-alias:
SSLv2 (the command show ssl cipher SSLv2 has been
entered):
8 configured cipher(s) in alias
1) Cipher Name: SSL2-RC4-MD5
   Description: SSLv2 Kx=RSA      Au=RSA
   Enc=RC4(128)  Mac=MD5
2) Cipher Name: SSL2-EXP-RC4-MD5
   Description: SSLv2 Kx=RSA(512) Au=RSA
   Enc=RC4(40)   Mac=MD5 export
3) Cipher Name: SSL2-RC2-CBC-MD5
   Description: SSLv2 Kx=RSA      Au=RSA
   Enc=RC2(128)  Mac=MD5
4) Cipher Name: SSL2-EXP-RC2-CBC-MD5
   Description: SSLv2 Kx=RSA(512) Au=RSA
   Enc=RC2(40)   Mac=MD5 export
5) Cipher Name: SSL2-DES-CBC-MD5
   Description: SSLv2 Kx=RSA      Au=RSA
   Enc=DES(56)   Mac=MD5
6) Cipher Name: SSL2-DES-CBC3-MD5
   Description: SSLv2 Kx=RSA      Au=RSA
   Enc=3DES(168) Mac=MD5
7) Cipher Name: SSL2-RC4-64-MD5
   Description: SSLv2 Kx=RSA      Au=RSA
   Enc=RC4(64)   Mac=MD5
```

[Top](#)

rm ssl cipher

Synopsis

`rm ssl cipher <cipherGroupName>`

Description

Removes a user-defined cipher group from the appliance.

Parameters

cipherGroupName

Name of the user-defined cipher group to remove.

cipherName

The cipher(s) to be removed from the cipher group.

Example

```
1)      rm ssl cipher mygroup SSL2-RC4-MD5
The above example removes the cipher SSL2-RC4-MD5
from the cipher group mygroup.
2)      rm ssl cipher mygroup
The above example will remove the cipher group
'mygroup' from the system.
```

[Top](#)

unbind ssl cipher

Synopsis

`unbind ssl cipher <cipherGroupName> [-cipherName <string> ...]`

Description

Removes all the ciphers from a user-defined cipher group. You can only remove individual ciphers from a user-defined cipher group. Removing groups is not supported.

Parameters

cipherGroupName

Name of the user-defined cipher group.

cipherName

Name(s) of the cipher(s) to be removed from the user-defined cipher group.

Example

```
1)      rm ssl cipher mygroup SSL2-RC4-MD5
The above example removes the cipher SSL2-RC4-MD5
from the cipher group mygroup.
2)      rm ssl cipher mygroup
```

The above example will remove the cipher group 'mygroup' from the system.

[Top](#)

ssl crt

[[add](#) | [create](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add ssl crt

Synopsis

```
add ssl crt <crlName> <crlPath> [-inform ( DER | PEM )] [-refresh ( ENABLED |
DISABLED )] [-CAcert <string>] [-method ( HTTP | LDAP )] [-server <ip_addr|ipv6_addr|
*> | -url <URL>] [-port <port>] [-baseDN <string>] [-scope ( Base | One )] [-interval
<interval>] [-day <integer>] [-time <HH:MM>] [-bindDN <string>] {-password } [-binary
( YES | NO )]
```

Description

Adds a Certificate Revocation List (CRL). A CRL identifies invalid certificates by serial number and issuer. In a high availability configuration, the CRL must be in the same location on the primary and secondary nodes.

Parameters

crlName

Name for the Certificate Revocation List (CRL). Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the CRL is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my crt" or 'my crt').

crlPath

Path to the CRL file. /var/netscaler/ssl/ is the default path.

inform

Input format of the CRL file. The two formats supported on the appliance are: PEM - Privacy Enhanced Mail. DER - Distinguished Encoding Rule. Possible values: DER, PEM
Default value: FORMAT_PEM

refresh

Set CRL auto refresh. Possible values: ENABLED, DISABLED

CAcert

CA certificate that has issued the CRL. Required if CRL Auto Refresh is selected. Install the CA certificate on the appliance before adding the CRL.

method

Method for CRL refresh. If LDAP is selected, specify the method, CA certificate, base DN, port, and LDAP server name. If HTTP is selected, specify the CA certificate,

method, URL, and port. Cannot be changed after a CRL is added. Possible values: HTTP, LDAP

server

IP address of the LDAP server from which to fetch the CRLs.

url

URL of the CRL distribution point.

port

Port for the LDAP server. Minimum value: 1

baseDN

Base distinguished name (DN), which is used in an LDAP search to search for a CRL. Citrix recommends searching for the Base DN instead of the Issuer Name from the CA certificate, because the Issuer Name field might not exactly match the LDAP directory structure's DN.

scope

Extent of the search operation on the LDAP server. Available settings function as follows: One - One level below Base DN. Base - Exactly the same level as Base DN. Possible values: Base, One Default value: NSAPI_ONESCOPE

interval

CRL refresh interval. Use the NONE setting to unset this parameter. Possible values: MONTHLY, WEEKLY, DAILY, NONE

day

Day on which to refresh the CRL, or, if the Interval parameter is not set, the number of days after which to refresh the CRL. If Interval is set to MONTHLY, specify the date. If Interval is set to WEEKLY, specify the day of the week (for example, Sun=0 and Sat=6). This parameter is not applicable if the Interval is set to DAILY. Maximum value: 31

time

Time, in hours (1-24) and minutes (1-60), at which to refresh the CRL.

bindDN

Bind distinguished name (DN) to be used to access the CRL object in the LDAP repository if access to the LDAP repository is restricted or anonymous access is not allowed.

password

Password to access the CRL in the LDAP repository if access to the LDAP repository is restricted or anonymous access is not allowed.

binary

Set the LDAP-based CRL retrieval mode to binary. Possible values: YES, NO Default value: NO

Example

```
1) add ssl certkey CAcert -cert /nsconfig/ssl/
   ca_cert.pem
```



```
add ssl crl crl_file /var/netscaler/ssl/crl.pem -
cacert CAcert
The above command adds a CRL from local storage
system (HDD) with no refresh set.
2) add ssl certkey CAcert -cert /nsconfig/ssl/
ca_cert.pem
add ssl crl crl_file /var/netscaler/ssl/
crl_new.pem -cacert CAcert -refresh ENABLED -
server 10.102.1.100 -port 389 -interval DAILY -
baseDN o=example.com,ou=security,c=US
The above command adds a CRL to the system by
fetching the CRL from the LDAP server and setting
the refresh interval as daily.
```

[Top](#)

create ssl crl

Synopsis

```
create ssl crl <CAcertFile> <CAkeyFile> <indexFile> (-revoke <input_filename> | -
genCRL <output_filename>) {-password }
```

Description

Revokes a certificate, or list of certificates, or generates a CRL for the list of revoked certificates.

Parameters

CAcertFile

Name of and, optionally, path to the CA certificate file. /nsconfig/ssl/ is the default path. Maximum value: 63

CAkeyFile

Name of and, optionally, path to the CA key file. /nsconfig/ssl/ is the default path. Maximum value: 63

indexFile

Name of and, optionally, path to the file containing the serial numbers of all the certificates that are revoked. Revoked certificates are appended to the file. /nsconfig/ssl/ is the default path. Maximum value: 63

revoke

Name of and, optionally, path to the certificate to be revoked. /nsconfig/ssl/ is the default path. Maximum value: 63

genCRL

Name of and, optionally, path to the CRL file to be generated. The list of certificates that have been revoked is obtained from the index file. /nsconfig/ssl/ is the default path. Maximum value: 63

password

Password for the CA key file. Maximum value: 31

Example

```
1)      create_crl /nsconfig/ssl/cacert.pem /
nsconfig/ssl/cakey.pem /nsconfig/ssl/index.txt -
gencrl /var/netScaler/ssl/crl.pem
```

[Top](#)

rm ssl crl

Synopsis

rm ssl crl <crlName> ...

Description

Removes the specified CRL from the appliance.

Parameters

crlName

Name of the CRL to remove.

Example

```
1)      rm ssl crl ca_crl
The above CLI command to delete the CRL object
ca_crl from the system is.
```

[Top](#)

set ssl crl

Synopsis

```
set ssl crl <crlName> [-refresh ( ENABLED | DISABLED )] [-CAcert <string>] [-server
<ip_addr|ipv6_addr|*> | -url <URL>] [-method ( HTTP | LDAP )] [-port <port>] [-baseDN
<string>] [-scope ( Base | One )] [-interval <interval>] [-day <integer>] [-time <HH:MM>]
[-bindDN <string>] {-password } [-binary ( YES | NO )]
```

Description

Modifies all the parameters of a CRL, except the CRL name and method.

Parameters

crlName

Name of the CRL to be modified.

refresh

Set CRL auto refresh. Possible values: ENABLED, DISABLED

CAcert

CA certificate that has issued the CRL. Required if CRL Auto Refresh is selected. Install the CA certificate on the appliance before adding the CRL.

server

IP address of the LDAP server from which to fetch the CRLs.

method

Method for CRL refresh. If LDAP is selected, specify the method, CA certificate, base DN, port, and LDAP server name. If HTTP is selected, specify the CA certificate, method, URL, and port. Cannot be changed after a CRL is added. Possible values: HTTP, LDAP

port

Port for the LDAP server. Minimum value: 1

baseDN

Base distinguished name (DN), which is used in an LDAP search to search for a CRL. Citrix recommends searching for the Base DN instead of the Issuer Name from the CA certificate, because the Issuer Name field might not exactly match the LDAP directory structure's DN.

scope

Extent of the search operation on the LDAP server. Available settings function as follows: One - One level below Base DN. Base - Exactly the same level as Base DN. Possible values: Base, One Default value: NSAPI_ONESCOPE

interval

CRL refresh interval. Use the NONE setting to unset this parameter. Possible values: MONTHLY, WEEKLY, DAILY, NOW, NONE

day

Day on which to refresh the CRL, or, if the Interval parameter is not set, the number of days after which to refresh the CRL. If Interval is set to MONTHLY, specify the date. If Interval is set to WEEKLY, specify the day of the week (for example, Sun=0 and Sat=6). This parameter is not applicable if the Interval is set to DAILY. Maximum value: 31

time

Time, in hours (1-24) and minutes (1-60), at which to refresh the CRL.

bindDN

Bind distinguished name (DN) to be used to access the CRL object in the LDAP repository if access to the LDAP repository is restricted or anonymous access is not allowed.

password

Password to access the CRL in the LDAP repository if access to the LDAP repository is restricted or anonymous access is not allowed.

binary

Set the LDAP-based CRL retrieval mode to binary. Possible values: YES, NO Default value: NO

Example

```
1)    set ssl crl crl_file -refresh ENABLE -
interval MONTHLY -days 10 -time 12:00
The above example sets the CRL refresh to every
Month, on date=10, and time=12:00hrs.
2)    set ssl crl crl_file -refresh ENABLE -
interval WEEKLY -days 1 -time 00:10
The above example sets the CRL refresh every Week,
on weekday=Monday, and at time 10 past midnight.
3)    set ssl crl crl_file -refresh ENABLE -
interval DAILY -days 1 -time 12:00
The above example sets the CRL refresh every Day,
at 12:00hrs.
4)    set ssl crl crl_file -refresh ENABLE -days 10
The above example sets the CRL refresh after every
10 days.
Note: The CRL will be refreshed after every 10
days. The time for CRL refresh will be 00:00 hrs.
5)    set ssl crl crl_file -refresh ENABLE -time
01:00
The above example sets the CRL refresh after every
1 hour.
6)    set ssl crl crl_file -refresh ENABLE -
interval NOW
The above example sets the CRL refresh
instantaneously.
```

[Top](#)

unset ssl crl

Synopsis

```
unset ssl crl <crlName> [-refresh] [-CAcert] [-server] [-method] [-url] [-port] [-baseDN]
[-scope] [-interval] [-day] [-time] [-bindDN] [-password] [-binary]
```

Description

Use this command to remove ssl crl settings. Refer to the set ssl crl command for meanings of the arguments.

[Top](#)

show ssl crl

Synopsis

```
show ssl crl [<crlName>]
```

Description

Displays information about all the CRLs configured on the appliance, or displays detailed information about the specified CRL.

Parameters

crlName

Name of the CRL for which to show detailed information.

Example

```

1) An example output of the show ssl crl command
is as follows:
1 configured CRL(s)
1 Name: ca_crl
CRL Path: /var/netscaler/ssl/crl.der
Format: DER Cacert: ca_cert
Refresh: DISABLED

2) An example of the output of the show ssl crl
ca_crl command is as follows:
Name: ca_crl Status: Valid, Days to expiration: 21
CRL Path: /var/netscaler/ssl/crl.der
Format: DER    Cacert: ca_cert
Refresh: DISABLED
Version: 1
Signature Algorithm: md5WithRSAEncryption
Issuer: /C=US/ST=CA/L=santa clara /O=CA/OU=security
Last_update:Dec 21 09:47:16 2001 GMT
Next_update:Jan 20 09:47:16 2002 GMT
Revoked Certificates:
    Serial Number: 01
    Revocation Date:Dec 21 09:47:02 2001 GMT
    Serial Number: 02
    Revocation Date:Dec 21 09:47:02 2001 GMT

```

[Top](#)

ssl action

[[add](#) | [rm](#) | [show](#)]

add ssl action

Synopsis

```

add ssl action <name> [-clientAuth ( DOCLIENTAUTH | NOCLIENTAUTH )] [-clientCert
( ENABLED | DISABLED ) -certHeader <string>] [-clientCertSerialNumber ( ENABLED |
DISABLED ) -certSerialHeader <string>] [-clientCertSubject ( ENABLED | DISABLED ) -
certSubjectHeader <string>] [-clientCertHash ( ENABLED | DISABLED ) -certHashHeader
<string>] [-clientCertIssuer ( ENABLED | DISABLED ) -certIssuerHeader <string>] [-
sessionID ( ENABLED | DISABLED ) -sessionIDHeader <string>] [-cipher ( ENABLED |
DISABLED ) -cipherHeader <string>] [-clientCertNotBefore ( ENABLED | DISABLED ) -
certNotBeforeHeader <string>] [-clientCertNotAfter ( ENABLED | DISABLED ) -
certNotAfterHeader <string>] [-OWASupport ( ENABLED | DISABLED )]

```

Description

Creates a new SSL action. An SSL action defines SSL settings that you can apply to the selected requests. You associate an action with one or more policies. Data in client connection requests or responses is compared to a rule (expression) specified in the policy, and the action is applied to connections that match the rule.

Parameters

name

Name for the SSL action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the action is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

clientAuth

Perform client certificate authentication. Possible values: DOCLIENTAUTH, NOCLIENTAUTH

clientCert

Insert the entire client certificate into the HTTP header of the request being sent to the web server. The certificate is inserted in ASCII (PEM) format. Possible values: ENABLED, DISABLED

clientCertSerialNumber

Insert the entire client serial number into the HTTP header of the request being sent to the web server. Possible values: ENABLED, DISABLED

clientCertSubject

Insert the client certificate subject, also known as the distinguished name (DN), into the HTTP header of the request being sent to the web server. Possible values: ENABLED, DISABLED

clientCertHash

Insert the certificate signature (hash) into the HTTP header of the request being sent to the web server. Possible values: ENABLED, DISABLED

clientCertIssuer

Insert the certificate issuer details into the HTTP header of the request being sent to the web server. Possible values: ENABLED, DISABLED

sessionID

Insert the SSL session ID into the HTTP header of the request being sent to the web server. Every SSL connection that the client and the NetScaler share has a unique ID that identifies the specific connection. Possible values: ENABLED, DISABLED

cipher

Insert the cipher suite that the client and the NetScaler appliance negotiated for the SSL session into the HTTP header of the request being sent to the web server. The appliance inserts the cipher-suite name, SSL protocol, export or non-export string, and cipher strength bit, depending on the type of browser connecting to the SSL

virtual server or service (for example, Cipher-Suite: RC4- MD5 SSLv3 Non-Export 128-bit). Possible values: ENABLED, DISABLED

clientCertNotBefore

Insert the date from which the certificate is valid into the HTTP header of the request being sent to the web server. Every certificate is configured with the date and time from which it is valid. Possible values: ENABLED, DISABLED

clientCertNotAfter

Insert the date of expiry of the certificate into the HTTP header of the request being sent to the web server. Every certificate is configured with the date and time at which the certificate expires. Possible values: ENABLED, DISABLED

OWASupport

If the appliance is in front of an Outlook Web Access (OWA) server, insert a special header field, FRONT-END-HTTPS: ON, into the HTTP requests going to the OWA server. This header communicates to the server that the transaction is HTTPS and not HTTP. Possible values: ENABLED, DISABLED

Example

```
add ssl action certInsert_act -clientCert ENABLED -
certHeader CERT
```

[Top](#)

rm ssl action

Synopsis

```
rm ssl action <name>
```

Description

Removes the specified SSL action.

Parameters

name

Name of the SSL action to remove.

Example

```
rm ssl action certInsert_act
```

[Top](#)

show ssl action

Synopsis

```
show ssl action [<name>]
```

Description

Displays information about all the SSL actions configured on the appliance, or displays detailed information about the specified SSL action.

Parameters

name

Name of the SSL action for which to show detailed information.

Example

```
show ssl action
1 Configured SSL action:
1)      Name: certInsert_act
        Data Insertion Action:
        Cert Header: ENABLED          Cert Tag:
CERT
```

[Top](#)

ssl policy

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add ssl policy

Synopsis

```
add ssl policy <name> -rule <expression> [-action <string>] [-undefAction <string>] [-comment <string>]
```

Description

Adds an SSL policy. An SSL policy evaluates incoming traffic and applies a predefined action to requests that match a rule (expression). You have to configure the actions before creating the policies, so that you can specify an action when you create a policy.

Parameters

name

Name for the new SSL policy. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the policy is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy').

rule

Expression, against which traffic is evaluated. Written in the classic or default syntax. Note: Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-

character string as follows: "<string of 255 characters>" + "<string of 245 characters>" (Classic expressions are not supported in the cluster build.) The following requirements apply only to the NetScaler CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

reqAction

The name of the action to be performed on the request. Refer to 'add ssl action' command to add a new action. Builtin actions like NOOP, RESET, DROP, CLIENTAUTH and NOCLIENTAUTH are also allowed.

action

Name of the built-in or user-defined action to perform on the request. Available built-in actions are NOOP, RESET, DROP, CLIENTAUTH, and NOCLIENTAUTH.

undefAction

Name of the action to be performed when the result of rule evaluation is undefined. Possible values for control policies: CLIENTAUTH, NOCLIENTAUTH, NOOP, RESET, DROP. Possible values for data policies: NOOP, RESET or DROP.

comment

Any comments associated with this policy.

Example

```
add ssl action certInsert_act -clientCert ENABLED -
certHeader CERT
    add ssl policy certInsert_pol -rule
'HTTP.REQ.URL.STARTSWITH("/secure/")' -reqAction
certInsert_act
The above example adds an SSL policy to do Client
certificate insertion into the HTTP requests for
any web-objects under /secure/.
```

[Top](#)

rm ssl policy**Synopsis**

```
rm ssl policy <name>
```

Description

Removes an SSL policy.

Parameters**name**

Name of the SSL policy to be removed.

Example

```
rm ssl policy certInsert_pol
```

[Top](#)

set ssl policy

Synopsis

```
set ssl policy <name> [-rule <expression>] [-action <string>] [-undefAction <string>] [-comment <string>]
```

Description

Modifies the parameters of an SSL default syntax policy.

Parameters

name

Name of the SSL policy to modify.

rule

Expression, against which traffic is evaluated. Written in the classic or default syntax. Note: Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>" (Classic expressions are not supported in the cluster build.) The following requirements apply only to the NetScaler CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action

Name of the built-in or user-defined action to perform on the request. Available built-in actions are NOOP, RESET, DROP, CLIENTAUTH, and NOCLIENTAUTH.

undefAction

Name of the action to be performed when the result of rule evaluation is undefined. Possible values for control policies: CLIENTAUTH, NOCLIENTAUTH, NOOP, RESET, DROP. Possible values for data policies: NOOP, RESET or DROP.

comment

Any comments associated with this policy.

Example

```
set ssl policy poll -rule "HTTP.REQ.HEADER(\n\nheader\\").CONTAINS(\\\"qh2\\\") "
```

[Top](#)

unset ssl policy

Synopsis

unset ssl policy <name> [-undefAction] [-comment]

Description

Removes the attributes of an SSL default syntax policy. Attributes for which a default value is available revert to their default values. Refer to the set ssl policy command for a description of the parameters..Refer to the set ssl policy command for meanings of the arguments.

Example

```
unset ssl policy poll -undefAction
```

[Top](#)

show ssl policy

Synopsis

show ssl policy [<name>]

Description

Displays information about all the SSL policies configured on the appliance, or displays detailed information about the specified SSL policy.

Parameters

name

Name of the SSL policy for which to display detailed information.

Example

```
show ssl policy
1 SSL policy:
1)      Name: certInsert_pol      Rule: URL == /*
      Action: certInsert_act      Hits: 0
```

[Top](#)

ssl policylabel

[[add](#) | [rm](#) | [bind](#) | [unbind](#) | [show](#)]

add ssl policylabel

Synopsis

add ssl policylabel <labelName> -type (CONTROL | DATA)

Description

Creates an SSL policy label. An SSL policy label can be a control label or a data label.

Parameters

labelName

Name for the SSL policy label. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the policy label is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my label" or 'my label').

type

Type of policies that the policy label can contain. Possible values: CONTROL, DATA

Example

```
add ssl policylabel ssl_pol_label -type REQ
```

[Top](#)

rm ssl policylabel

Synopsis

rm ssl policylabel <labelName>

Description

Removes an SSL policy label.

Parameters

labelName

Name of the SSL policy label to remove.

Example

```
rm ssl policylabel ssl_pol_label
```

[Top](#)

bind ssl policylabel

Synopsis

```
bind ssl policylabel <labelName> <policyName> <priority> [<gotoPriorityExpression>] [-  
invoke (<labelType> <labelName>)]
```

Description

Binds an SSL policy to an SSL policy label and specifies the order in which the policies in the label are to be evaluated.

Parameters

labelName

Name of the SSL policy label to which to bind policies.

policyName

Name of the SSL policy to bind to the policy label.

Example

```
bind ssl policylabel ssl_pol_label -policyName  
ssl_pol -priority 1
```

[Top](#)

unbind ssl policylabel

Synopsis

```
unbind ssl policylabel <labelName> <policyName> [-priority <positive_integer>]
```

Description

Unbinds an SSL policy from an SSL policy label.

Parameters

labelName

Name of the SSL policy label from which to unbind policies.

policyName

Name of the SSL policy to unbind.

Example

```
unbind ssl policylabel ssl_pol_label ssl_pol
```

[Top](#)

show ssl polyclabel

Synopsis

show ssl polyclabel [<labelName>]

Description

Displays information about all the SSL policy labels, or displays detailed information about the specified policy label.

Parameters

labelName

Name of the SSL policy label for which to show detailed information.

Example

```
i)    show ssl polyclabel ssl_pol_label
ii)   show ssl polyclabel
```

[Top](#)

ssl ocsponder

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add ssl ocsponder

Synopsis

add ssl ocsponder <name> -url <URL> [-cache (ENABLED | DISABLED) [-cacheTimeout <positive_integer>]] [-batchingDepth <positive_integer>] [-batchingDelay <positive_integer>] [-resptimeout <positive_integer>] [-responderCert <string> | -trustResponder] [-producedAtTimeSkew <positive_integer>] [-signingCert <string>] [-useNonce (YES | NO)] [-insertClientCert (YES | NO)]

Description

Adds an OCSP responder. An OCSP responder identifies the OCSP server that validates a certificate. NetScaler appliances support OCSP as defined in RFC 2560.

Parameters

name

Name for the OCSP responder. Cannot begin with a hash (#) or space character and must contain only ASCII alphanumeric, underscore (_), hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the responder is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my responder" or 'my responder').

url

URL of the OCSP responder.

cache

Enable caching of responses. Caching of responses received from the OCSP responder enables faster responses to the clients and reduces the load on the OCSP responder. Possible values: ENABLED, DISABLED

cacheTimeout

Timeout for caching the OCSP response. After the timeout, the NetScaler sends a fresh request to the OCSP responder for the certificate status. If a timeout is not specified, the timeout provided in the OCSP response applies. Default value: 1 Minimum value: 1 Maximum value: 1440

batchingDepth

Number of client certificates to batch together into one OCSP request. Batching avoids overloading the OCSP responder. A value of 1 signifies that each request is queried independently. For a value greater than 1, specify a timeout (batching delay) to avoid inordinately delaying the processing of a single certificate. Minimum value: 1 Maximum value: 8

batchingDelay

Maximum time, in milliseconds, to wait to accumulate OCSP requests to batch. Does not apply if the Batching Depth is 1. Maximum value: 10000

resptimeout

Time, in milliseconds, to wait for an OCSP response. When this time elapses, an error message appears or the transaction is forwarded, depending on the settings on the virtual server. Includes Batching Delay time. Maximum value: 120000

producedAtTimeSkew

Time, in seconds, for which the NetScaler waits before considering the response as invalid. The response is considered invalid if the Produced At time stamp in the OCSP response exceeds or precedes the current NetScaler clock time by the amount of time specified. Default value: 300 Maximum value: 86400

signingCert

Certificate-key pair that is used to sign OCSP requests. If this parameter is not set, the requests are not signed.

useNonce

Enable the OCSP nonce extension, which is designed to prevent replay attacks. Possible values: YES, NO

insertClientCert

Include the complete client certificate in the OCSP request. Possible values: YES, NO

Example

```
1) add ssl ocsponder -url http://
   ocsponder.example.com -producedAtTimeSkew 0
The above command will only allow responses that
were generated in the same second to be used.
That is, if the response was generated at
12:00:01, it would have to be received by the
NetScaler by 12:00:59 to be considered still valid.
2) add ssl ocsponder -url http://
```

```
ocsp.example.com -producedAtTimeSkew 300
This command will allow responses to vary up to
five minutes plus or minus. That is, if the
response has a producedAt time of 12:00:00, it
will be accepted at the NetScaler if the local
clock is between 11:55:00 and 12:05:00
```

[Top](#)

rm ssl ocspResponder

Synopsis

rm ssl ocspResponder <name> ...

Description

Removes the specified OCSP responder from the appliance.

Parameters

name

Name of the OCSP responder to remove. The OCSP responder is removed only if it is not referenced by any other object.

Example

```
1)      rm ssl ocspResponder o1
The above command removes the OCSP responder o1
from the system.
```

[Top](#)

set ssl ocspResponder

Synopsis

set ssl ocspResponder <name> [-url <URL>] [-cache (ENABLED | DISABLED)] [-cacheTimeout <positive_integer>] [-batchingDepth <positive_integer>] [-batchingDelay <positive_integer>] [-resptimeout <positive_integer>] [-responderCert <string> | -trustResponder] [-producedAtTimeSkew <positive_integer>] [-signingCert <string>] [-useNonce (YES | NO)] [-insertClientCert (YES | NO)]

Description

Modifies the parameters of an OCSP responder.

Parameters

name

Name of the OCSP responder to modify.

url

URL of the OCSP responder.

cache

Enable caching of responses. Caching of responses received from the OCSP responder enables faster responses to the clients and reduces the load on the OCSP responder. Possible values: ENABLED, DISABLED

cacheTimeout

Timeout for caching the OCSP response. After the timeout, the NetScaler sends a fresh request to the OCSP responder for the certificate status. If a timeout is not specified, the timeout provided in the OCSP response applies. Default value: 1 Minimum value: 1 Maximum value: 1440

batchingDepth

Number of client certificates to batch together into one OCSP request. Batching avoids overloading the OCSP responder. A value of 1 signifies that each request is queried independently. For a value greater than 1, specify a timeout (batching delay) to avoid inordinately delaying the processing of a single certificate. Minimum value: 1 Maximum value: 8

batchingDelay

Maximum time, in milliseconds, to wait to accumulate OCSP requests to batch. Does not apply if the Batching Depth is 1. Maximum value: 10000

resptimeout

Time, in milliseconds, to wait for an OCSP response. When this time elapses, an error message appears or the transaction is forwarded, depending on the settings on the virtual server. Includes Batching Delay time. Maximum value: 120000

producedAtTimeSkew

Time, in seconds, for which the NetScaler waits before considering the response as invalid. The response is considered invalid if the Produced At time stamp in the OCSP response exceeds or precedes the current NetScaler clock time by the amount of time specified. Default value: 300 Maximum value: 86400

signingCert

Certificate-key pair that is used to sign OCSP requests. If this parameter is not set, the requests are not signed.

useNonce

Enable the OCSP nonce extension, which is designed to prevent replay attacks. Possible values: YES, NO

insertClientCert

Include the complete client certificate in the OCSP request. Possible values: YES, NO

Example

```
1) add ssl ocsponder -url http://
   ocsponder.example.com -producedAtTimeSkew 0
The above command will only allow responses that
were generated in the same second to be used.
That is, if the response was generated at
12:00:01, it would have to be received by the
NetScaler by 12:00:59 to be considered still valid.
2) add ssl ocsponder -url http://
```

```
ocsp.example.com -producedAtTimeSkew 300
This command will allow responses to vary up to
five minutes plus or minus. That is, if the
response has a producedAt time of 12:00:00, it
will be accepted at the NetScaler if the local
clock is between 11:55:00 and 12:05:00
```

[Top](#)

unset ssl ocspResponder

Synopsis

```
unset ssl ocspResponder <name> [-trustResponder] [-insertClientCert ( YES | NO )] [-
cache] [-cacheTimeout] [-batchingDepth] [-batchingDelay] [-resptimeout] [-
responderCert] [-producedAtTimeSkew] [-signingCert] [-useNonce]
```

Description

Removes the attributes of an OCSP responder. Attributes for which a default value is available revert to their default values. Refer to the set ssl ocspResponder command for descriptions of the arguments..Refer to the set ssl ocspResponder command for meanings of the arguments.

[Top](#)

show ssl ocspResponder

Synopsis

```
show ssl ocspResponder [<name>]
```

Description

Displays information about all the OCSP responders configured on the appliance, or displays detailed information about the specified OCSP responder.

Parameters

name

Name of the OCSP responder for which to show detailed information.

[Top](#)

ssl rsakey

create ssl rsakey

Synopsis

```
create ssl rsakey <keyFile> <bits> [-exponent ( 3 | F4 )] [-keyform ( DER | PEM )] [-des
| -des3] {-password }
```

Description

Generates an RSA key.

Parameters

keyFile

Name for and, optionally, path to the RSA key file. /nsconfig/ssl/ is the default path.
Maximum value: 63

bits

Size, in bits, of the RSA key. Minimum value: 512 Maximum value: 4096

exponent

Public exponent for the RSA key. The exponent is part of the cipher algorithm and is required for creating the RSA key. Possible values: 3, F4 Default value: FIPSEXP_F4

keyform

Format in which the RSA key file is stored on the appliance. Possible values: DER, PEM Default value: FORMAT_PEM

des

Encrypt the generated RSA key by using the DES algorithm. On the command line, you are prompted to enter the pass phrase (password) that is used to encrypt the key.

des3

Encrypt the generated RSA key by using the Triple-DES algorithm. On the command line, you are prompted to enter the pass phrase (password) that is used to encrypt the key.

password

Pass phrase to use for encryption if DES or DES3 option is selected. Maximum value: 31

Example

```
create ssl rsakey /nsconfig/ssl/rsa1024.pem 1024 -
exp F4
```

ssl pkcs12

convert ssl pkcs12

Synopsis

```
convert ssl pkcs12 <outfile> [-import [-pkcs12File <input_filename>] [-des | -des3] ] [-
export [-certFile <input_filename>] [-keyFile <input_filename>]] {-password } {-
PEMPassPhrase }
```

Description

Converts the end-user certificate from PEM encoding format to PKCS#12 format. This certificate can then be distributed and installed in browsers as client certificates.

Parameters

outfile

Name for and, optionally, path to, the output file that contains the certificate and the private key after converting from PKCS#12 to PEM format. /nsconfig/ssl/ is the default path. If importing, the certificate-key pair is stored in PEM format. If exporting, the certificate-key pair is stored in PKCS#12 format. Maximum value: 63

import

Convert the certificate and private-key from PKCS#12 format to PEM format.

export

Convert the certificate and private key from PEM format to PKCS#12 format. On the command line, you are prompted to enter the pass phrase.

Example

```
1)    convert ssl pkcs12 /nsconfig/ssl/
      client_certkey.p12 -export -cert /nsconfig/ssl/
      client_certcert.pem -key /nsconfig/ssl/
      client_key.pem
The above example CLI command converts the PEM
encoded certificate and key file to PKCS#12.
2)    convert ssl pkcs12 /nsconfig/ssl/
      client_certkey.pem -import -pkcs12 /nsconfig/ssl/
      client_certcertkey.p12
The above example CLI command converts the PKCS12
file to PEM format.
3)    convert ssl pkcs12 /nsconfig/ssl/
      client_certkey.pem -import -pkcs12 /nsconfig/ssl/
      client_certcertkey.p12 -des
The above example CLI command converts the PKCS12
file to PEM format, with encrypted key.

Note:    The -des option will encrypt the output
key using DES algorithm. User will be prompted to
enter the pass-phrase to be used for encryption.
```

ssl pkcs8

convert ssl pkcs8

Synopsis

```
convert ssl pkcs8 <pkcs8File> <keyFile> [-keyform ( DER | PEM )] {-password }
```

Description

Convert a PEM or DER format key file to PKCS#8 format before importing it into the FIPS appliance.

Parameters

pkcs8File

Name for and, optionally, path to, the output file where the PKCS#8 format key file is stored. /nsconfig/ssl/ is the default path. Maximum value: 63

keyFile

Name of and, optionally, path to the input key file to be converted from PEM or DER format to PKCS#8 format. /nsconfig/ssl/ is the default path. Maximum value: 63

keyform

Format in which the key file is stored on the appliance. Possible values: DER, PEM
Default value: FORMAT_PEM

password

Password to assign to the file if the key is encrypted. Applies only for PEM format files. Maximum value: 31

Example

```
convert ssl pkcs8 /nsconfig/ssl/key.pk8 /  
nsconfig/ssl/key.pem
```

ssl dhParam

create ssl dhParam

Synopsis

```
create ssl dhParam <dhFile> [<bits>] [-gen ( 2 | 5 )]
```

Description

Generates a Diffie-Hellman (DH) key.

Parameters

dhFile

Name of and, optionally, path to the DH key file. /nsconfig/ssl/ is the default path.
Maximum value: 63

bits

Size, in bits, of the DH key being generated. Minimum value: 512 Maximum value: 2048

gen

Random number required for generating the DH key. Required as part of the DH key generation algorithm. Possible values: 2, 5 Default value: 2

Example

```
1)      create ssl dhparam /nsconfig/ssl/dh1024.pem
1024 -gen 5
```

ssl dsaKey

create ssl dsaKey

Synopsis

```
create ssl dsaKey <keyFile> <bits> [-keyform ( DER | PEM )] [-des | -des3] {-password }
```

Description

Generates a DSA key.

Parameters

keyFile

Name for and, optionally, path to the DSA key file. /nsconfig/ssl/ is the default path.
Maximum value: 63

bits

Size, in bits, of the DSA key. Minimum value: 512 Maximum value: 2048

keyform

Format in which the DSA key file is stored on the appliance. Possible values: DER, PEM Default value: FORMAT_PEM

des

Encrypt the generated DSA key by using the DES algorithm. On the command line, you are prompted to enter the pass phrase (password) that will be used to encrypt the key.

des3

Encrypt the generated DSA key by using the Triple-DES algorithm. On the command line, you are prompted to enter the pass phrase (password) that will be used to encrypt the key.

password

Pass phrase to use for encryption if DES or DES3 option is selected. Maximum value: 31

Example

```
create ssl dsakey /nsconfig/ssl/dsa1024.pem 1024
```

ssl certLink

show ssl certLink

Synopsis

show ssl certLink

Description

Displays information about all the linked certificate-key pairs on the appliance.

Example

```
The following shows an example of the output of
the show ssl certlink command:
linked certificate:
1) Cert Name: siteAcertkey CA Cert Name: CAcertkey
```

ssl certReq

create ssl certReq

Synopsis

```
create ssl certReq <reqFile> (-keyFile <input_filename> | -fipsKeyName <string>) [-
keyform ( DER | PEM ) {-PEMPassPhrase }] -countryName <string> -stateName <string> -
organizationName <string> [-organizationUnitName <string>] [-localityName <string>] [-
commonName <string>] [-emailAddress <string>] {-challengePassword } [-companyName
<string>]
```

Description

Generates a new Certificate Signing Request (CSR). A CSR is a collection of information including the domain name, company details, and the private key to be used to create the certificate. Send the CSR to a Certificate Authority (CA) to obtain an X509 certificate for the user domain (web site).

Parameters

reqFile

Name for and, optionally, path to the certificate signing request (CSR). /nsconfig/ssl/ is the default path. Maximum value: 63

keyFile

Name of and, optionally, path to the private key used to create the certificate signing request, which then becomes part of the certificate-key pair. The private key can be either an RSA or a DSA key. The key must be present in the appliance's local storage. /nsconfig/ssl is the default path. Maximum value: 63

fipsKeyName

Name of the FIPS key used to create the certificate signing request. FIPS keys are created inside the Hardware Security Module of the FIPS card.

keyform

Format in which the key is stored on the appliance. Possible values: DER, PEM Default value: FORMAT_PEM

countryName

Two letter ISO code for your country. For example, US for United States.

stateName

Full name of the state or province where your organization is located. Do not abbreviate.

organizationName

Name of the organization that will use this certificate. The organization name (corporation, limited partnership, university, or government agency) must be registered with some authority at the national, state, or city level. Use the legal name under which the organization is registered. Do not abbreviate the organization name and do not use the following characters in the name: Angle brackets (< >) tilde (~), exclamation mark, at (@), pound (#), zero (0), caret (^), asterisk (*), forward slash (/), square brackets ([]), question mark (?).

organizationUnitName

Name of the division or section in the organization that will use the certificate.

localityName

Name of the city or town in which your organization's head office is located.

commonName

Fully qualified domain name for the company or web site. The common name must match the name used by DNS servers to do a DNS lookup of your server. Most browsers use this information for authenticating the server's certificate during the SSL handshake. If the server name in the URL does not match the common name as given in the server certificate, the browser terminates the SSL handshake or prompts the user with a warning message. Do not use wildcard characters, such as asterisk (*) or question mark (?), and do not use an IP address as the common name. The common name must not contain the protocol specifier <http://> or <https://>.

emailAddress

Contact person's e-mail address. This address is publically displayed as part of the certificate. Provide an e-mail address that is monitored by an administrator who can be contacted about the certificate.

challengePassword

Pass phrase, embedded in the certificate signing request that is shared only between the client or server requesting the certificate and the SSL certificate issuer (typically the certificate authority). This pass phrase can be used to authenticate a client or server that is requesting a certificate from the certificate authority.

companyName

Additional name for the company or web site.

Example

```
create ssl certreq /nsconfig/ssl/csr.pem -keyFile /
nsconfig/ssl/rsa1024.pem
```

ssl cert

create ssl cert

Synopsis

```
create ssl cert <certFile> <reqFile> <certType> [-keyFile <input_filename>] [-keyform
( DER | PEM ) {-PEMPassPhrase }}] [-days <positive_integer>] [-certForm ( DER | PEM )] [-
CAcert <input_filename>] [-CAcertForm ( DER | PEM )] [-CAkey <input_filename>] [-
CAkeyForm ( DER | PEM )] [-CAserial <output_filename>]
```

Description

Generates a signed X509 Certificate.

Parameters

certFile

Name for and, optionally, path to the generated certificate file. /nsconfig/ssl/ is the default path. Maximum value: 63

reqFile

Name for and, optionally, path to the certificate-signing request (CSR). /nsconfig/ssl/ is the default path. Maximum value: 63

certType

Type of certificate to generate. Specify one of the following: * ROOT_CERT - Self-signed Root-CA certificate. You must specify the key file name. The generated Root-CA certificate can be used for signing end-user client or server certificates or to create Intermediate-CA certificates. * INTM_CERT - Intermediate-CA certificate. * CLNT_CERT - End-user client certificate used for client authentication. * SRVR_CERT - SSL server certificate used on SSL servers for end-to-end encryption. Possible values: ROOT_CERT, INTM_CERT, CLNT_CERT, SRVR_CERT

keyFile

Name for and, optionally, path to the private key. You can either use an existing RSA or DSA key that you own or create a new private key on the NetScaler appliance. This file is required only when creating a self-signed Root-CA certificate. The key file is stored in the /nsconfig/ssl directory by default. If the input key specified is an encrypted key, you are prompted to enter the PEM pass phrase that was used for encrypting the key. Maximum value: 63

keyform

Format in which the key is stored on the appliance. Possible values: DER, PEM Default value: FORMAT_PEM

days

Number of days for which the certificate will be valid, beginning with the time and day (system time) of creation. Default value: 365 Minimum value: 1 Maximum value: 3650

certForm

Format in which the certificate is stored on the appliance. Possible values: DER, PEM
Default value: FORMAT_PEM

CAcert

Name of the CA certificate file that issues and signs the Intermediate-CA certificate or the end-user client and server certificates. Maximum value: 63

CAcertForm

Format of the CA certificate. Possible values: DER, PEM Default value: FORMAT_PEM

CAkey

Private key, associated with the CA certificate that is used to sign the Intermediate-CA certificate or the end-user client and server certificate. If the CA key file is password protected, the user is prompted to enter the pass phrase that was used to encrypt the key. Maximum value: 63

CAkeyForm

Format for the CA certificate. Possible values: DER, PEM Default value: FORMAT_PEM

CAserial

Serial number file maintained for the CA certificate. This file contains the serial number of the next certificate to be issued or signed by the CA. If the specified file does not exist, a new file is created, with /nsconfig/ssl/ as the default path. If you do not specify a proper path for the existing serial file, a new serial file is created. This might change the certificate serial numbers assigned by the CA certificate to each of the certificates it signs. Maximum value: 63

Example

```
1) create ssl cert /nsconfig/ssl/root_cert.pem /
nsconfig/ssl/root_csr.pem ROOT_CERT -keyFile /
nsconfig/ssl/root_key.pem -days 1000
The above example creates a self signed Root-CA
certificate.
2) create ssl cert /nsconfig/ssl/server_cert.pem /
nsconfig/ssl/server_csr.pem SRVR_CERT -CAcert /
nsconfig/ssl/root_cert.pem -CAkey /nsconfig/ssl/
root_key.pem -CAserial /nsconfig/ssl/root.srl
The above example creates a Server certificate
which is signed by the Root-CA certificate:
root_cert.pem
```

ssl stats

show ssl stats

Synopsis

show ssl stats - alias for 'stat ssl'

Description

show ssl stats is an alias for stat ssl

ssl parameter

[[set](#) | [unset](#) | [show](#)]

set ssl parameter

Synopsis

```
set ssl parameter [-quantumSize <quantumSize>] [-crlMemorySizeMB
<positive_integer>] [-strictCAChecks ( YES | NO )] [-sslTriggerTimeout
<positive_integer>] [-sendCloseNotify ( YES | NO )] [-encryptTriggerPktCount
<positive_integer>] [-denySSLReneg <denySSLReneg>] [-insertionEncoding ( Unicode |
UTF-8 )] [-ocspCacheSize <positive_integer>] [-pushFlag <positive_integer>] [-
dropReqWithNoHostHeader ( YES | NO )] [-pushEncTriggerTimeout <positive_integer>] [-
undefActionCode <string>] [-undefActionData <string>]
```

Parameters

quantumSize

Amount of data to collect before the data is pushed to the crypto hardware for encryption. For large downloads, a larger quantum size better utilizes the crypto resources. Possible values: 4096, 8192, 16384 Default value: 8192

crlMemorySizeMB

Maximum memory size to use for certificate revocation lists (CRLs). This parameter reserves memory for a CRL but sets a limit to the maximum memory that the CRLs loaded on the appliance can consume. Default value: 256 Minimum value: 10 Maximum value: 1024

strictCAChecks

Enable strict CA certificate checks on the appliance. Possible values: YES, NO Default value: NO

sslTriggerTimeout

Time, in milliseconds, after which encryption is triggered for transactions that are not tracked on the NetScaler appliance because their length is not known. There can be a delay of up to 10ms from the specified timeout value before the packet is pushed into the queue. Default value: 100 Minimum value: 1 Maximum value: 200

sendCloseNotify

Send an SSL Close-Notify message to the client at the end of a transaction. Possible values: YES, NO Default value: YES

encryptTriggerPktCount

Maximum number of queued packets after which encryption is triggered. Use this setting for SSL transactions that send small packets from server to NetScaler. Default value: 45 Minimum value: 10 Maximum value: 50

denySSLReneg

Deny renegotiation in specified circumstances. Available settings function as follows:
* NO - Allow SSL renegotiation. * FRONTEND_CLIENT - Deny secure and nonsecure SSL renegotiation initiated by the client. * FRONTEND_CLIENTSERVER - Deny secure and nonsecure SSL renegotiation initiated by the client or the NetScaler during policy-based client authentication. * ALL - Deny all secure and nonsecure SSL renegotiation. * NONSECURE - Deny nonsecure SSL renegotiation. Allows only clients that support RFC 5746. Possible values: NO, FRONTEND_CLIENT, FRONTEND_CLIENTSERVER, ALL, NONSECURE Default value: NO

insertionEncoding

Encoding method used to insert the subject or issuer's name in HTTP requests to servers. Possible values: Unicode, UTF-8 Default value: UNICODE_INSERTION

ocspCacheSize

Size, per packet engine, in megabytes, of the OCSP cache. A maximum of 10% of the packet engine memory can be assigned. Because the maximum allowed packet engine memory is 4GB, the maximum value that can be assigned to the OCSP cache is approximately 410 MB. Default value: 10 Maximum value: 512

pushFlag

Insert PUSH flag into decrypted, encrypted, or all records. If the PUSH flag is set to a value other than 0, the buffered records are forwarded on the basis of the value of the PUSH flag. Available settings function as follows: 0 - Auto (PUSH flag is not set.) 1 - Insert PUSH flag into every decrypted record. 2 - Insert PUSH flag into every encrypted record. 3 - Insert PUSH flag into every decrypted and encrypted record. Maximum value: 3

dropReqWithNoHostHeader

Host header check for SNI enabled sessions. If this check is enabled and the HTTP request does not contain the host header for SNI enabled sessions, the request is dropped. Possible values: YES, NO Default value: NO

pushEncTriggerTimeout

PUSH encryption trigger timeout value. The timeout value is applied only if you set the Push Encryption Trigger parameter to Timer in the SSL virtual server settings. Default value: 1 Minimum value: 1 Maximum value: 200

undefActionControl

Name of the undefined built-in control action: CLIENTAUTH, NOCLIENTAUTH, NOOP, RESET, or DROP. Default value: "CLIENTAUTH"

undefActionData

Name of the undefined built-in data action: NOOP, RESET or DROP. Default value: "NOOP"

[Top](#)

unset ssl parameter

Synopsis

unset ssl parameter [-quantumSize] [-crlMemorySizeMB] [-strictCABChecks] [-sslTriggerTimeout] [-sendCloseNotify] [-encryptTriggerPktCount] [-denySSLReneg] [-insertionEncoding] [-ocspCacheSize] [-pushFlag] [-dropReqWithNoHostHeader] [-pushEncTriggerTimeout] [-undefActionCode] [-undefActionCode]

Description

Use this command to remove ssl parameter settings. Refer to the set ssl parameter command for meanings of the arguments.

[Top](#)

show ssl parameter

Synopsis

show ssl parameter

Description

Displays information about advanced SSL parameters.

[Top](#)

ssl fips

[[set](#) | [unset](#) | [reset](#) | [show](#) | [update](#)]

set ssl fips

Synopsis

set ssl fips -initHSM Level-2 [-hsmLabel <string>]

Description

Initializes the Hardware Security Module (HSM) on the FIPS card and sets a new security officer password and user password. CAUTION: This command erases all data on the FIPS card. You are prompted before proceeding with the command execution. A restart is required before and after executing this command for the changes to apply. Save the configuration after executing this command and before restarting the appliance.

Parameters

initHSM

FIPS initialization level. The appliance currently supports Level-2 (FIPS 140-2).
Possible values: Level-2

soPassword

Security officer password that will be in effect after you have configured the HSM.

oldSoPassword

Old password for the security officer.

userPassword

The Hardware Security Module's (HSM) User password.

hsmLabel

Label to identify the Hardware Security Module (HSM).

Example

```
1) set fips -initHSM Level-2 fipssl123
oldfipssl123 fipuser123 -hsmLabel FIPS-140-2
>This command will erase all data on the FIPS
card. You must save the configuration (saveconfig)
after executing this command.Do you want to
continue?(Y/N)y
```

The above command initializes the FIPS card to FIPS-140-2 Level-2 and sets the HSM's Security Officer and User passwords.

[Top](#)

unset ssl fips**Synopsis**

unset ssl fips -hsmLabel

Description

Use this command to remove ssl fips settings.Refer to the set ssl fips command for meanings of the arguments.

[Top](#)

reset ssl fips**Synopsis**

reset ssl fips

Description

Resets the FIPS card to the default password for Security Officer and User accounts. This command can be used only if the FIPS card has been locked because of three or more unsuccessful login attempts.

Example

```
reset fips
```

[Top](#)

show ssl fips

Synopsis

show ssl fips

Description

Displays the information on the FIPS card.

Example

An example of the output for show ssl fips command is as follows:

```
FIPS HSM Info:
  HSM Label           : FIPS1
  Initialization      : FIPS-140-2 Level-2
  HSM Serial Number   : 238180016
  Firmware Version    : 4.3.0
  Total Flash Memory  : 1900428
  Free Flash Memory   : 1899720
  Total SRAM Memory   : 26210216
  Free SRAM Memory    : 17857232
```

[Top](#)

update ssl fips

Synopsis

update ssl fips -fipsFW 4.6.1

Description

Updates the FIPS firmware. Note: Only compatible firmware version upgrade is allowed. For example, 4.6.0 to 4.6.1

Parameters

fipsFW

FIPS firmware update. Possible values: 4.6.1

Example

```
update ssl fips -fipsFW 4.6.1
```

[Top](#)

ssl service

[[set](#) | [unset](#) | [bind](#) | [unbind](#) | [show](#)]

set ssl service

Synopsis

```
set ssl service <serviceName>@ [-dh ( ENABLED | DISABLED ) -dhFile <string>] [-dhCount <positive_integer>] [-eRSA ( ENABLED | DISABLED ) [-eRSACount <positive_integer>]] [-sessReuse ( ENABLED | DISABLED ) [-sessTimeout <positive_integer>]] [-cipherRedirect ( ENABLED | DISABLED ) [-cipherURL <URL>]] [-sslv2Redirect ( ENABLED | DISABLED ) [-sslv2URL <URL>]] [-clientAuth ( ENABLED | DISABLED ) [-clientCert ( Mandatory | Optional )]] [-sslRedirect ( ENABLED | DISABLED )] [-redirectPortRewrite ( ENABLED | DISABLED )] [-nonFipsCiphers ( ENABLED | DISABLED )] [-ssl2 ( ENABLED | DISABLED )] [-ssl3 ( ENABLED | DISABLED )] [-tls1 ( ENABLED | DISABLED )] [-tls11 ( ENABLED | DISABLED )] [-tls12 ( ENABLED | DISABLED )] [-SNIEnable ( ENABLED | DISABLED )] [-serverAuth ( ENABLED | DISABLED ) [-commonName <string>]] [-pushEncTrigger <pushEncTrigger>] [-sendCloseNotify ( YES | NO )] [-dtlsProfileName <string>]
```

Description

Sets the advanced SSL configuration for an SSL service.

Parameters

serviceName

Name of the SSL service.

dh

State of Diffie-Hellman (DH) key exchange. This parameter is not applicable when configuring a backend service. Possible values: ENABLED, DISABLED Default value: DISABLED

dhCount

Number of interactions, between the client and the NetScaler appliance, after which the DH private-public pair is regenerated. A value of zero (0) specifies infinite use (no refresh). This parameter is not applicable when configuring a backend service. Maximum value: 65534

eRSA

State of Ephemeral RSA (eRSA) key exchange. Ephemeral RSA allows clients that support only export ciphers to communicate with the secure server even if the server certificate does not support export clients. The ephemeral RSA key is automatically generated when you bind an export cipher to an SSL or TCP-based SSL virtual server or service. When you remove the export cipher, the eRSA key is not deleted. It is reused at a later date when another export cipher is bound to an SSL or TCP-based SSL virtual server or service. The eRSA key is deleted when the appliance restarts. This parameter is not applicable when configuring a backend service. Possible values: ENABLED, DISABLED Default value: DISABLED

sessReuse

State of session reuse. Establishing the initial handshake requires CPU-intensive public key encryption operations. With the ENABLED setting, session key exchange is avoided for session resumption requests received from the client. Possible values: ENABLED, DISABLED Default value: ENABLED

cipherRedirect

State of Cipher Redirect. If this parameter is set to ENABLED, you can configure an SSL virtual server or service to display meaningful error messages if the SSL handshake fails because of a cipher mismatch between the virtual server or service and the client. This parameter is not applicable when configuring a backend service. Possible values: ENABLED, DISABLED Default value: DISABLED

sslv2Redirect

State of SSLv2 Redirect. If this parameter is set to ENABLED, you can configure an SSL virtual server or service to display meaningful error messages if the SSL handshake fails because of a protocol version mismatch between the virtual server or service and the client. This parameter is not applicable when configuring a backend service. Possible values: ENABLED, DISABLED Default value: DISABLED

clientAuth

State of client authentication. In service-based SSL offload, the service terminates the SSL handshake if the SSL client does not provide a valid certificate. This parameter is not applicable when configuring a backend service. Possible values: ENABLED, DISABLED Default value: DISABLED

sslRedirect

State of HTTPS redirects for the SSL service. For an SSL session, if the client browser receives a redirect message, the browser tries to connect to the new location. However, the secure SSL session breaks if the object has moved from a secure site (https://) to an unsecure site (http://). Typically, a warning message appears on the screen, prompting the user to continue or disconnect. If SSL Redirect is ENABLED, the redirect message is automatically converted from http:// to https:// and the SSL session does not break. This parameter is not applicable when configuring a backend service. Possible values: ENABLED, DISABLED Default value: DISABLED

redirectPortRewrite

State of the port rewrite while performing HTTPS redirect. If this parameter is set to ENABLED, and the URL from the server does not contain the standard port, the port is rewritten to the standard. Possible values: ENABLED, DISABLED Default value: DISABLED

nonFipsCiphers

State of usage of ciphers that are not FIPS approved. Valid only for an SSL service bound with a FIPS key and certificate. Possible values: ENABLED, DISABLED Default value: DISABLED

ssl2

State of SSLv2 protocol support for the SSL service. This parameter is not applicable when configuring a backend service. Possible values: ENABLED, DISABLED Default value: DISABLED

ssl3

State of SSLv3 protocol support for the SSL service. Possible values: ENABLED, DISABLED Default value: ENABLED

tls1

State of TLSv1.0 protocol support for the SSL service. Possible values: ENABLED, DISABLED Default value: ENABLED

tls11

State of TLSv1.1 protocol support for the SSL service. Enabled for Front-end service on MPX-CVM platform only. Possible values: ENABLED, DISABLED Default value: ENABLED

tls12

State of TLSv1.2 protocol support for the SSL service. Enabled for Front-end service on MPX-CVM platform only. Possible values: ENABLED, DISABLED Default value: ENABLED

SNIEnable

State of the Server Name Indication (SNI) feature on the virtual server and service-based offload. SNI helps to enable SSL encryption on multiple domains on a single virtual server or service if the domains are controlled by the same organization and share the same second-level domain name. For example, *.sports.net can be used to secure domains such as login.sports.net and help.sports.net. Possible values: ENABLED, DISABLED Default value: DISABLED

serverAuth

State of server authentication support for the SSL service. Possible values: ENABLED, DISABLED Default value: DISABLED

pushEncTrigger

Trigger encryption on the basis of the PUSH flag value. Available settings function as follows: * ALWAYS - Any PUSH packet triggers encryption. * IGNORE - Ignore PUSH packet for triggering encryption. * MERGE - For a consecutive sequence of PUSH packets, the last PUSH packet triggers encryption. * TIMER - PUSH packet triggering encryption is delayed by the time defined in the set ssl parameter command or in the Change Advanced SSL Settings dialog box. Possible values: Always, Merge, Ignore, Timer

sendCloseNotify

Enable sending SSL Close-Notify at the end of a transaction Possible values: YES, NO Default value: YES

dtlsProfileName

Name of the DTLS profile whose settings are to be applied to the virtual server.

Example

```
1)    set ssl service sslsvc -dh ENABLED -dhFile /
nsconfig/ssl/dh1024.pem -dhCount 500
The above example sets the DH parameters for the
SSL service 'sslsvc'.
2.    set ssl service sslsvc -ssl2 DISABLED
The above example disables the support for SSLv2
protocol for the SSL service 'sslsvc'.
```

[Top](#)

unset ssl service

Synopsis

```
unset ssl service <serviceName>@ [-dh] [-dhFile] [-dhCount] [-eRSA] [-eRSACount] [-sessReuse] [-sessTimeout] [-cipherRedirect] [-cipherURL] [-ssl2Redirect] [-ssl2URL] [-clientAuth] [-clientCert] [-sslRedirect] [-redirectPortRewrite] [-nonFipsCiphers] [-ssl2] [-ssl3] [-tls1] [-tls11] [-tls12] [-SNIEnable] [-serverAuth] [-commonName] [-sendCloseNotify] [-dtlsProfileName]
```

Description

Use this command to remove ssl service settings. Refer to the set ssl service command for meanings of the arguments.

[Top](#)

bind ssl service

Synopsis

```
bind ssl service <serviceName>@ ((-policyName <string> [-priority <positive_integer>] [-gotoPriorityExpression <expression>] [-invoke (<labelType> <labelName>)] ) | ((-certkeyName <string> [-CA [-crlCheck ( Mandatory | Optional ) ] -ocspCheck ( Mandatory | Optional )] [-skipCAName]) | -SNICert] ) | -cipherName <string>))
```

Description

Binds an SSL certificate-key pair or an SSL policy to a transparent SSL service.

Parameters

serviceName

Name of the SSL service for which to set advanced configuration.

policyName

Name of the SSL policy to bind to the service.

certkeyName

Name of the certificate-key pair.

cipherName

Name of the individual cipher, user-defined cipher group, or predefined (built-in) cipher alias.

Example

```
bind ssl service ssl_svc -policyName
certInsert_pol -priority 10
```

[Top](#)

unbind ssl service

Synopsis

```
unbind ssl service <serviceName>@ ((-policyName <string> [-priority  
<positive_integer>]) | ((-certkeyName <string> [(-CA [-crlCheck ( Mandatory |  
Optional )]) | -SNICert] ) | -cipherName <string>))
```

Description

Unbinds an SSL policy, cipher, and certificate-key pair from an SSL service.

Parameters

serviceName

Name of the SSL service.

policyName

Name of the SSL policy to unbind from the SSL service.

certkeyName

The certificate key pair binding.

cipherName

Name of the individual cipher, user-defined cipher group, or predefined (built-in) cipher alias.

Example

```
unbind ssl service ssl_svc -policyName  
certInsert_pol
```

[Top](#)

show ssl service

Synopsis

```
show ssl service [<serviceName>] [-cipherDetails]
```

Description

Displays information about SSL-specific configuration information for all SSL services, or displays detailed information about the specified SSL service.

Parameters

serviceName

Name of the SSL service for which to show detailed information.

cipherDetails

Display details of the individual ciphers bound to the SSL service.

Example

An example of output of show ssl service command is as shown below
 show ssl service svc1

```

    Advanced SSL configuration for Back-end
SSL Service svc1:
    DH: DISABLED
    Ephemeral RSA: ENABLED           Refresh
Count: 0
    Session Reuse: ENABLED           Timeout:
300 seconds
    Cipher Redirect: DISABLED
    SSLv2 Redirect: DISABLED
    Server Auth: DISABLED
    SSL Redirect: DISABLED
    Non FIPS Ciphers: DISABLED
    SSLv2: DISABLED SSLv3: ENABLED   TLSv1:
ENABLED

    1)      Cipher Name: ALL
    Description: Predefined Cipher Alias
  
```

[Top](#)

ssl serviceGroup

[[set](#) | [unset](#) | [bind](#) | [unbind](#) | [show](#)]

set ssl serviceGroup

Synopsis

```

set ssl serviceGroup <serviceName>@ [-sessReuse ( ENABLED | DISABLED ) [-
sessTimeout <positive_integer>]] [-nonFipsCiphers ( ENABLED | DISABLED )] [-ssl3
( ENABLED | DISABLED )] [-tls1 ( ENABLED | DISABLED )] [-serverAuth ( ENABLED |
DISABLED )] [-commonName <string>]] [-sendCloseNotify ( YES | NO )]
  
```

Description

Sets the advanced SSL configuration for an SSL service group.

Parameters

serviceName

Name of the SSL service group for which to set advanced configuration.

sessReuse

State of session reuse. Establishing the initial handshake requires CPU-intensive public key encryption operations. With the ENABLED setting, session key exchange is avoided for session resumption requests received from the client. Possible values: ENABLED, DISABLED Default value: ENABLED

nonFipsCiphers

State of usage of ciphers that are not FIPS approved. Valid only for an SSL service bound with a FIPS key and certificate. Possible values: ENABLED, DISABLED Default value: DISABLED

ssl3

State of SSLv3 protocol support for the SSL service group. Possible values: ENABLED, DISABLED Default value: ENABLED

tls1

State of TLSv1.0 protocol support for the SSL service group. Possible values: ENABLED, DISABLED Default value: ENABLED

serverAuth

State of server authentication support for the SSL service group. Possible values: ENABLED, DISABLED Default value: DISABLED

sendCloseNotify

Enable sending SSL Close-Notify at the end of a transaction Possible values: YES, NO Default value: YES

Example

```
1)      set ssl servicegroup svcg1 -sessReuse
        DISABLED
        The above example disables session reuse for the
        service group 'svcg1'.
```

[Top](#)

unset ssl serviceGroup

Synopsis

```
unset ssl serviceGroup <serviceName>@ [-sessReuse] [-sessTimeout] [-
nonFipsCiphers] [-ssl3] [-tls1] [-serverAuth] [-commonName] [-sendCloseNotify]
```

Description

Use this command to remove ssl serviceGroup settings. Refer to the set ssl serviceGroup command for meanings of the arguments.

[Top](#)

bind ssl serviceGroup

Synopsis

```
bind ssl serviceGroup <serviceName>@ ((-certkeyName <string> [(-CA [-crlCheck
( Mandatory | Optional ) | -ocspCheck ( Mandatory | Optional )]) | -SNICert] ) | -
cipherName <string>)
```

Description

Bind a SSL certkey or a SSL policy to a SSL service.

Parameters

serviceGroupName

The name of the SSL service to which the SSL policy needs to be bound.

certkeyName

The name of the CertKey

cipherName

A cipher-suite can consist of an individual cipher name, the system predefined cipher-alias name, or user defined cipher-group name.

Example

```
bind ssl service ssl_svc -policyName
certInsert_pol -priority 10
```

[Top](#)

unbind ssl serviceGroup

Synopsis

```
unbind ssl serviceGroup <serviceGroupName>@ ((-certkeyName <string> [(-CA [-
crlCheck ( Mandatory | Optional )]) | -SNICert] ) | -cipherName <string>)
```

Description

Unbind a SSL policy from a SSL service.

Parameters

serviceGroupName

The name of the SSL service from which the SSL policy needs to be unbound.

certkeyName

The name of the certificate bound to the SSL service group.

cipherName

A cipher-suite can consist of an individual cipher name, the system predefined cipher-alias name, or user defined cipher-group name.

Example

```
unbind ssl service ssl_svc -policyName
certInsert_pol
```

[Top](#)

show ssl serviceGroup

Synopsis

```
show ssl serviceGroup [<serviceName>] [-cipherDetails]
```

Description

Displays information about SSL-specific configuration for all SSL service groups, or displays detailed information about the specified SSL service group.

Parameters

serviceName

Name of the SSL service group for which to show detailed information.

cipherDetails

Display details of the individual ciphers bound to the SSL service group.

Example

```
An example of output of show ssl servicegroup
command is as shown below
show ssl servicegroup ssl_svcg

      Advanced SSL configuration for Back-end
SSL Service Group ssl_svcg:
      Session Reuse: ENABLED           Timeout:
300 seconds
      Server Auth: DISABLED
      Non FIPS Ciphers: DISABLED
      SSLv3: ENABLED  TLSv1: ENABLED

1)      Cipher Name: ALL
      Description: Predefined Cipher Alias
```

[Top](#)

ssl vserver

[[set](#) | [unset](#) | [bind](#) | [unbind](#) | [show](#)]

set ssl vserver

Synopsis

```
set ssl vserver <vServerName>@ [-clearTextPort <port>] [-dh ( ENABLED | DISABLED ) -
dhFile <string>] [-dhCount <positive_integer>] [-eRSA ( ENABLED | DISABLED ) [-
eRSACount <positive_integer>]] [-sessReuse ( ENABLED | DISABLED ) [-sessTimeout
<positive_integer>]] [-cipherRedirect ( ENABLED | DISABLED ) [-cipherURL <URL>]] [-
sslv2Redirect ( ENABLED | DISABLED ) [-sslv2URL <URL>]] [-clientAuth ( ENABLED |
DISABLED ) [-clientCert ( Mandatory | Optional )]] [-sslRedirect ( ENABLED | DISABLED )]
[-redirectPortRewrite ( ENABLED | DISABLED )] [-nonFipsCiphers ( ENABLED |
DISABLED )] [-ssl2 ( ENABLED | DISABLED )] [-ssl3 ( ENABLED | DISABLED )] [-tls1
```



```
( ENABLED | DISABLED )) [-tls11 ( ENABLED | DISABLED )) [-tls12 ( ENABLED |
DISABLED )) [-SNIEnable ( ENABLED | DISABLED )) [-pushEncTrigger <pushEncTrigger>] [-
sendCloseNotify ( YES | NO )) [-dtlsProfileName <string>]
```

Description

Sets advanced SSL configuration for an SSL virtual server.

Parameters

vServerName

Name of the SSL virtual server for which to set advanced configuration.

clearTextPort

Port on which clear-text data is sent by the appliance to the server. Do not specify this parameter for SSL offloading with end-to-end encryption.

dh

State of Diffie-Hellman (DH) key exchange. Possible values: ENABLED, DISABLED
Default value: DISABLED

dhCount

Number of interactions, between the client and the NetScaler appliance, after which the DH private-public pair is regenerated. A value of zero (0) specifies infinite use (no refresh). Maximum value: 65534

eRSA

State of Ephemeral RSA (eRSA) key exchange. Ephemeral RSA allows clients that support only export ciphers to communicate with the secure server even if the server certificate does not support export clients. The ephemeral RSA key is automatically generated when you bind an export cipher to an SSL or TCP-based SSL virtual server or service. When you remove the export cipher, the eRSA key is not deleted. It is reused at a later date when another export cipher is bound to an SSL or TCP-based SSL virtual server or service. The eRSA key is deleted when the appliance restarts. Possible values: ENABLED, DISABLED Default value: ENABLED

sessReuse

State of session reuse. Establishing the initial handshake requires CPU-intensive public key encryption operations. With the ENABLED setting, session key exchange is avoided for session resumption requests received from the client. Possible values: ENABLED, DISABLED Default value: ENABLED

cipherRedirect

State of Cipher Redirect. If cipher redirect is enabled, you can configure an SSL virtual server or service to display meaningful error messages if the SSL handshake fails because of a cipher mismatch between the virtual server or service and the client. Possible values: ENABLED, DISABLED Default value: DISABLED

sslV2Redirect

State of SSLv2 Redirect. If SSLv2 redirect is enabled, you can configure an SSL virtual server or service to display meaningful error messages if the SSL handshake fails because of a protocol version mismatch between the virtual server or service and the client. Possible values: ENABLED, DISABLED Default value: DISABLED

clientAuth

State of client authentication. If client authentication is enabled, the virtual server terminates the SSL handshake if the SSL client does not provide a valid certificate. Possible values: ENABLED, DISABLED Default value: DISABLED

sslRedirect

State of HTTPS redirects for the SSL virtual server. For an SSL session, if the client browser receives a redirect message, the browser tries to connect to the new location. However, the secure SSL session breaks if the object has moved from a secure site (https://) to an unsecure site (http://). Typically, a warning message appears on the screen, prompting the user to continue or disconnect. If SSL Redirect is ENABLED, the redirect message is automatically converted from http:// to https:// and the SSL session does not break. Possible values: ENABLED, DISABLED Default value: DISABLED

redirectPortRewrite

State of the port rewrite while performing HTTPS redirect. If this parameter is ENABLED and the URL from the server does not contain the standard port, the port is rewritten to the standard. Possible values: ENABLED, DISABLED Default value: DISABLED

nonFipsCiphers

State of usage of non-FIPS approved ciphers. Valid only for an SSL service bound with a FIPS key and certificate. Possible values: ENABLED, DISABLED Default value: DISABLED

ssl2

State of SSLv2 protocol support for the SSL Virtual Server. Possible values: ENABLED, DISABLED Default value: DISABLED

ssl3

State of SSLv3 protocol support for the SSL Virtual Server. Possible values: ENABLED, DISABLED Default value: ENABLED

tls1

State of TLSv1.0 protocol support for the SSL Virtual Server. Possible values: ENABLED, DISABLED Default value: ENABLED

tls11

State of TLSv1.1 protocol support for the SSL Virtual Server. Enabled for Virtual Server on MPX-CVM platform only Possible values: ENABLED, DISABLED Default value: ENABLED

tls12

State of TLSv1.2 protocol support for the SSL Virtual Server. Enabled for Virtual Server on MPX-CVM platform only Possible values: ENABLED, DISABLED Default value: ENABLED

SNIEnable

State of the Server Name Indication (SNI) feature on the virtual server and service-based offload. SNI helps to enable SSL encryption on multiple domains on a single virtual server or service if the domains are controlled by the same organization and share the same second-level domain name. For example, *.sports.net can be used to

secure domains such as login.sports.net and help.sports.net. Possible values: ENABLED, DISABLED Default value: DISABLED

pushEncTrigger

Trigger encryption on the basis of the PUSH flag value. Available settings function as follows: * ALWAYS - Any PUSH packet triggers encryption. * IGNORE - Ignore PUSH packet for triggering encryption. * MERGE - For a consecutive sequence of PUSH packets, the last PUSH packet triggers encryption. * TIMER - PUSH packet triggering encryption is delayed by the time defined in the set ssl parameter command or in the Change Advanced SSL Settings dialog box. Possible values: Always, Merge, Ignore, Timer

sendCloseNotify

Enable sending SSL Close-Notify at the end of a transaction Possible values: YES, NO Default value: YES

dtlsProfileName

Name of the DTLS profile whose settings are to be applied to the virtual server.

Example

```
1)      set ssl vsriver sslvip -dh ENABLED -dhFile /
siteA/dh1024.pem -dhCount 500
The above example set the DH parameters for the
SSL virtual server 'sslvip'.
3)      set ssl vsriver sslvip -ssl2 DISABLED
The above example disables the support for SSLv2
protocol for the SSL virtual server 'sslvip'.
```

[Top](#)

unset ssl vsriver

Synopsis

```
unset ssl vsriver <vServerName>@ [-clearTextPort] [-dh] [-dhFile] [-dhCount] [-eRSA] [-eRSACount] [-sessReuse] [-sessTimeout] [-cipherRedirect] [-cipherURL] [-ssl2Redirect] [-ssl2URL] [-clientAuth] [-clientCert] [-sslRedirect] [-redirectPortRewrite] [-nonFipsCiphers] [-ssl2] [-ssl3] [-tls1] [-tls11] [-tls12] [-SNIEnable] [-sendCloseNotify] [-dtlsProfileName]
```

Description

Use this command to remove ssl vsriver settings. Refer to the set ssl vsriver command for meanings of the arguments.

[Top](#)

bind ssl vsriver

Synopsis

```
bind ssl vsriver <vServerName>@ ((-policyName <string> [-priority <positive_integer>] [-gotoPriorityExpression <expression>] [-invoke (<labelType> <labelName>)] ) ) | ((-
```

```
certkeyName <string> [(-CA [-crlCheck ( Mandatory | Optional ) | -ocspCheck  
( Mandatory | Optional )] [-skipCAName]) | -SNICert] ) | -cipherName <string>))
```

Description

Binds an SSL certificate-key pair or an SSL policy to an SSL virtual server.

Parameters

vServerName

Name of the SSL virtual server.

policyName

Name of the SSL policy to bind to the SSL virtual server.

certkeyName

Name of the certificate-key pair.

cipherName

Name of the individual cipher, user-defined cipher group, or predefined (built-in) cipher alias.

Example

```
1. bind ssl vserver ssl_vip -certkeyName cert1  
In the above example the certificate cert1 is  
bound to the SSL vserver ssl_vip as server  
certificate.  
2. bind ssl vserver ssl_vip -certkeyName cert2 -CA  
In the above example the certificate cert2 is  
bound to the SSL vserver ssl_vip as CA certificate.  
3. bind ssl vserver ssl_vip -certkeyName cert3 -CA  
-ocspCheck Mandatory  
In the above example the certificate cert3 is  
bound to the SSL vserver ssl_vip as CA  
certificate, with OCSP check set to Mandatory.  
4. bind ssl vserver ssl_vip -policyName  
certInsert_pol -priority 10  
In the above example the SSL policy certInsert_pol  
is bound to the SSL vserver ssl_vip with priority  
10.
```

[Top](#)

unbind ssl vserver

Synopsis

```
unbind ssl vserver <vServerName>@ ((-policyName <string> [-priority  
<positive_integer>]) | ((-certkeyName <string> [-CA | -SNICert] ) | -cipherName  
<string>))
```

Description

Unbinds an SSL policy, cipher, and certificate-key pair from an SSL virtual server.

Parameters**vServerName**

Name of the SSL virtual server.

policyName

Name of the SSL policy to unbind from the SSL virtual server.

certkeyName

The name of the certificate key pair binding.

cipherName

Name of the cipher.

Example

```
unbind ssl vserver ssl_vip -policyName
certInsert_pol
```

[Top](#)

show ssl vserver**Synopsis**

show ssl vserver [<vServerName>] [-cipherDetails]

Description

Displays SSL specific configuration information for all SSL virtual servers, or displays detailed information for the specified SSL virtual server.

Parameters**vServerName**

Name of the SSL virtual server for which to show detailed information.

cipherDetails

Display details of the individual ciphers bound to the SSL virtual server.

Example

```
An example of the output of the show vserver
sslvip command is as follows:
sh ssl vserver val

          Advanced SSL configuration for VServer val:
          DH: DISABLED
          Ephemeral RSA: ENABLED           Refresh
Count: 0
          Session Reuse: ENABLED           Timeout:
120 seconds
          Cipher Redirect: DISABLED
          SSLv2 Redirect: DISABLED
```

```

ClearText Port: 0
Client Auth: DISABLED
SSL Redirect: DISABLED
Non FIPS Ciphers: DISABLED
SSLv2: DISABLED SSLv3: ENABLED TLSv1:
ENABLED

1)      1 bound certificate:
CertKey Name: buy      Server Certificate

1)      1 bound CA certificate:
CertKey Name: rtca      CA Certificate

1)      Cipher Name: DEFAULT
Description: Predefined Cipher Alias

```

[Top](#)

ssl fipsSIMTarget

[\[enable | init \]](#)

enable ssl fipsSIMTarget

Synopsis

```
enable ssl fipsSIMTarget <keyVector> <sourceSecret>
```

Description

Enables secure transfer of FIPS keys in a high availability setup from the primary appliance to the secondary appliance.

Parameters

keyVector

Name of and, optionally, path to the target FIPS appliance's key vector. /nsconfig/ssl/ is the default path.

sourceSecret

Name of and, optionally, path to the source FIPS appliance's secret data. /nsconfig/ssl/ is the default path.

Example

```
enable fipsSIMtarget /nsconfig/ssl/target.key /
nsconfig/ssl/source.secret
```

[Top](#)

init ssl fipsSIMTarget

Synopsis

init ssl fipsSIMTarget <certFile> <keyVector> <targetSecret>

Description

Initialize the target (secondary) FIPS appliance for participating in a secure exchange of keys with the primary FIPS appliance.

Parameters

certFile

Name of and, optionally, path to the source FIPS appliance's certificate file. /nsconfig/ssl/ is the default path.

keyVector

Name for and, optionally, path to the target FIPS appliance's key vector. /nsconfig/ssl/ is the default path.

targetSecret

Name for and, optionally, path to the target FIPS appliance's secret data. The default input path for the secret data is /nsconfig/ssl/.

Example

```
init fipsSIMtarget /nsconfig/ssl/source.cert /  
nsconfig/ssl/target.key /nsconfig/ssl/target.secret
```

[Top](#)

ssl fipsSIMSource

[[enable](#) | [init](#)]

enable ssl fipsSIMSource

Synopsis

enable ssl fipsSIMSource <targetSecret> <sourceSecret>

Description

Enable the source FIPS appliance to participate in a secure exchange of keys with the target (secondary) FIPS appliance.

Parameters

targetSecret

Name of and, optionally, path to the target FIPS appliance's secret data. /nsconfig/ssl/ is the default path.

sourceSecret

Name for and, optionally, path to the source FIPS appliance's secret data. /nsconfig/ssl/ is the default path.

Example

```
enable fipsSIMsource /nsconfig/ssl/target.secret /
nsconfig/ssl/source.secret
```

[Top](#)

init ssl fipsSIMSource

Synopsis

```
init ssl fipsSIMSource <certFile>
```

Description

Initialize the source FIPS appliance for participating in a secure exchange of keys with the target (secondary) FIPS appliance.

Parameters

certFile

Name for and, optionally, path to the source FIPS appliance's certificate file. /nsconfig/ssl/ is the default path.

Example

```
init fipsSIMsource /nsconfig/ssl/source.cert
```

[Top](#)

ssl global

[[bind](#) | [unbind](#) | [show](#)]

bind ssl global

Synopsis

```
bind ssl global [-policyName <string>] [-priority <positive_integer>] [-
gotoPriorityExpression <expression>] [-type <type>] [-invoke (<labelType>
<labelName>)] ]
```

Description

Binds an SSL policy globally.

Parameters

policyName
Name of the SSL policy.

Example

```
bind ssl global -policyName certInsert_pol -  
priority 100
```

[Top](#)**unbind ssl global****Synopsis**

unbind ssl global [-policyName <string> [-type <type>] [-priority <positive_integer>]]

Description

Unbinds a globally bound SSL policy.

Parameters

policyName
Name of the SSL policy to unbind.

Example

```
unbind ssl global -policyName certInsert_pol
```

[Top](#)**show ssl global****Synopsis**

show ssl global [-type <type>]

Description

Displays globally bound SSL policies.

Parameters

type
Global bind point to which the policy is bound. Possible values: CONTROL_OVERRIDE, CONTROL_DEFAULT, DATA_OVERRIDE, DATA_DEFAULT

Example

```
show ssl global
      1 Globally Active SSL Policy:
1)      Name: certInsert_pol      Priority: 100
```

[Top](#)

ssl dtlsProfile

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add ssl dtlsProfile

Synopsis

```
add ssl dtlsProfile <name> [-pmtuDiscovery ( ENABLED | DISABLED )] [-maxRecordSize
<positive_integer>] [-maxRetryTime <positive_integer>] [-helloVerifyRequest ( ENABLED
| DISABLED )] [-terminateSession ( ENABLED | DISABLED )] [-maxPacketSize
<positive_integer>]
```

Description

Add a new DTLS profile on the Netscaler

Parameters

name

Name of the DTLS profile

pmtuDiscovery

Enable/disable PMTU discovery Possible values: ENABLED, DISABLED Default value: DISABLED

maxRecordSize

Maximum record size Default value: 1460 Maximum value: 1472

maxRetryTime

Maximum retry time Default value: 3

helloVerifyRequest

Enable/disable sending of hello verify request Possible values: ENABLED, DISABLED Default value: DISABLED

terminateSession

Option to decide whether to terminate the session if bad MAC decode error happens. Possible values: ENABLED, DISABLED Default value: DISABLED

maxPacketSize

Max packet count to reassemble for a fragmented record - attack protection if client send small packets Default value: 120 Maximum value: 86400

Example

```
add ldapprofile <profile name> -dropInvalReqs ON -
markHttp09Inval ON
```

[Top](#)**rm ssl dtlsProfile****Synopsis**

```
rm ssl dtlsProfile <name>
```

Description

Remove a DTLS profile on the Netscaler

Parameters

name
Name of the DTLS profile

Example

```
rm dtlsprofile <profile name>
```

[Top](#)**set ssl dtlsProfile****Synopsis**

```
set ssl dtlsProfile <name> [-pmtuDiscovery ( ENABLED | DISABLED )] [-maxRecordSize
<positive_integer>] [-maxRetryTime <positive_integer>] [-helloVerifyRequest ( ENABLED
| DISABLED )] [-terminateSession ( ENABLED | DISABLED )] [-maxPacketSize
<positive_integer>]
```

Description

Set/modify DTLS profile values

Parameters

name
Name of the DTLS profile

pmtuDiscovery
Enable/disable PMTU discovery Possible values: ENABLED, DISABLED Default value: DISABLED

maxRecordSize
Maximum record size Default value: 1460 Maximum value: 1472

maxRetryTime

Maximum retry time Default value: 3

helloVerifyRequest

Enable/disable sending of hello verify request Possible values: ENABLED, DISABLED

Default value: DISABLED

terminateSession

Option to decide whether to terminate the session if bad MAC decode error happens.

Possible values: ENABLED, DISABLED Default value: DISABLED

maxPacketSize

Max packet count to reassemble for a fragmented record - attack protection if client send small packets Default value: 120 Maximum value: 86400

Example

```
set dtlsprofile <profile name> -dropInvalReqs ON -  
markHttp09Inval ON
```

[Top](#)

unset ssl dtlsProfile**Synopsis**

unset ssl dtlsProfile <name> [-pmtuDiscovery] [-maxRecordSize] [-maxRetryTime] [-helloVerifyRequest] [-terminateSession] [-maxPacketSize]

Description

Use this command to remove ssl dtlsProfile settings. Refer to the set ssl dtlsProfile command for meanings of the arguments.

[Top](#)

show ssl dtlsProfile**Synopsis**

show ssl dtlsProfile [<name>]

Description

Display all the configured DTLS profiles in the system. If a name is specified, then only that profile is shown.

Parameters

name

Name of the DTLS profile.

Example

```
show dtls profile [profile name]
```

[Top](#)

Stream Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [stream selector](#)
- ♦ [stream identifier](#)
- ♦ [stream session](#)

stream selector

[[add](#) | [set](#) | [rm](#) | [show](#)]

add stream selector

Synopsis

```
add stream selector <name> <rule> ...
```

Description

Creates a selector for Action Analytics or traffic rate limiting.

Parameters

name

Name for the selector. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. If the name includes one or more spaces, and you are using the NetScaler CLI, enclose the name in double or single quotation marks (for example, "my selector" or 'my selector').

rule

Set of up to five individual (not compound) default syntax expressions. Maximum length: 7499 characters. Each expression must identify a specific request characteristic, such as the client's IP address (with CLIENT.IP.SRC) or requested server resource (with HTTP.REQ.URL). Note: If two or more selectors contain the same expressions in different order, a separate set of records is created for each selector.

Example

```
add stream selector sel_subnet HTTP.REQ.URL  
CLIENT.IP.SRC.SUBNET(24)
```

[Top](#)

set stream selector

Synopsis

set stream selector <name> -rule <expression> ...

Description

Modifies the set of expressions in a stream selector. Note: You can change an expression if the selector is not yet being used in an identifier. If the selector is already in use, you can change only the order of the expressions, not the expressions themselves.

Parameters

name

Name of the selector for which to modify parameters.

rule

Set of up to five individual (not compound) default syntax expressions. Maximum length: 7499 characters. Each expression must identify a specific request characteristic, such as the client's IP address (with CLIENT.IP.SRC) or requested server resource (with HTTP.REQ.URL). Note: If two or more selectors contain the same expressions in different order, a separate set of records is created for each selector.

Example

```
set stream sel_subnet HTTP.REQ.URL CLIENT.IP.SRC
```

[Top](#)

rm stream selector

Synopsis

rm stream selector <name>

Description

Removes a selector. Note: Before you remove a selector, make sure that it is not being used by an identifier.

Parameters

name

Name for the selector. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. If the name includes one or more spaces, and you are using the NetScaler CLI, enclose the name in double or single quotation marks (for example, "my selector" or 'my selector').

Example

```
rm stream selector sel_subnet
```

[Top](#)**show stream selector****Synopsis**

```
show stream selector [<name>]
```

Description

Displays the expressions configured for the specified selector or, if no selector name is specified, the expressions configured for all selectors.

Parameters**name**

Name for the selector. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. If the name includes one or more spaces, and you are using the NetScaler CLI, enclose the name in double or single quotation marks (for example, "my selector" or 'my selector').

Example

```
show ns limitSelector sel_subnet
```

[Top](#)**stream identifier**

[[add](#) | [set](#) | [unset](#) | [rm](#) | [show](#) | [stat](#)]

add stream identifier**Synopsis**

```
add stream identifier <name> <selectorName> [-interval <positive_integer>] [-SampleCount <positive_integer>] [-sort <sort>]
```

Description

Creates a stream identifier. A stream identifier specifies how data is collected and stored for an Action Analytics configuration.

Parameters**name**

The name of stream identifier.

selectorName

Name of the selector to use with the stream identifier.

interval

Number of minutes of data to use when calculating session statistics (number of requests, bandwidth, and response times). The interval is a moving window that keeps the most recently collected data. Older data is discarded at regular intervals. Default value: 1 Minimum value: 1

SampleCount

Size of the sample from which to select a request for evaluation. The smaller the sample count, the more accurate is the statistical data. To evaluate all requests, set the sample count to 1. However, such a low setting can result in excessive consumption of memory and processing resources. Default value: 1 Minimum value: 1 Maximum value: 65535

sort

Sort stored records by the specified statistics column, in descending order. Performed during data collection, the sorting enables real-time data evaluation through NetScaler policies (for example, compression and caching policies) that use functions such as IS_TOP(n). Possible values: REQUESTS, CONNECTIONS, RESPTIME, BANDWIDTH, NONE Default value: STREAM_DIMENSION_REQUESTS

Example

```
add stream identifier stream_id top_url -interval
10 -sampleCount 1 -sort REQUESTS
```

[Top](#)

set stream identifier

Synopsis

```
set stream identifier <name> [-selectorName <string>] [-interval <positive_integer>] [-
SampleCount <positive_integer>] [-sort <sort>]
```

Description

Modifies the specified parameters of a stream identifier. Parameters for which a default value is available revert to their default values.

Parameters

name

The name of stream identifier.

selectorName

Name of the selector to use with the stream identifier.

interval

Number of minutes of data to use when calculating session statistics (number of requests, bandwidth, and response times). The interval is a moving window that

keeps the most recently collected data. Older data is discarded at regular intervals.
Default value: 1 Minimum value: 1

SampleCount

Size of the sample from which to select a request for evaluation. The smaller the sample count, the more accurate is the statistical data. To evaluate all requests, set the sample count to 1. However, such a low setting can result in excessive consumption of memory and processing resources. Default value: 1 Minimum value: 1 Maximum value: 65535

sort

Sort stored records by the specified statistics column, in descending order. Performed during data collection, the sorting enables real-time data evaluation through NetScaler policies (for example, compression and caching policies) that use functions such as IS_TOP(n). Possible values: REQUESTS, CONNECTIONS, RESPTIME, BANDWIDTH, NONE Default value: STREAM_DIMENSION_REQUESTS

Example

```
set stream identifier stream_id -selectorName
top_clients -interval 1 -sampleCount 1 -sort NONE
```

[Top](#)

unset stream identifier

Synopsis

```
unset stream identifier <name> [-selectorName] [-interval] [-SampleCount] [-sort]
```

Description

Use this command to remove stream identifier settings. Refer to the set stream identifier command for meanings of the arguments.

[Top](#)

rm stream identifier

Synopsis

```
rm stream identifier <name>
```

Description

Removes a stream identifier. Note: You cannot remove a stream identifier if it is being used in a policy.

Parameters

name

The name of stream identifier.

Example

```
rm stream identifier stream_id
```

[Top](#)

show stream identifier

Synopsis

```
show stream identifier [<name>]
```

Description

Displays the parameters of the specified stream identifier or, if no stream identifier name is specified, the parameters of all configured stream identifiers.

Parameters

name

The name of stream identifier.

Example

```
show stream identifier stream_id
```

[Top](#)

stat stream identifier

Synopsis

```
stat stream identifier <name> [<pattern> ...] [-detail] [-fullValues] [-ntimes  
<positive_integer>] [-logFile <input_filename>] [-clearstats ( basic | full )] [-sortBy  
<sortBy> [<sortOrder>]]
```

Description

Displays the statistics that the NetScaler appliance has collected for the specified stream identifier.

Parameters

name

Name of the stream identifier.

pattern

Values on which grouping is performed are displayed in the output as row titles. If grouping is performed on two or more fields, their values are separated by a question mark in the row title. For example, consider a selector that contains the expressions HTTP.REQ.URL and CLIENT.IP.SRC (in that order), on an appliance that has accumulated records of a number of requests for two URLs, example.com/page1.html and example.com/page2.html, from two client IP addresses, 192.0.2.10 and 192.0.2.11. With a pattern of ? ?, the appliance performs grouping on both fields

and displays statistics for the following: * Requests for example.com/abc.html from 192.0.2.10, with a row title of example.com/abc.html?192.0.2.10. * Requests for example.com/abc.html from 192.0.2.11, with a row title of example.com/abc.html?192.0.2.11. * Requests for example.com/def.html from 192.0.2.10, with a row title of example.com/def.html?192.0.2.10. * Requests for example.com/def.html from 192.0.2.11, with a row title of example.com/def.html?192.0.2.11. With a pattern of * ?, the appliance performs grouping on only the client IP address values and displays statistics for the following requests: * All requests from 192.0.2.10, with the IP address as the row title. * All requests from 192.0.2.11, with the IP address as the row title. With a pattern of ? *, the appliance performs grouping on only the URL values and displays statistics for the following requests: * All requests for example.com/abc.html, with the URL as the row title. * All requests for example.com/def.html, with the URL as the row title. With a pattern of ** , the appliance displays one set of collective statistics for all the requests received, with no row title. With a pattern of example.com/abc.html ?, the appliance displays statistics for requests for example.com/abc.html from each unique client IP address. With a pattern of * 192.0.2.11, the appliance displays statistics for all requests from 192.0.2.11.

clearstats

Clear the statistics / counters Possible values: basic, full

sortBy

use this argument to sort by specific key Possible values: Req, BandW, RspTime, Conn

[Top](#)

stream session

clear stream session

Synopsis

clear stream session <name>

Description

Flushes all the records that have been accumulated for the specified stream identifier.

Parameters

name

Name of the stream identifier.

Example

```
clear stream session stream_id
```

System Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [system](#)
- ♦ [system cmdPolicy](#)
- ♦ [system user](#)
- ♦ [system group](#)
- ♦ [system session](#)
- ♦ [system cpu](#)
- ♦ [system memory](#)
- ♦ [system entitydata](#)
- ♦ [system entity](#)
- ♦ [system globaldata](#)
- ♦ [system counters](#)
- ♦ [system countergroup](#)
- ♦ [system entitytype](#)
- ♦ [system eventhistory](#)
- ♦ [system core](#)
- ♦ [system dataSource](#)
- ♦ [system global](#)
- ♦ [system collectionparam](#)
- ♦ [system parameter](#)
- ♦ [system backup](#)

system

stat system

Synopsis

```
stat system [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile  
<input_filename>] [-clearstats ( basic | full )]
```

Description

This command displays system statistics

Parameters

clearstats

Clear the statistics / counters Possible values: basic, full

system cmdPolicy

[[add](#) | [rm](#) | [set](#) | [show](#)]

add system cmdPolicy

Synopsis

add system cmdPolicy <policyName> <action> <cmdSpec>

Description

Adds a command policy to the system. A command policy specifies the access rights of the system user. By default, the appliance already has the following policies defined: * operator * read-only * network * superuser

Parameters

policyName

Name for a command policy. Must begin with a letter, number, or the underscore (_) character, and must contain only alphanumeric, hyphen (-), period (.), hash (#), space (), at (@), equal (=), colon (:), and underscore characters. Cannot be changed after the policy is created. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy').

action

Action to perform when a request matches the policy. Possible values: ALLOW, DENY

cmdSpec

Regular expression specifying the data that matches the policy.

[Top](#)

rm system cmdPolicy

Synopsis

rm system cmdPolicy <policyName>

Description

Removes a command policy from the appliance. Note: You cannot remove command policies that are bound to a system user.

Parameters

policyName

Name of the command policy to remove.

[Top](#)

set system cmdPolicy

Synopsis

set system cmdPolicy <policyName> <action> <cmdSpec>

Description

Modifies the specified attributes of an existing command policy.

Parameters

policyName

Name of the command policy to be modified.

action

Action to perform when a request matches the policy. Possible values: ALLOW, DENY

cmdSpec

Regular expression specifying the data that matches the policy.

[Top](#)

show system cmdPolicy

Synopsis

show system cmdPolicy [<policyName>]

Description

Displays information about all configured system command policies, or about the specified policy.

Parameters

policyName

Name of the system command policy about which to display information.

[Top](#)

system user

[[add](#) | [rm](#) | [set](#) | [unset](#) | [bind](#) | [unbind](#) | [show](#)]

add system user

Synopsis

add system user <userName> [-externalAuth (ENABLED | DISABLED)] [-promptString <string>] [-timeout <secs>]

Description

Adds a new user to the system. Note: You must provide the password after the user name.

Parameters

userName

Name for a user. Must begin with a letter, number, or the underscore (_) character, and must contain only alphanumeric, hyphen (-), period (.), hash (#), space (), at (@), equal (=), colon (:), and underscore characters. Cannot be changed after the

user is added. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my user" or 'my user').

password

Password for the system user. Can include any ASCII character.

externalAuth

Whether to use external authentication servers for the system user authentication or not
Possible values: ENABLED, DISABLED
Default value: ENABLED

promptString

String to display at the command-line prompt. Can consist of letters, numbers, hyphen (-), period (.), hash (#), space (), at (@), equal (=), colon (:), underscore (_), and the following variables: *%u - Will be replaced by the user name. *%h - Will be replaced by the hostname of the NetScaler appliance. *%t - Will be replaced by the current time in 12-hour format. *%T - Will be replaced by the current time in 24-hour format. *%d - Will be replaced by the current date. *%s - Will be replaced by the state of the NetScaler appliance. Note: The 63-character limit for the length of the string does not apply to the characters that replace the variables.

timeout

CLI session inactivity timeout, in seconds. Timeout cannot have values in between 1 and 9. Maximum value: 100000000

[Top](#)

rm system user

Synopsis

```
rm system user <userName>
```

Description

Removes a system user from the appliance.

Parameters

userName

Name of the system user to remove.

[Top](#)

set system user

Synopsis

```
set system user <userName> {-password } [-externalAuth ( ENABLED | DISABLED )] [-promptString <string>] [-timeout <secs>]
```

Description

Modifies the specified parameters of a system-user entry.

Parameters

userName

Name of the system-user entry to modify.

password

Password for the system user. Can include any ASCII character.

externalAuth

Whether to use external authentication servers for the system user authentication or not Possible values: ENABLED, DISABLED Default value: ENABLED

promptString

String to display at the command-line prompt. Can consist of letters, numbers, hyphen (-), period (.), hash (#), space (), at (@), equal (=), colon (:), underscore (_), and the following variables: * %u - Will be replaced by the user name. * %h - Will be replaced by the hostname of the NetScaler appliance. * %t - Will be replaced by the current time in 12-hour format. * %T - Will be replaced by the current time in 24-hour format. * %d - Will be replaced by the current date. * %s - Will be replaced by the state of the NetScaler appliance. Note: The 63-character limit for the length of the string does not apply to the characters that replace the variables.

timeout

CLI session inactivity timeout, in seconds. Timeout cannot have values in between 1 and 9. Maximum value: 100000000

[Top](#)

unset system user

Synopsis

```
unset system user <userName> [-externalAuth] [-promptString] [-timeout]
```

Description

Use this command to remove system user settings. Refer to the set system user command for meanings of the arguments.

[Top](#)

bind system user

Synopsis

```
bind system user <userName> <policyName> <priority>
```

Description

Binds a command policy to a system user.

Parameters

userName

Name of the system-user entry to which to bind the command policy.

policyName

Name of the command policy to bind to the system user.

[Top](#)

unbind system user

Synopsis

unbind system user <userName> <policyName>

Description

Unbinds a command policy from the system user.

Parameters

userName

Name of the user entry from which to unbind the command policy.

policyName

Name of the command policy to unbind.

[Top](#)

show system user

Synopsis

show system user [<userName>]

Description

Displays information about all system users configured on the appliance, or about the specified user.

Parameters

userName

Name of a system user about whom to display information.

[Top](#)

system group

[[add](#) | [rm](#) | [bind](#) | [unbind](#) | [show](#) | [set](#) | [unset](#)]

add system group

Synopsis

add system group <groupName> [-promptString <string>] [-timeout <secs>]

Description

Creates a system-user group, to which you can bind individual users by using the bind system group command.

Parameters

groupName

Name for the group. Must begin with a letter, number, or the underscore (_) character, and must contain only alphanumeric, hyphen (-), period (.), hash (#), space (), at (@), equal (=), colon (:), and underscore characters. Cannot be changed

after the group is created. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my group" or 'my group').

promptString

String to display at the command-line prompt. Can consist of letters, numbers, hyphen (-), period (.), hash (#), space (), at (@), equal (=), colon (:), underscore (_), and the following variables: * %u - Will be replaced by the user name. * %h - Will be replaced by the hostname of the NetScaler appliance. * %t - Will be replaced by the current time in 12-hour format. * %T - Will be replaced by the current time in 24-hour format. * %d - Will be replaced by the current date. * %s - Will be replaced by the state of the NetScaler appliance. Note: The 63-character limit for the length of the string does not apply to the characters that replace the variables.

timeout

CLI session inactivity timeout, in seconds. Timeout cannot have values in between 1 and 9. Maximum value: 100000000

[Top](#)

rm system group

Synopsis

rm system group <groupName>

Description

Removes a system group from the appliance.

Parameters

groupName

Name of the system group to remove.

[Top](#)

bind system group

Synopsis

bind system group <groupName> [-userName <string>] [-policyName <string> <priority>]

Description

Binds a system user to a system group.

Parameters

groupName

Name of the system group.

userName

Name of a system user to bind to the group.

policyName

Name of the command policy to be bind to the group.

[Top](#)

unbind system group

Synopsis

unbind system group <groupName> [-userName <string>] [-policyName <string>]

Description

Unbinds a system user from a group.

Parameters

groupName

Name of the system group from which to unbind the user.

userName

Name of the system user to unbind from the group.

policyName

Command policy to unbind from the group.

[Top](#)

show system group

Synopsis

show system group [<groupName>]

Description

Displays information about all system groups configured on the appliance, or about the specified group.

Parameters

groupName

Name of the system group about which to display information.

[Top](#)

set system group

Synopsis

set system group <groupName> [-promptString <string>] [-timeout <secs>]

Description

Modifies the specified parameters of a system group.

Parameters

groupName

Name of system group to be modified.

promptString

String to display at the command-line prompt. Can consist of letters, numbers, hyphen (-), period (.), hash (#), space (), at (@), equal (=), colon (:), underscore (_),

and the following variables: * %u - Will be replaced by the user name. * %h - Will be replaced by the hostname of the NetScaler appliance. * %t - Will be replaced by the current time in 12-hour format. * %T - Will be replaced by the current time in 24-hour format. * %d - Will be replaced by the current date. * %s - Will be replaced by the state of the NetScaler appliance. Note: The 63-character limit for the length of the string does not apply to the characters that replace the variables.

timeout

CLI session inactivity timeout, in seconds. Timeout cannot have values in between 1 and 9. Maximum value: 100000000

[Top](#)

unset system group

Synopsis

unset system group <groupName> [-promptString] [-timeout]

Description

Use this command to remove system group settings. Refer to the set system group command for meanings of the arguments.

[Top](#)

system session

[[show](#) | [kill](#)]

show system session

Synopsis

show system session [<sid>]

Description

Displays information about all current system sessions, or about the specified session. The system might reclaim sessions with no active connections before expiry time.

Parameters

sid

ID of the system session about which to display information. Minimum value: 1

[Top](#)

kill system session

Synopsis

kill system session (<sid> | -all)

Description

Kills one system session, or all system sessions except the current session.

Parameters**sid**

ID of the system session to terminate. CLI users: You can get the session ID by using the show system session command. Minimum value: 1

all

Terminate all the system sessions except the current session.

[Top](#)

system cpu

stat system cpu

Synopsis

```
stat system cpu [<id>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile  
<input_filename>] [-clearstats ( basic | full )]
```

Description

Displays statistics of all CPUs available on the appliance, or statistics of the specified CPU.

Parameters**id**

ID of the CPU for which to display statistics. Default value: 65535 Maximum value: 65534

clearstats

Clear the statistics / counters Possible values: basic, full

system memory

stat system memory

Synopsis

```
stat system memory [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile  
<input_filename>] [-clearstats ( basic | full )]
```

Description

Displays system-memory statistics.

Parameters**clearstats**

Clear the statistics / counters Possible values: basic, full

Example

```
stat system memory
```

system entitydata

[[rm](#) | [show](#)]

rm system entitydata

Synopsis

```
rm system entitydata [<type>] [<name>] [-allDeleted] [-allInactive] [-dataSource  
<string>] [-core <integer>]
```

Description

Removes the specified entity from historical charting along with all the associated counters till the current time stamp.

Parameters

type

Specify the entity type.

name

Specify the entity name.

allDeleted

Specify this if you would like to delete information about all deleted entities from the database.

allInactive

Specify this if you would like to delete information about all inactive entities from the database.

dataSource

Specifies the source which contains all the stored counter values.

core

Specify core ID of the PE in nCore.

[Top](#)

show system entitydata

Synopsis

```
show system entitydata <type> <name> <counters> [-startTime <string> | (-last  
<integer> [<unit>])] [-endTime <string>] [-dataSource <string>] [-core <integer>]
```

Description

Display the historical data for entity specific counters.

Parameters

type

Specify the entity type.

name

Specify the entity name.

counters

Specify the counters to be collected.

startTime

Specify start time in mmddyyyyhhmm to start collecting values from that timestamp.

endTime

Specify end time in mmddyyyyhhmm upto which values have to be collected.

last

Last is literal way of saying a certain time period from the current moment.

Example: -last 1 hour, -last 1 day, et cetera. Default value: 1

dataSource

Specifies the source which contains all the stored counter values.

core

Specify core ID of the PE in nCore.

Example

```
show system entitydata lbvserver v1 totalrequests -  
last 1 days
```

[Top](#)

system entity

show system entity

Synopsis

```
show system entity <type> [-dataSource <string>] [-core <integer>]
```

Description

Display entities in historical data.

Parameters

type

Specify the entity type.

dataSource

Specifies the source which contains all the stored counter values.

core

Specify core ID of the PE in nCore.

Example

```
show system entity lbvserver
```

system globaldata

show system globaldata

Synopsis

```
show system globaldata <counters> [<countergroup>] [-startTime <string> | (-last  
<integer> [<unit>])] [-endTime <string>] [-dataSource <string>] [-core <integer>]
```

Description

Display historical data for global counters.

Parameters

counters

Specify the counters to be collected.

countergroup

Specify the (counter) group name which contains all the counters specific to this particular group.

startTime

Specify start time in mmddyyyyhhmm to start collecting values from that timestamp.

endTime

Specify end time in mmddyyyyhhmm upto which values have to be collected.

last

Last is literal way of saying a certain time period from the current moment.
Example: -last 1 hour, -last 1 day, et cetera. Default value: 1

dataSource

Specifies the source which contains all the stored counter values.

core

Specify core ID of the PE in nCore.

Example

```
show system globaldata cpu_usage -last 1 hours
```


system counters

show system counters

Synopsis

show system counters [<countergroup>] [-dataSource <string>]

Description

Display entities in historical data.

Parameters

countergroup

Specify the (counter) group name which contains all the counters specific tot his particular group.

dataSource

Specifies the source which contains all the stored counter values.

system countergroup

show system countergroup

Synopsis

show system countergroup [-dataSource <string>]

Description

Display available counter groups.

Parameters

dataSource

Specifies the source which contains all the stored counter values.

system entitytype

show system entitytype

Synopsis

show system entitytype [-dataSource <string>]

Description

Display available entity types.

Parameters

dataSource

Specifies the source which contains all the stored counter values.

system eventhistory

show system eventhistory

Synopsis

show system eventhistory [-startTime <string> | (-last <integer> [<unit>])] [-endTime <string>] -dataSource <string>

Description

Display events in historical data.

Parameters

startTime

Specify start time in mmddyyyyhhmm to start collecting values from that timestamp.

endTime

Specify end time in mmddyyyyhhmm upto which values have to be collected.

last

Last is literal way of saying a certain time period from the current moment.

Example: -last 1 hour, -last 1 day, et cetera. Default value: 1

dataSource

Specifies the source which contains all the stored counter values.

system core

show system core

Synopsis

show system core [-dataSource <string>]

Description

Display entities in historical data.

Parameters

dataSource

Specifies the source which contains all the stored counter values.

system dataSource

show system dataSource

Synopsis

show system dataSource [<dataSource>]

Description

Display entities in historical data.

Parameters**dataSource**

Specifies the source which contains all the stored counter values.

system global

[[bind](#) | [unbind](#) | [show](#)]

bind system global

Synopsis

bind system global [<policyName> [-priority <positive_integer>]]

Description

Binds policies globally.

Parameters**policyName**

Name of the policy to bind globally.

[Top](#)

unbind system global

Synopsis

unbind system global <policyName>

Description

Unbinds a globally bound policy.

Parameters**policyName**

Name of the globally bound policy to unbind.

[Top](#)

show system global

Synopsis

show system global

Description

Displays information about all global policy bindings.

[Top](#)

system collectionparam

[[set](#) | [unset](#) | [show](#)]

set system collectionparam

Synopsis

set system collectionparam [-logLevel <string>] [-dataPath <string>]

Description

Modifies a collection parameters for historical charting in nscollect.ini file.

Parameters

communityName

SNMPv1 community name for authentication.

logLevel

specify the log level. Possible values CRITICAL, WARNING, INFO, DEBUG1, DEBUG2

dataPath

specify the data path to the database.

[Top](#)

unset system collectionparam

Synopsis

unset system collectionparam [-logLevel] [-dataPath]

Description

Use this command to remove system collectionparam settings. Refer to the set system collectionparam command for meanings of the arguments.

[Top](#)

show system collectionparam

Synopsis

show system collectionparam

Description

Displays collection parameters for historical charting present in nscollect.ini file.

[Top](#)

system parameter

[[set](#) | [unset](#) | [show](#)]

set system parameter

Synopsis

set system parameter [-rbaOnResponse (ENABLED | DISABLED)] [-promptString <string>] [-natPcbForceFlushLimit <positive_integer>] [-natPcbRstOnTimeout (ENABLED | DISABLED)] [-timeout <secs>]

Description

Modifies the specified system parameters.

Parameters

rbaOnResponse

Enable or disable Role-Based Authentication (RBA) on responses. Possible values: ENABLED, DISABLED Default value: ENABLED

promptString

String to display at the command-line prompt. Can consist of letters, numbers, hyphen (-), period (.), hash (#), space (), at (@), equal (=), colon (:), underscore (_), and the following variables: *%u - Will be replaced by the user name. *%h - Will be replaced by the hostname of the NetScaler appliance. *%t - Will be replaced by the current time in 12-hour format. *%T - Will be replaced by the current time in 24-hour format. *%d - Will be replaced by the current date. *%s - Will be replaced by the state of the NetScaler appliance. Note: The 63-character limit for the length of the string does not apply to the characters that replace the variables.

natPcbForceFlushLimit

Flush the system if the number of Network Address Translation Protocol Control Blocks (NATPCBs) exceeds this value. Default value: 2147483647 Minimum value: 1000

natPcbRstOnTimeout

Send a reset signal to client and server connections when their NATPCBs time out. Avoids the buildup of idle TCP connections on both the sides. Possible values: ENABLED, DISABLED Default value: DISABLED

timeout

CLI session inactivity timeout, in seconds. Timeout cannot have values in between 1 and 9. Maximum value: 100000000

[Top](#)

unset system parameter

Synopsis

```
unset system parameter [-rbaOnResponse] [-promptString] [-natPcbForceFlushLimit] [-natPcbRstOnTimeout] [-timeout]
```

Description

Use this command to remove system parameter settings. Refer to the set system parameter command for meanings of the arguments.

[Top](#)

show system parameter

Synopsis

```
show system parameter
```

Description

Displays information about the system parameters.

[Top](#)

system backup

[[create](#) | [restore](#) | [rm](#) | [show](#)]

create system backup

Synopsis

create system backup [<fileName>] [-level (basic | full)] [-comment <string>]

Description

Creates a backup file (*.tgz) that is stored in the /var/ns_sys_backup/ directory. This file can be used to restore the appliance by using the "restore system backup" command.

Parameters

fileName

Name of the backup file (*.tgz) to be restored.

level

Level of data to be backed up. Possible values: basic, full Default value: CLEARCONF1

comment

Comment specified at the time of creation of the backup file (*.tgz).

[Top](#)

restore system backup

Synopsis

restore system backup <fileName>

Description

Restores an appliance by using the backup file (*.tgz) that was created by using the "create system backup" command.

Parameters

fileName

Name of the backup file (*.tgz) to be restored.

[Top](#)

rm system backup

Synopsis

rm system backup <fileName>

Description

Removes a backup file (*.tgz) that was created by using the "create system backup" command.

Parameters

fileName

Name of the backup file(*.tgz) to be restored.

[Top](#)

show system backup**Synopsis**

show system backup [<fileName>]

Description

Retrieves the backed up files that were created in the appliance.

Parameters

fileName

Name of the backup file(*.tgz) to be restored.

[Top](#)

TM Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [tm sessionPolicy](#)
- ♦ [tm sessionAction](#)
- ♦ [tm trafficPolicy](#)
- ♦ [tm formSSOAction](#)
- ♦ [tm samlSSOProfile](#)
- ♦ [tm trafficAction](#)
- ♦ [tm global](#)
- ♦ [tm sessionParameter](#)

tm sessionPolicy

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add tm sessionPolicy**Synopsis**

add tm sessionPolicy <name> <rule> <action>

Description

Creates a traffic management (TM) session policy, which is applied after the user logs on to the AAA virtual server, to customize user sessions.

Parameters

name

Name for the session policy. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Cannot be changed after a session policy is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy').

rule

Expression, against which traffic is evaluated. Written in the classic syntax. Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>". The following requirements apply only to the NetScaler CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action

Action to be applied to connections that match this policy.

[Top](#)

rm tm sessionPolicy

Synopsis

```
rm tm sessionPolicy <name>
```

Description

Removes an existing traffic management (TM) session policy.

Parameters

name

Name of the session policy to remove.

[Top](#)

set tm sessionPolicy

Synopsis

```
set tm sessionPolicy <name> [-rule <expression>] [-action <string>]
```


Description

Modifies the rule or action of an existing traffic management (TM) session policy.

Parameters

name

Name of the session policy to modify.

rule

Expression, against which traffic is evaluated. Written in the classic syntax. Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>". The following requirements apply only to the NetScaler CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action

Action to be applied to connections that match this policy.

[Top](#)

unset tm sessionPolicy

Synopsis

```
unset tm sessionPolicy <name> [-rule] [-action]
```

Description

Use this command to remove tm sessionPolicy settings. Refer to the set tm sessionPolicy command for meanings of the arguments.

[Top](#)

show tm sessionPolicy

Synopsis

```
show tm sessionPolicy [<name>]
```

Description

Displays information about all the configured traffic management (TM) session policies, or displays detailed information about the specified TM session policy.

Parameters

name

Name of the session policy for which to display detailed information.

[Top](#)

tm sessionAction

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add tm sessionAction

Synopsis

```
add tm sessionAction <name> [-sessTimeout <mins>] [-defaultAuthorizationAction  
( ALLOW | DENY )] [-SSO ( ON | OFF )] [-ssoCredential ( PRIMARY | SECONDARY )] [-  
ssoDomain <string>] [-httpOnlyCookie ( YES | NO )] [-kcdAccount <string>] [-  
persistentCookie ( ON | OFF )] [-persistentCookieValidity <mins>] [-homePage <URL>]
```

Description

Creates a session action (profile) that allows you to override global settings for any of the session parameters.

Parameters

name

Name for the session action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after a session action is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

sessTimeout

Session timeout, in minutes. If there is no traffic during the timeout period, the user is disconnected and must reauthenticate to access intranet resources. Minimum value: 1

defaultAuthorizationAction

Allow or deny access to content for which there is no specific authorization policy. Possible values: ALLOW, DENY

SSO

Use single sign-on (SSO) to log users on to all web applications automatically after they authenticate, or pass users to the web application logon page to authenticate to each application individually. Possible values: ON, OFF Default value: OFF

ssoCredential

Use the primary or secondary authentication credentials for single sign-on (SSO). Possible values: PRIMARY, SECONDARY

ssoDomain

Domain to use for single sign-on (SSO).

httpOnlyCookie

Allow only an HTTP session cookie, in which case the cookie cannot be accessed by scripts. Possible values: YES, NO

kcdAccount

Kerberos constrained delegation account name

persistentCookie

Enable or disable persistent SSO cookies for the traffic management (TM) session. A persistent cookie remains on the user device and is sent with each HTTP request. The cookie becomes stale if the session ends. This setting is overwritten if a traffic action sets persistent cookie to OFF. Note: If persistent cookie is enabled, make sure you set the persistent cookie validity. Possible values: ON, OFF

persistentCookieValidity

Integer specifying the number of minutes for which the persistent cookie remains valid. Can be set only if the persistent cookie setting is enabled. Minimum value: 1

homePage

Web address of the home page that a user is displayed when authentication vserver is bookmarked and used to login.

[Top](#)

rm tm sessionAction**Synopsis**

```
rm tm sessionAction <name>
```

Description

Deletes an existing session action.

Parameters**name**

Name of the session action to delete.

[Top](#)

set tm sessionAction**Synopsis**

```
set tm sessionAction <name> [-sessTimeout <mins>] [-defaultAuthorizationAction  
( ALLOW | DENY )] [-SSO ( ON | OFF )] [-ssoCredential ( PRIMARY | SECONDARY )] [-  
ssoDomain <string>] [-kcdAccount <string>] [-httpOnlyCookie ( YES | NO )] [-  
persistentCookie ( ON | OFF )] [-persistentCookieValidity <positive_integer>] [-  
homePage <URL>]
```

Description

Modifies the specified parameters of an existing session action.

Parameters**name**

Name of the session action to modify.

sessTimeout

Session timeout, in minutes. If there is no traffic during the timeout period, the user is disconnected and must reauthenticate to access intranet resources. Minimum value: 1

defaultAuthorizationAction

Allow or deny access to content for which there is no specific authorization policy.
Possible values: ALLOW, DENY

SSO

Use single sign-on (SSO) to log users on to all web applications automatically after they authenticate, or pass users to the web application logon page to authenticate to each application individually. Possible values: ON, OFF Default value: OFF

ssoCredential

Use the primary or secondary authentication credentials for single sign-on (SSO).
Possible values: PRIMARY, SECONDARY

ssoDomain

Domain to use for single sign-on (SSO).

kcdAccount

Kerberos constrained delegation account name

httpOnlyCookie

Allow only an HTTP session cookie, in which case the cookie cannot be accessed by scripts. Possible values: YES, NO

persistentCookie

Enable or disable persistent SSO cookies for the traffic management (TM) session. A persistent cookie remains on the user device and is sent with each HTTP request. The cookie becomes stale if the session ends. This setting is overwritten if a traffic action sets persistent cookie to OFF. Note: If persistent cookie is enabled, make sure you set the persistent cookie validity. Possible values: ON, OFF

persistentCookieValidity

Integer specifying the number of minutes for which the persistent cookie remains valid. Can be set only if the persistent cookie setting is enabled. Minimum value: 1

homePage

Web address of the home page that a user is displayed when authentication vserver is bookmarked and used to login.

[Top](#)

unset tm sessionAction

Synopsis

```
unset tm sessionAction <name> [-sessTimeout] [-defaultAuthorizationAction] [-SSO] [-ssoCredential] [-ssoDomain] [-kcdAccount] [-httpOnlyCookie] [-persistentCookie] [-persistentCookieValidity] [-homePage]
```

Description

Use this command to remove tm sessionAction settings. Refer to the set tm sessionAction command for meanings of the arguments.

[Top](#)

show tm sessionAction

Synopsis

show tm sessionAction [<name>]

Description

Displays information about all configured traffic management (TM) session actions, or detailed information about the specified TM session action.

Parameters

name

Name of the existing traffic management (TM) session action for which to display detailed information.

[Top](#)

tm trafficPolicy

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#) | [stat](#)]

add tm trafficPolicy

Synopsis

add tm trafficPolicy <name> <rule> <action>

Description

Adds a traffic policy to use for setting connection timeout, single sign-on, and initiating logout. The policy sets the characteristics of application traffic at run time.

Parameters

name

Name for the traffic policy. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the policy is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy').

rule

Expression, against which traffic is evaluated. Written in the classic syntax. Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>". The following requirements apply only to the NetScaler CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action

Name of the action to apply to requests or connections that match this policy.

[Top](#)

rm tm trafficPolicy

Synopsis

rm tm trafficPolicy <name>

Description

Removes an existing traffic policy.

Parameters

name

Name of the traffic policy to remove.

[Top](#)

set tm trafficPolicy

Synopsis

set tm trafficPolicy <name> [-rule <expression>] [-action <string>]

Description

Modifies the specified parameters of an existing traffic policy.

Parameters

name

Name of the traffic policy to modify.

rule

Expression, against which traffic is evaluated. Written in the classic syntax. Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>". The following requirements apply only to the NetScaler CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action

Name of the action to apply to requests or connections that match this policy.

[Top](#)

unset tm trafficPolicy

Synopsis

unset tm trafficPolicy <name> [-rule] [-action]

Description

Use this command to remove tm trafficPolicy settings. Refer to the set tm trafficPolicy command for meanings of the arguments.

[Top](#)

show tm trafficPolicy

Synopsis

show tm trafficPolicy [<name>]

Description

Displays information about all configured traffic management (TM) traffic policies, or displays detailed information about the specified TM traffic policy.

Parameters

name

Name of the traffic policy for which to display detailed information.

[Top](#)

stat tm trafficPolicy

Synopsis

stat tm trafficPolicy [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-clearstats (basic | full)]

Description

Display Traffic Management traffic policy statistics.

Parameters

name

The name of the TM traffic policy for which statistics will be displayed. If not given statistics are shown for all policies.

clearstats

Clear the statistics / counters Possible values: basic, full

Example

```
stat tm trafficpolicy.
```

[Top](#)

tm formSSOAction

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add tm formSSOAction

Synopsis

```
add tm formSSOAction <name> -actionURL <URL> -userField <string> -passwdField  
<string> -ssoSuccessRule <expression> [-nameValuePair <string>] [-responsesize  
<positive_integer>] [-nvtype ( STATIC | DYNAMIC )] [-submitMethod ( GET | POST )]
```

Description

Creates a form-based single sign-on traffic profile (action.) Form-based single sign-on allows users to access web applications that require an HTML form-based logon without having to type their password again for each new application.

Parameters

name

Name for the new form-based single sign-on profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an SSO action is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

actionURL

URL to which the completed form is submitted.

userField

Name of the form field in which the user types in the user ID.

passwdField

Name of the form field in which the user types in the password.

ssoSuccessRule

Expression, that checks to see if single sign-on is successful.

nameValuePair

Name-value pair attributes to send to the server in addition to sending the username and password. Value names are separated by an ampersand (&) (for example, name1=value1&name2=value2).

responsesize

Number of bytes, in the response, to parse for extracting the forms. Default value: 8096

nvtype

Type of processing of the name-value pair. If you specify STATIC, the values configured by the administrator are used. For DYNAMIC, the response is parsed, and the form is extracted and then submitted. Possible values: STATIC, DYNAMIC Default value: NS_ACT_FSSO_NV_DYNAMIC

submitMethod

HTTP method used by the single sign-on form to send the logon credentials to the logon server. Applies only to STATIC name-value type. Possible values: GET, POST
Default value: NS_ACT_FSSO_SUBMIT_GET

[Top](#)**rm tm formSSOAction****Synopsis**

rm tm formSSOAction <name>

Description

Deletes an existing form-based single sign-on traffic profile (action.)

Parameters**name**

Name of the form-based single sign-on profile to delete.

[Top](#)**set tm formSSOAction****Synopsis**

set tm formSSOAction <name> [-actionURL <URL>] [-userField <string>] [-passwdField <string>] [-ssoSuccessRule <expression>] [-responsesize <positive_integer>] [-nameValuePair <string>] [-nvtype (STATIC | DYNAMIC)] [-submitMethod (GET | POST)]

Description

Modifies the specified attributes of a form-based single sign-on traffic profile (action.)

Parameters**name**

Name of the form-based single sign-on profile (action) to modify.

actionURL

URL to which the completed form is submitted.

userField

Name of the form field in which the user types in the user ID.

passwdField

Name of the form field in which the user types in the password.

ssoSuccessRule

Expression, that checks to see if single sign-on is successful.

responsesize

Number of bytes, in the response, to parse for extracting the forms. Default value: 8096

nameValuePair

Name-value pair attributes to send to the server in addition to sending the username and password. Value names are separated by an ampersand (&) (for example, name1=value1&name2=value2).

nvtype

Type of processing of the name-value pair. If you specify STATIC, the values configured by the administrator are used. For DYNAMIC, the response is parsed, and the form is extracted and then submitted. Possible values: STATIC, DYNAMIC Default value: NS_ACT_FSSO_NV_DYNAMIC

submitMethod

HTTP method used by the single sign-on form to send the logon credentials to the logon server. Applies only to STATIC name-value type. Possible values: GET, POST Default value: NS_ACT_FSSO_SUBMIT_GET

[Top](#)

unset tm formSSOAction

Synopsis

```
unset tm formSSOAction <name> [-responsesize] [-nameValuePair] [-nvtype] [-submitMethod]
```

Description

Use this command to remove tm formSSOAction settings. Refer to the set tm formSSOAction command for meanings of the arguments.

[Top](#)

show tm formSSOAction

Synopsis

```
show tm formSSOAction [<name>]
```

Description

Displays information about all configured form-based single sign-on actions, or displays detailed information about the specified action.

Parameters

name

Name of the SSO action for which to display detailed information.

[Top](#)

tm samlSSOProfile

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add tm samlSSOProfile

Synopsis

```
add tm samlSSOProfile <name> -samlSigningCertName <string> -
assertionConsumerServiceURL <URL> -relaystateRule <expression> [-sendPassword ( ON
| OFF )] [-samlIssuerName <string>]
```

Description

Creates a SAML single sign-on profile. This profile is employed in triggering saml assertion to a target service based on traffic profile.

Parameters

name

Name for the new saml single sign-on profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an SSO action is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

samlSigningCertName

Name of the signing authority as given in the SAML server's SSL certificate.

assertionConsumerServiceURL

URL to which the assertion is to be sent.

relaystateRule

Expression to extract relaystate to be sent along with assertion.

sendPassword

Option to send password in assertion. Possible values: ON, OFF Default value: OFF

samlIssuerName

The name to be used in requests sent from Netscaler to IdP to uniquely identify Netscaler.

[Top](#)

rm tm samlSSOProfile

Synopsis

```
rm tm samlSSOProfile <name>
```

Description

Deletes an existing saml single sign-on traffic profile.

Parameters

name

Name for the new saml single sign-on profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an SSO action is created. The following requirement applies

only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

[Top](#)

set tm samlSSOProfile

Synopsis

```
set tm samlSSOProfile <name> [-samlSigningCertName <string>] [-assertionConsumerServiceURL <URL>] [-sendPassword ( ON | OFF )] [-samlIssuerName <string>] [-relaystateRule <expression>]
```

Description

Modifies the specified attributes of a saml single sign-on traffic profile.

Parameters

name

Name for the new saml single sign-on profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an SSO action is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

samlSigningCertName

Name of the signing authority as given in the SAML server's SSL certificate.

assertionConsumerServiceURL

URL to which the assertion is to be sent.

sendPassword

Option to send password in assertion. Possible values: ON, OFF Default value: OFF

samlIssuerName

The name to be used in requests sent from Netscaler to IdP to uniquely identify Netscaler.

relaystateRule

Expression to extract relaystate to be sent along with assertion.

[Top](#)

unset tm samlSSOProfile

Synopsis

```
unset tm samlSSOProfile <name> [-samlSigningCertName] [-sendPassword] [-samlIssuerName]
```

Description

Use this command to remove tm samlSSOProfile settings. Refer to the set tm samlSSOProfile command for meanings of the arguments.

[Top](#)

show tm samlSSOProfile

Synopsis

show tm samlSSOProfile [<name>]

Description

Displays information about all configured saml single sign-on profiles, or displays detailed information about the specified action.

Parameters

name

Name for the new saml single sign-on profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an SSO action is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

[Top](#)

tm trafficAction

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add tm trafficAction

Synopsis

add tm trafficAction <name> [-appTimeout <mins>] [-SSO (ON | OFF)] [-formSSOAction <string>]] [-persistentCookie (ON | OFF)] [-InitiateLogout (ON | OFF)] [-kcdAccount <string>] [-samlSSOProfile <string>]

Description

Creates a traffic action to set traffic characteristics at run time. You can create a traffic action for an application that is installed in the internal network (for example, an action that defines the destination IP address and destination port, and sets the amount of time a user can stay logged on to the application, such as 15 minutes).

Parameters

name

Name for the traffic action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after a traffic action is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

appTimeout

Time interval, in minutes, of user inactivity after which the connection is closed.
Minimum value: 1 Maximum value: 715827

SSO

Use single sign-on for the resource that the user is accessing now. Possible values: ON, OFF

formSSOAction

Name of the configured form-based single sign-on profile.

persistentCookie

Use persistent cookies for the traffic session. A persistent cookie remains on the user device and is sent with each HTTP request. The cookie becomes stale if the session ends. Possible values: ON, OFF

InitiateLogout

Initiate logout for the traffic management (TM) session if the policy evaluates to true. The session is then terminated after two minutes. Possible values: ON, OFF

kcdAccount

Kerberos constrained delegation account name Default value: "None"

samlSSOProfile

Profile to be used for doing SAML SSO to remote relying party

[Top](#)

rm tm trafficAction

Synopsis

rm tm trafficAction <name>

Description

Removes an existing traffic action.

Parameters

name

Name of the traffic action to remove.

[Top](#)

set tm trafficAction

Synopsis

set tm trafficAction <name> [-appTimeout <mins>] [-SSO (ON | OFF)] [-formSSOAction <string>] [-persistentCookie (ON | OFF)] [-InitiateLogout (ON | OFF)] [-kcdAccount <string>] [-samlSSOProfile <string>]

Description

Modifies the specified parameters of an existing traffic action.

Parameters

name

Name of the traffic action to modify.

appTimeout

Time interval, in minutes, of user inactivity after which the connection is closed.
Minimum value: 1 Maximum value: 715827

SSO

Use single sign-on for the resource that the user is accessing now. Possible values:
ON, OFF

formSSOAction

Name of the configured form-based single sign-on profile.

persistentCookie

Use persistent cookies for the traffic session. A persistent cookie remains on the user device and is sent with each HTTP request. The cookie becomes stale if the session ends. Possible values: ON, OFF

InitiateLogout

Initiate logout for the traffic management (TM) session if the policy evaluates to true. The session is then terminated after two minutes. Possible values: ON, OFF

kcdAccount

Kerberos constrained delegation account name Default value: "None"

samlSSOProfile

Profile to be used for doing SAML SSO to remote relying party

[Top](#)

unset tm trafficAction**Synopsis**

```
unset tm trafficAction <name> [-persistentCookie] [-kcdAccount]
```

Description

Use this command to remove tm trafficAction settings. Refer to the set tm trafficAction command for meanings of the arguments.

[Top](#)

show tm trafficAction**Synopsis**

```
show tm trafficAction [<name>]
```

Description

Displays information about all configured traffic management (TM) traffic actions, or displays detailed information about the specified TM traffic action.

Parameters**name**

Name of the traffic action for which to display detailed information.

[Top](#)

tm global

[[bind](#) | [unbind](#) | [show](#)]

bind tm global

Synopsis

bind tm global [-policyName <string> [-priority <positive_integer>]]

Description

Binds traffic, sessions, nslog, and syslog policies to traffic management (TM) Global.

Parameters

policyName

Name of the policy that you are binding.

[Top](#)

unbind tm global

Synopsis

unbind tm global -policyName <string>

Description

Unbinds a globally bound traffic session policy.

Parameters

policyName

Name of the policy to unbind.

[Top](#)

show tm global

Synopsis

show tm global

Description

Displays information about TM global bindings.

[Top](#)

tm sessionParameter

[[set](#) | [unset](#) | [show](#)]

set tm sessionParameter

Synopsis

```
set tm sessionParameter [-sessTimeout <mins>] [-defaultAuthorizationAction ( ALLOW | DENY )] [-SSO ( ON | OFF )] [-ssoCredential ( PRIMARY | SECONDARY )] [-ssoDomain <string>] [-kcdAccount <string>] [-httpOnlyCookie ( YES | NO )] [-persistentCookie ( ON | OFF )] [-persistentCookieValidity <positive_integer>] [-homePage <URL>]
```

Description

Sets global parameters for the traffic management (TM) session. Parameters defined when adding a traffic session action override these parameters.

Parameters

sessTimeout

Session timeout, in minutes. If there is no traffic during the timeout period, the user is disconnected and must reauthenticate to access the intranet resources. Default value: 30 Minimum value: 1

defaultAuthorizationAction

Allow or deny access to content for which there is no specific authorization policy. Possible values: ALLOW, DENY Default value: NS_ALLOW

SSO

Log users on to all web applications automatically after they authenticate, or pass users to the web application logon page to authenticate for each application. Possible values: ON, OFF Default value: OFF

ssoCredential

Use primary or secondary authentication credentials for single sign-on. Possible values: PRIMARY, SECONDARY Default value: VPN_SESS_ACT_USE_PRIMARY_CREDENTIALS

ssoDomain

Domain to use for single sign-on.

kcdAccount

Kerberos constrained delegation account name

httpOnlyCookie

Allow only an HTTP session cookie, in which case the cookie cannot be accessed by scripts. Possible values: YES, NO Default value: VPN_SESS_ACT_HTTPONLYCOOKIE_ALLOW

persistentCookie

Use persistent SSO cookies for the traffic session. A persistent cookie remains on the user device and is sent with each HTTP request. The cookie becomes stale if the session ends. Possible values: ON, OFF Default value: OFF

persistentCookieValidity

Integer specifying the number of minutes for which the persistent cookie remains valid. Can be set only if the persistence cookie setting is enabled. Minimum value: 1

homePage

Web address of the home page that a user is displayed when authentication vserver is bookmarked and used to login. Default value: "None"

[Top](#)

unset tm sessionParameter**Synopsis**

```
unset tm sessionParameter [-sessTimeout] [-SSO] [-ssoDomain] [-kcdAccount] [-persistentCookie] [-homePage] [-defaultAuthorizationAction] [-ssoCredential] [-httpOnlyCookie] [-persistentCookieValidity]
```

Description

Resets the attributes of the specified traffic session parameters. Attributes for which a default value is available revert to their default values. Refer to the `set tm sessionParameter` command for descriptions of the parameters..Refer to the `set tm sessionParameter` command for meanings of the arguments.

[Top](#)

show tm sessionParameter**Synopsis**

```
show tm sessionParameter
```

Description

Displays information about traffic session parameters.

[Top](#)

Transform Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [transform profile](#)
- ♦ [transform action](#)
- ♦ [transform policy](#)
- ♦ [transform policylabel](#)
- ♦ [transform global](#)

transform profile

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add transform profile**Synopsis**

```
add transform profile <name> [-type URL]
```

Description

Creates a URL transformation profile, which contains a list of actions that define how the URLs in a request or response are to be modified. NOTE: In the URL Transformation feature (unlike all other NetScaler features), profile and action are not synonymous but refer to distinct entities. You must create the profile first, and then the actions.

Parameters

name

Name for the URL transformation profile. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space (), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the URL transformation profile is added. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, my transform profile or my transform profile).

type

Type of transformation. Always URL for URL Transformation profiles. Possible values: URL

[Top](#)

rm transform profile

Synopsis

rm transform profile <name>

Description

Removes a URL Transformation profile.

Parameters

name

Name of the profile to remove.

[Top](#)

set transform profile

Synopsis

set transform profile <name> [-type URL] [-onlyTransformAbsURLinBody (ON | OFF)] [-comment <string>]

Description

Modifies the settings of a URL Transformation profile.

Parameters

name

Name of the profile to be modified.

type

Type of transformation. Always URL for URL Transformation profiles. Possible values: URL

onlyTransformAbsURLinBody

In the HTTP body, transform only absolute URLs. Relative URLs are ignored. Possible values: ON, OFF

comment

Any comments to preserve information about this URL Transformation profile.

[Top](#)

unset transform profile

Synopsis

unset transform profile <name> [-type] [-onlyTransformAbsURLinBody] [-comment]

Description

Use this command to remove transform profile settings. Refer to the set transform profile command for meanings of the arguments.

[Top](#)

show transform profile

Synopsis

show transform profile [<name>]

Description

Displays the current settings for the specified URL Transformation profile. If no URL Transformation profile name is specified, displays a list of all URL Transformation profiles currently configured on the NetScaler appliance.

Parameters

name

Name of the profile.

[Top](#)

transform action

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add transform action

Synopsis

add transform action <name> <profileName> <priority> [-state (ENABLED | DISABLED)]

Description

Creates a URL Transformation action, which defines how a specific element in URLs in the request or response is to be modified. NOTE: In the URL Transformation feature

(unlike all other NetScaler features), profile and action are not synonymous but refer to distinct entities. You must create the profile first, and then the actions.

Parameters

name

Name for the URL transformation action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space (), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the URL Transformation action is added. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, my transform action or my transform action).

profileName

Name of the URL Transformation profile with which to associate this action.

priority

Positive integer specifying the priority of the action within the profile. A lower number specifies a higher priority. Must be unique within the list of actions bound to the profile. Policies are evaluated in the order of their priority numbers, and the first policy that matches is applied. Minimum value: 1 Maximum value: 2147483647

state

Enable or disable this action. Possible values: ENABLED, DISABLED Default value: GENENABLED

[Top](#)

rm transform action

Synopsis

```
rm transform action <name>
```

Description

Removes a URL Transformation action.

Parameters

name

Name of the action.

[Top](#)

set transform action

Synopsis

```
set transform action <name> [-priority <positive_integer>] [-reqUrlFrom <expression>]
[-reqUrlInto <expression>] [-resUrlFrom <expression>] [-resUrlInto <expression>] [-
cookieDomainFrom <expression>] [-cookieDomainInto <expression>] [-state ( ENABLED |
DISABLED )] [-comment <string>]
```

Description

Modifies the settings of the specified URL Transformation action.

Parameters

name

Name of the URL Transformation action to modify.

priority

Positive integer specifying the priority of the action within the profile. A lower number specifies a higher priority. Must be unique within the list of actions bound to the profile. Policies are evaluated in the order of their priority numbers, and the first policy that matches is applied. Minimum value: 1 Maximum value: 2147483647

reqUrlFrom

PCRE-format regular expression that describes the request URL pattern to be transformed.

reqUrlInto

PCRE-format regular expression that describes the transformation to be performed on URLs that match the reqUrlFrom pattern.

resUrlFrom

PCRE-format regular expression that describes the response URL pattern to be transformed.

resUrlInto

PCRE-format regular expression that describes the transformation to be performed on URLs that match the resUrlFrom pattern.

cookieDomainFrom

Pattern that matches the domain to be transformed in Set-Cookie headers.

cookieDomainInto

PCRE-format regular expression that describes the transformation to be performed on cookie domains that match the cookieDomainFrom pattern. NOTE: The cookie domain to be transformed is extracted from the request.

state

Enable or disable this action. Possible values: ENABLED, DISABLED Default value: GENENABLED

comment

Any comments to preserve information about this URL Transformation action.

[Top](#)

unset transform action

Synopsis

```
unset transform action <name> [-reqUrlFrom] [-reqUrlInto] [-resUrlFrom] [-resUrlInto]
[-cookieDomainFrom] [-cookieDomainInto] [-state] [-comment]
```

Description

Use this command to remove transform action settings. Refer to the set transform action command for meanings of the arguments.

[Top](#)

show transform action

Synopsis

show transform action [<name>]

Description

Displays a list of all URL Transformation actions currently assigned to the specified profile.

Parameters

name

Name of the profile.

[Top](#)

transform policy

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#) | [stat](#) | [rename](#)]

add transform policy

Synopsis

add transform policy <name> <rule> <profileName> [-comment <string>] [-logAction <string>]

Description

Creates a URL Transformation policy, which specifies the requests and responses to be transformed by the associated profile.

Parameters

name

Name for the URL Transformation policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space (), at (@), equals (=), colon (:), and underscore characters. Can be changed after the URL Transformation policy is added. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, my transform policy or my transform policy).

rule

Expression, or name of a named expression, against which to evaluate traffic. Can be written in either default or classic syntax. Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>". The following requirements apply only to the NetScaler CLI: * If the expression includes blank spaces, the entire expression must be enclosed in double quotation marks. * If the expression itself includes double quotation marks, you must escape the quotations by using the \ character. *

Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

profileName

Name of the URL Transformation profile to use to transform requests and responses that match the policy.

comment

Any comments to preserve information about this URL Transformation policy.

logAction

Log server to use to log connections that match this policy.

[Top](#)

rm transform policy

Synopsis

rm transform policy <name>

Description

Removes the specified URL Transformation policy.

Parameters

name

Name of the policy to remove.

Example

```
rm transform policy trans_pol
```

[Top](#)

set transform policy

Synopsis

set transform policy <name> [-rule <expression>] [-profileName <string>] [-comment <string>] [-logAction <string>]

Description

Modifies the specified parameters of a URL Transformation policy.

Parameters

name

Name of the policy to modify.

rule

Expression, or name of a named expression, against which to evaluate traffic. Can be written in either default or classic syntax. Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For

example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>" The following requirements apply only to the NetScaler CLI: * If the expression includes blank spaces, the entire expression must be enclosed in double quotation marks. * If the expression itself includes double quotation marks, you must escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

profileName

Name of the URL Transformation profile to use to transform requests and responses that match the policy.

comment

Any comments to preserve information about this URL Transformation policy.

logAction

Log server to use to log connections that match this policy.

Example

```
set transform policy pol9 -rule "HTTP.REQ.HEADER(\
\"header\\").CONTAINS(\\\"qh2\\") "
```

[Top](#)

unset transform policy**Synopsis**

```
unset transform policy <name> [-comment] [-logAction]
```

Description

Removes the settings of an existing URL Transformation policy. Attributes for which a default value is available revert to their default values. See the set transform policy command for a description of the parameters..Refer to the set transform policy command for meanings of the arguments.

Example

```
unset transform policy pol9 -undefAction
```

[Top](#)

show transform policy**Synopsis**

```
show transform policy [<name>]
```

Description

Displays the current settings for the specified URL Transformation policy. If no policy name is specified, displays a list of all URL Transformation policies currently configured on the NetScaler appliance.

Parameters

name
Name of the URL Transformation policy.

[Top](#)

stat transform policy

Synopsis

```
stat transform policy [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-clearstats ( basic | full )]
```

Description

Displays statistics for the specified URL Transformation policy. If no policy name is specified, displays abbreviated statistics for all URL Transformation policies currently configured on the NetScaler appliance.

Parameters

name
Name of the policy.

clearstats
Clear the statistics / counters Possible values: basic, full

Example

```
stat transform policy
```

[Top](#)

rename transform policy

Synopsis

```
rename transform policy <name>@ <newName>@
```

Description

Renames a URL Transformation policy.

Parameters

name
Existing name of the policy.

newName

New name for the policy. Must begin with a letter, number, or the underscore character (`_`), and must contain only letters, numbers, and the hyphen (`-`), period (`.`) pound (`#`), space (), at (`@`), equals (`=`), colon (`:`), and underscore characters. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, `my transform policy` or `my transform policy`).

Example

```
rename transform policy oldname newname
```

[Top](#)

transform policylabel

[[add](#) | [rm](#) | [bind](#) | [unbind](#) | [show](#) | [stat](#) | [rename](#)]

add transform policylabel

Synopsis

```
add transform policylabel <labelName> <policylabeltype>
```

Description

Creates a URL Transformation policy label. A policy label is a tool for evaluating a set of policies in a specified order. By using a policy label, you can configure the URL Transformation feature to choose the next policy, invoke a different policy label, or terminate policy evaluation completely by looking at whether the previous policy evaluated to TRUE or FALSE.

Parameters

labelName

Name for the policy label. Must begin with a letter, number, or the underscore character (`_`), and must contain only letters, numbers, and the hyphen (`-`), period (`.`) pound (`#`), space (), at (`@`), equals (`=`), colon (`:`), and underscore characters. Can be changed after the URL Transformation policy label is added. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, `my transform policylabel` or `my transform policylabel`).

policylabeltype

Types of transformations allowed by the policies bound to the label. For URL transformation, always `http_req` (HTTP Request). Possible values: `http_req`

Example

```
add transform policylabel trans_policylabel
http_req
```

[Top](#)

rm transform policylabel

Synopsis

rm transform policylabel <labelName>

Description

Removes a URL Transformation policy label.

Parameters

labelName

Name of the policy label to remove.

Example

```
rm transform policylabel trans_policylabel
```

[Top](#)

bind transform policylabel

Synopsis

bind transform policylabel <labelName> <policyName> <priority>
[<gotoPriorityExpression>] [-invoke (<labelType> <labelName>)]

Description

Binds the specified URL Transformation policy to the specified policy label.

Parameters

labelName

Name of the URL Transformation policy label to which to bind the policy.

policyName

Name of the URL Transformation policy to bind to the policy label.

Example

```
i)      bind transform policylabel trans_policylabel
pol_1 1 2 -invoke reqvserver CURRENT
```

```
ii)      bind transform policylabel  
trans_policylabel pol_2 2
```

[Top](#)

unbind transform policylabel

Synopsis

unbind transform policylabel <labelName> <policyName> [-priority <positive_integer>]

Description

Unbinds the specified URL Transformation policy from the specified policy label.

Parameters

labelName

Name of the label from which to unbind the policy.

policyName

Name of the label to which to bind the policy.

priority

Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

```
unbind transform policylabel trans_policylabel  
pol_1
```

[Top](#)

show transform policylabel

Synopsis

show transform policylabel [<labelName>]

Description

Displays the current settings for the specified URL Transformation policy label. If no policy label is specified, displays a list of all URL Transformation policy labels currently configured on the NetScaler appliance.

Parameters

labelName

Name for the policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.), pound (#), space (), at (@), equals (=), colon (:), and underscore characters. Can be changed after the URL Transformation policy label is added. The following requirement applies only to the NetScaler CLI: If the name includes one or more

spaces, enclose the name in double or single quotation marks (for example, my transform policylabel or my transform policylabel).

Example

```
i)    show transform policylabel trans_policylabel
ii)   show transform policylabel
```

[Top](#)

stat transform policylabel

Synopsis

```
stat transform policylabel [<labelName>] [-detail] [-fullValues] [-ntimes
<positive_integer>] [-logFile <input_filename>] [-clearstats ( basic | full )]
```

Description

Displays statistics for the specified URL Transformation policy label. If no policy label name is provided, displays abbreviated statistics for all URL Transformation policy labels currently configured on the NetScaler appliance.

Parameters

labelName

The name of the URL Transformation policy label.

clearstats

Clear the statistics / counters Possible values: basic, full

[Top](#)

rename transform policylabel

Synopsis

```
rename transform policylabel <labelName>@ <newName>@
```

Description

Renames a URL Transformation policy label.

Parameters

labelName

Current name of the policy label.

newName

New name for the policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space (), at (@), equals (=), colon (:), and underscore characters. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, my transform policylabel or my transform policylabel).

Example

```
rename transform policylabel oldname newname
```

[Top](#)

transform global

[[bind](#) | [unbind](#) | [show](#)]

bind transform global

Synopsis

```
bind transform global <policyName> <priority> [<gotoPriorityExpression>] [-type
( REQ_OVERRIDE | REQ_DEFAULT )] [-invoke (<labelType> <labelName>)]
```

Description

Activates the specified URL Transformation policy for all traffic received by this NetScaler appliance. If you set policyName to a name that does not match an existing URL Transformation policy name, this command creates the policy, with the configuration that you specify.

Parameters**policyName**

Name of the policy. If you want to create the policy as well as activate it, specify a name for the policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space (), at (@), equals (=), colon (:), and underscore characters. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, my transform policy or my transform policy).

Example

```
bind transform global pol9 9
```

[Top](#)

unbind transform global

Synopsis

```
unbind transform global <policyName> [-type ( REQ_OVERRIDE | REQ_DEFAULT )] [-
priority <positive_integer>]
```

Description

Unbinds the specified URL Transformation policy from URL Transformation global.

Parameters

policyName

The name of the policy to be unbound.

priority

Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

```
unbind transform global pol9
```

[Top](#)

show transform global

Synopsis

show transform global [-type (REQ_OVERRIDE | REQ_DEFAULT)]

Description

Displays the policies bound to the specified URL Transformation global bind point. If no bind point is specified, displays a list of all policies bound to URL Transformation global.

Parameters

type

Specifies the bind point to which to bind the policy. Available settings function as follows: * REQ_OVERRIDE. Request override. Binds the policy to the priority request queue. * REQ_DEFAULT. Binds the policy to the default request queue. Possible values: REQ_OVERRIDE, REQ_DEFAULT

Example

```
show transform global
```

[Top](#)

Tunnel Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [tunnel trafficPolicy](#)
- ♦ [tunnel global](#)

tunnel trafficPolicy

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add tunnel trafficPolicy

Synopsis

add tunnel trafficPolicy <name> <rule> <action>

Description

Creates a tunnel traffic policy. A tunnel traffic policy defines the type of compression to be used for the tunneled traffic.

Parameters

name

Name for the tunnel traffic policy. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the policy is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy').

rule

Expression, against which traffic is evaluated. Written in classic or default syntax. Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>". The following requirements apply only to the NetScaler CLI: * If the expression includes blank spaces, the entire expression must be enclosed in double quotation marks. * If the expression itself includes double quotation marks, you must escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action

Name of the built-in compression action to associate with the policy.

Example

```
Example 1:
add tunnel trafficpolicy cmp_all_destport
"REQ.TCP.DESTPORT == 0-65535" GZIP
```

After creating above tunnel policy, it can be activated by binding it globally:

```
bind tunnel global cmp_all_destport
```

The policy is evaluated for all traffic flowing through the ssl-vpn tunnel, and compresses traffic for all TCP application ports.

```
Example 2:
The following tunnel policy disables compression
for all access from a specific subnet:
add tunnel trafficpolicy local_sub_nocmp "SOURCEIP
== 10.1.1.0 -netmask 255.255.255.0" NOCOMPRESS
bind tunnel global local_sub_nocmp
```

[Top](#)

rm tunnel trafficPolicy

Synopsis

```
rm tunnel trafficPolicy <name>
```

Description

Removes a tunnel traffic policy.

Parameters

name

Name of the tunnel traffic policy to remove.

Example

```
rm tunnel trafficpolicy tunnel_policy_name
The "show tunnel trafficpolicy" command shows all
tunnel policies that are currently defined.
```

[Top](#)

set tunnel trafficPolicy

Synopsis

```
set tunnel trafficPolicy <name> [-rule <expression>] [-action <string>]
```

Description

Modifies the specified parameters of an existing tunnel traffic policy.

Parameters

name

Name of the tunnel traffic policy to modify.

rule

Expression, against which traffic is evaluated. Written in classic or default syntax. Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>". The following requirements apply only to the NetScaler CLI: * If the expression includes blank spaces, the entire expression must be enclosed in double quotation marks. * If

the expression itself includes double quotation marks, you must escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action

Name of the built-in compression action to associate with the policy.

Example

```
add tunnel trafficpolicy cmp_all_destport
"REQ.TCP.DESTPORT == 0-65535" GZIP
set tunnel trafficpolicy cmp_all_destport -
action NOCOMPRESS
```

Above 'set' command changes action for policy cmp_all_destport from GZIP to NOCOMPRESS

[Top](#)

unset tunnel trafficPolicy

Synopsis

```
unset tunnel trafficPolicy <name> [-rule] [-action]
```

Description

Use this command to remove tunnel trafficPolicy settings. Refer to the set tunnel trafficPolicy command for meanings of the arguments.

[Top](#)

show tunnel trafficPolicy

Synopsis

```
show tunnel trafficPolicy [<name>]
```

Description

Displays information about all the configured tunnel traffic policies, or displays detailed information about the specified tunnel traffic policy.

Parameters

name

Name of the tunnel traffic policy for which to show detailed information.

Example

```
> show tunnel trafficpolicy
2 Tunnel policies:
1) Name: local_sub_nocmp Rule: SOURCEIP ==
10.1.1.0 -netmask 255.255.255.0
```

```

    Action: NOCOMPRESS
    Hits: 3

2) Name: cmp_all    Rule: REQ.TCP.DESTPORT ==
0-65535
    Action: GZIP
    Hits: 57125
    Bytes In:...796160      Bytes Out:... 197730
    Bandwidth saving...75.16%  Ratio 4.03:1
    Done

```

[Top](#)

tunnel global

[[bind](#) | [unbind](#) | [show](#)]

bind tunnel global

Synopsis

```
bind tunnel global (<policyName> [-priority <positive_integer>]) [-state ( ENABLED |
DISABLED )]
```

Description

Activates an existing tunnel traffic policy globally.

Parameters

policyName

Name of the tunnel traffic policy to activate or bind.

Example

```
add tunnel trafficpolicy cmp_all_destport
"REQ.TCP.DESTPORT == 0-65535" GZIP
```

After creating above tunnel policy, it can be activated by binding it globally:

```
bind tunnel global cmp_all_destport
```

After binding cmp_all_destport compression policy globally, the policy gets activated and the NetScaler will compress all TCP traffic accessed through ssl-vpn tunnel.

Globally active tunnel policies can be seen using command:

```
> show tunnel global
  1 Globally Active Tunnel Policies:
1) Policy Name: cmp_all_destport    Priority: 0
   Done
```

[Top](#)

unbind tunnel global

Synopsis

unbind tunnel global <policyName>

Description

Deactivates an active tunnel traffic policy.

Parameters

policyName

Name of the tunnel traffic policy to unbind or deactivate.

Example

Globally active tunnel policies can be seen using command:

```
> show tunnel global
 1 Globally Active Tunnel Policies:
1) Policy Name: cmp_all_destport   Priority: 0
Done
```

The globally active tunnel traffic policy can be deactivated on the NetScaler system by issuing the command:

```
unbind tunnel global cmp_all_destport
```

[Top](#)

show tunnel global

Synopsis

show tunnel global

Description

Displays globally active tunnel policies.

Example

```
> sh tunnel global
1) Policy Name: cmp_all_destport   Priority: 0
2) Policy Name: local_sub_nocmp   Priority: 500
Done
```

[Top](#)

Utility Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [nstrace](#)
- ♦ [scp](#)
- ♦ [shell](#)
- ♦ [install](#)
- ♦ [grep](#)
- ♦ [traceroute6](#)
- ♦ [traceroute](#)
- ♦ [ping6](#)
- ♦ [ping](#)
- ♦ [techsupport](#)
- ♦ [callhome](#)

nstrace

nstrace

Synopsis

```
nstrace [-nf <positive_integer>] [-time <secs>] [-size <positive_integer>] [-mode  
<mode> ...] [-tcpdump ( ENABLED | DISABLED ) [-perNIC ( ENABLED | DISABLED )]] [-  
name <string> [-id <string>]] [-filter <expression> [-link ( ENABLED | DISABLED )]]
```

Description

Invokes the nstrace program to log traffic flowing through the NetScaler appliance.

Parameters

h

prints this message - exclusive option

nf

Number of files to be generated in a single run of the command. Default value: 24

time

Number of seconds for which to log to trace file. Can be a mathematical expression. For example, to log to trace files for 2 hours, you can specify 2*60*60. Default value: 3600

size

Size of the packet to be logged (should be in the range of 60 to 1514 bytes). Set to 0 for full packet trace. Default value: 164 Maximum value: 1514

m

Capturing mode: sum of the values: 1 - Transmitted packets (TX) 2 - Packets buffered for transmission (TXB) 4 - Received packets (RX) Default value: 6

tcpDump

Log files in TCP dump format (instead of nstrace format). Possible values: NSTRACE, TCPDUMP

mode

Capturing mode for trace. Can be any of the following values, or a combination of these values: * RX - Received packets before NIC pipelining * NEW_RX - Received packets after NIC pipelining (packets that are not dropped) * TX - Transmitted packets * TXB - Packets buffered for transmission * IPV6 - Translated IPv6 packets * C2C - Capture core-to-core messages * NS_FR_TX - Flow receiver does not capture the TX/TXB packets. Applicable only for a cluster setup. You can also provide a combination of modes. For example: * -mode NEW_RX TXB: Capture RX packets after NIC handling and packets that are buffered for actual transmission. * -mode RX TX: Capture packet during NIC pipeline (filter expressions will not work for RX mode). * -mode NEW_RX TXB NS_FR_TX: Default mode except that TX/TXB packets on the flow receiver are not captured. Default value: DEFAULT_MODE

tcpdump

Log files format supported:nstrace-format, tcpdump-format. default:nstrace-format
Possible values: ENABLED, DISABLED Default value: DISABLED

name

Custom file name for nstrace files.

filter

Filter expression for nstrace. Maximum length of filter is 255 and it can be of the following format: "<expression> [<relop> <expression>"] where, <relop> can be the && or the || relational operators. <expression> is a string in the following format: <qualifier> <operator> <qualifier-value> where, <operator> can be any one of the following (except the commas): ==, eq, !=, neq, >, gt, <, lt, >=, ge, <=, le, BETWEEN Following are the valid qualifiers for the command: SOURCEIP, SOURCEPORT, DESTIP, DESTPORT, IP, PORT, SVCNAME, VSVRNAME, CONNID, VLAN, INTF. Example: nstrace -filter "SOURCEIP==10.102.34.201 || SVCNAME !=s1 && SOURCEPORT >80"

Example

```
nstrace -nf 10 -time 100 -mode RX IPV6 TXB -name
abc -tcpdump ENABLED -perNIC ENABLED
```

scp

scp**Synopsis**

```
scp [-r] [-C] [-q] <sourceString> <destString>
```

Description

Securely copies data from one computer to another, in SSH protocol.

Parameters

r
Recursively copy subdirectories.

C
Enable compression.

q
Quiet output. Disable the progress meter.

sourceString

Source user, host, and file path, specified as <user>@<host>:<path_to_copy_from>. The user and host parts are optional.

destString

Destination user, host, and file path, specified as <user>@<host>:<path_to_copy_to>. The user and host parts are optional.

Example

```
scp /nsconfig/ns.conf nsroot@10.102.4.107:/
nsconfig/
```

shell

shell

Synopsis

shell [(command)]

Description

Exits to the FreeBSD command prompt. Press Control + D or type exit to return to the NetScaler command prompt. Note: The shell can be accessed only by users who have write access to the NetScaler appliance.

Parameters

command
Shell command(s) to be invoked.

Example

```
> shell
# ps | grep nscli
485  p0  S      0:01.12 -nscli (nscli)
590  p0  S+     0:00.00 grep nscli
```



```
# ^D Done
> shell ps -aux |grep nscli
485  p0  S      0:01.12 -nscli (nscli)
590  p0  S+     0:00.00 grep nscli
```

install

install

Synopsis

```
install <url> [-c] [-y]
```

Description

Installs a version of NetScaler software on the system.

Parameters

url

http://[user]:[password]@host/path/to/file https://[user]:[password]@host/path/to/file sftp://[user]:[password]@host/path/to/file scp://[user]:[password]@host/path/to/file ftp://[user]:[password]@host/path/to/file file://path/to/file

c

Back up existing kernel.

y

Do not prompt for yes/no before rebooting.

Example

```
install http://host.netscaler.com/ns-6.0-41.2.tgz
```

grep

grep

Synopsis

```
grep [-c] [-E] [-i] [-v] [-w] [-x] <pattern>
```

Description

Searches files or output for lines containing a match to the specified <pattern>. By default, grep prints the matching lines.

Parameters

- c**
Suppress normal output. Instead print a count of matching lines. With the `-v` option, count non-matching lines.
- E**
Interpret `<pattern>` as an extended regular expression.
- i**
Ignore case distinctions.
- v**
Invert the sense of matching, to select non-matching lines.
- w**
Select only those lines containing matches that form whole words.
- x**
Select only those matches that exactly match the whole line.
- pattern**
The pattern (regular expression or text string) for which to search.

Example

```
show ns info | grep off -i
```

traceroute6

traceroute6

Synopsis

```
traceroute6 [-n] [I] [-r] [-v] [-m <hoplimit>] [-p <port>] [-q <probes>] [-s <src_addr>] [-T <td>] [-w <waittime>] <target> [<packetlen>]
```

Description

Invokes the UNIX `traceroute6` command. Traceroute6 attempts to track the route that the packets follow to reach the destination host.

Parameters

- n**
Print hop addresses numerically rather than symbolically and numerically.
- I**
Use ICMP ECHO for probes.
- r**
Bypass normal routing tables and send directly to a host on an attached network. If the host is not on a directly attached network, an error is returned.

- v**
Verbose output. List received ICMP packets other than TIME_EXCEEDED and UNREACHABLE.
- m**
Maximum hop value for outgoing probe packets. Default value: 64 Minimum value: 1 Maximum value: 255
- p**
Base port number used in probes. Default value: 33434 Minimum value: 1 Maximum value: 65535
- q**
Number of probes per hop. Default value: 3 Minimum value: 1 Maximum value: 65535
- s**
Source IP address to use in the outgoing query packets. If the IP address does not belong to this appliance, an error is returned and nothing is sent.
- T**
Traffic Domain Id Minimum value: 1 Maximum value: 4094
- w**
Time (in seconds) to wait for a response to a query. Default value: 5 Minimum value: 2 Maximum value: 86399
- host**
Destination host IP address or name.
- packetlen**
Length (in bytes) of the query packets. Default value: 44 Minimum value: 44 Maximum value: 32768

Example

```
traceroute6 2002::7
```

traceroute

traceroute

Synopsis

```
traceroute [-S] [-n] [-r] [-v] [-M <min_ttl>] [-m <max_ttl>] [-P <protocol>] [-p <portno>]
[-q <nqueries>] [-s <src_addr>] [-T <td>] [-t <tos>] [-w <wait>] <host> [<packetlen>]
```

Description

Invokes the UNIX traceroute command. This command attempts to track the route that the packets follow to reach the destination host.

Parameters

- S**
Print a summary of how many probes were not answered for each hop.
- n**
Print hop addresses numerically instead of symbolically and numerically.
- r**
Bypass normal routing tables and send directly to a host on an attached network. If the host is not on a directly attached network, an error is returned.
- v**
Verbose output. List received ICMP packets other than TIME_EXCEEDED and UNREACHABLE.
- M**
Minimum TTL value used in outgoing probe packets. Default value: 1 Minimum value: 1 Maximum value: 255
- m**
Maximum TTL value used in outgoing probe packets. Default value: 64 Minimum value: 1 Maximum value: 255
- P**
Send packets of specified IP protocol. The currently supported protocols are UDP and ICMP.
- p**
Base port number used in probes. Default value: 33434 Minimum value: 1 Maximum value: 65535
- q**
Number of queries per hop. Default value: 3 Minimum value: 1 Maximum value: 65535
- s**
Source IP address to use in the outgoing query packets. If the IP address does not belong to this appliance, an error is returned and nothing is sent.
- T**
Traffic Domain Id Minimum value: 1 Maximum value: 4094
- t**
Type-of-service in query packets. Maximum value: 255
- w**
Time (in seconds) to wait for a response to a query. Default value: 5 Minimum value: 2 Maximum value: 86399
- host**
Destination host IP address or name.
- packetlen**
Length (in bytes) of the query packets. Default value: 44 Minimum value: 44 Maximum value: 32768

Example

```
tracert 10.102.4.107
```

ping6

ping6

Synopsis

```
ping6 [-c <count>] [-i <interval>] [-I <interface>] [-n] [-p <pattern>] [-q] [-S sourceaddr]
[-V <vlanid>] [-T <td>] [-s <size>] Hostname
```

Description

Invokes the UNIX ping6 command. The hostName parameter must be used if the name is in the /etc/hosts file directory or is otherwise known in DNS.

Parameters

- c**
Number of packets to send. The default value is infinite. Minimum value: 1 Maximum value: 65535
- i**
Waiting time, in seconds. The default value is 1 second. Maximum value: 65535
- I**
Network interface on which to ping, if you have multiple interfaces.
- n**
Numeric output only. No name resolution.
- p**
Pattern to fill in packets. Can be up to 16 bytes, useful for diagnosing data-dependent problems.
- q**
Quiet output. Only summary is printed.
- s**
Data size, in bytes. The default value is 56. Maximum value: 65507
- V**
VLAN ID for link local address. Minimum value: 1 Maximum value: 4094
- S**
Source IP address to be used in the outgoing query packets.
- T**
Traffic Domain Id Minimum value: 1 Maximum value: 4094
- t**
Timeout in seconds before ping6 exits

hostName

Address of host to ping.

Example

```
ping6 -p ff -I 1/1 -c 4 2002::1
```

ping

ping

Synopsis

```
ping [-c <count>] [-i <interval>] [-I <interface>] [-n] [-p <pattern>] [-q] [-s <size>] [-S  
<src_addr>] [-T <td>] [-t <timeout>] <hostname>
```

Description

Invokes the UNIX ping command. The hostName parameter must be used if the name is in the /etc/hosts file directory or is otherwise known in DNS.

Parameters

- c**
Number of packets to send. The default value is infinite. Minimum value: 1 Maximum value: 65535
- i**
Waiting time, in seconds. The default value is 1 second. Maximum value: 65535
- I**
Network interface on which to ping, if you have multiple interfaces.
- n**
Numeric output only. No name resolution.
- p**
Pattern to fill in packets. Can be up to 16 bytes, useful for diagnosing data-dependent problems.
- q**
Quiet output. Only the summary is printed.
- s**
Data size, in bytes. The default value is 56. Maximum value: 65507
- S**
Source IP address to be used in the outgoing query packets. If the IP address does not belong to this appliance, an error is returned and nothing is sent.
- T**
Traffic Domain Id Minimum value: 1 Maximum value: 4094

t

Time-out, in seconds, before ping exits. Minimum value: 1 Maximum value: 3600

hostName

Address of host to ping.

Example

```
ping -p ff -c 4 10.102.4.107
```

techsupport

show techsupport

Synopsis

```
show techsupport [-scope ( NODE | CLUSTER )]
```

Description

Generates a tar of system configuration data and statistics. This file must be submitted to Citrix technical support with file name collector_<NS IP>_<P/S>_<DateTime>.tgz. The archive is always pointed by the symbolic link /var/tmp/support/support.tgz for each invocation of the command.

Parameters**scope**

Use this option to run showtechsupport on present node or all cluster nodes. Possible values: NODE, CLUSTER Default value: NS_TECH_NODE

Example

```
show techsupport
```

callhome

[[show](#) | [set](#) | [unset](#)]

show callhome

Synopsis

```
show callhome
```

Description

Displays the trigger events configured and the time when these events were triggered.

Example

```
show callhome
  E-mail address configured:xxx@yahoo.com

Trigger event          State      First
occurrence            Latest occurrence
-----
1) Compact flash errors
Enabled ..
2) Hard disk drive errors
Enabled ..
3) Power supply unit failure Enabled 27 Aug 2010
18:22:47      28 Aug 2010 18:22:47
4) SSL card failure    Enabled 25 Aug 2010
18:22:47      26 Aug 2010 18:22:47
5) Warm restart        Enabled  N/
A ..
```

[Top](#)**set callhome****Synopsis**

```
set callhome -emailAddress e-mailaddress
```

Description

Sets the contact person's E-mail address

Parameters**emailAddress**

The contact person's E-mail address.

proxyMode

Deploy the callhome proxy mode Possible values: YES, NO Default value: NO

Example

```
set callhome -emailAddress xxxx@yahoo.com
```

[Top](#)**unset callhome****Synopsis**

```
unset callhome [-emailAddress] [-proxyMode] [-IPAddress] [-port]
```


Description

Use this command to remove callhome settings. Refer to the set callhome command for meanings of the arguments.

[Top](#)

VPN Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [vpn](#)
- ♦ [vpn vserver](#)
- ♦ [vpn intranetApplication](#)
- ♦ [vpn nextHopServer](#)
- ♦ [vpn trafficPolicy](#)
- ♦ [vpn trafficAction](#)
- ♦ [vpn formSSOAction](#)
- ♦ [vpn samlSSOProfile](#)
- ♦ [vpn url](#)
- ♦ [vpn sessionPolicy](#)
- ♦ [vpn sessionAction](#)
- ♦ [vpn clientlessAccessPolicy](#)
- ♦ [vpn clientlessAccessProfile](#)
- ♦ [vpn stats](#)
- ♦ [vpn icaConnection](#)
- ♦ [vpn global](#)
- ♦ [vpn parameter](#)

vpn

stat vpn

Synopsis

```
stat vpn [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>]  
[-clearstats ( basic | full )]
```

Description

Displays the statistics for Access Gateway usage. Displays event information, such as the event that generated the message, a time stamp, the message type, and predefined log levels and message information.

Parameters

clearstats

Clear the statistics / counters Possible values: basic, full

vpn vserver

[[add](#) | [rm](#) | [set](#) | [unset](#) | [bind](#) | [unbind](#) | [enable](#) | [disable](#) | [show](#) | [stat](#) | [rename](#)]

add vpn vserver

Synopsis

```
add vpn vserver <name> <serviceType> (<IPAddress> [-range <positive_integer>]) <port>
[-state ( ENABLED | DISABLED )] [-authentication ( ON | OFF )] [-doubleHop ( ENABLED
| DISABLED )] [-maxAAUsers <positive_integer>] [-icaOnly ( ON | OFF )] [-
downStateFlush ( ENABLED | DISABLED )] [-Listenpolicy <expression> [-Listenpriority
<positive_integer>]] [-tcpProfileName <string>] [-httpProfileName <string>] [-comment
<string>] [-appflowLog ( ENABLED | DISABLED )] [-icmpVsrResponse ( PASSIVE |
ACTIVE )] [-netProfile <string>] [-cginfraHomePageRedirect ( ENABLED | DISABLED )] [-
maxLoginAttempts <positive_integer>] [-failedLoginTimeout <positive_integer>]]
```

Description

Creates an Access Gateway virtual server to allow authenticated users to access intranet resources, such as XenApp, XenDesktop, and web servers.

Parameters

name

Name for the Access Gateway virtual server. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the virtual server is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my server" or 'my server').

serviceType

Protocol used by the Access Gateway virtual server. Possible values: SSL Default value: NSSVC_SSL

IPAddress

IPv4 or IPv6 address of the Access Gateway virtual server. Usually a public IP address. User devices send connection requests to this IP address.

port

TCP port on which the virtual server listens. Minimum value: 1

state

State of the virtual server. If the virtual server is disabled, requests are not processed. Possible values: ENABLED, DISABLED Default value: ENABLED

authentication

Require authentication for users connecting to Access Gateway. Possible values: ON, OFF Default value: ON

doubleHop

Use the Access Gateway appliance in a double-hop configuration. A double-hop deployment provides an extra layer of security for the internal network by using three firewalls to divide the demilitarized zone (DMZ) into two stages. Such a deployment can have one appliance in the DMZ and one appliance in the secure network. Possible values: ENABLED, DISABLED Default value: DISABLED

maxAAUsers

Maximum number of concurrent user sessions allowed on this virtual server. The actual number of users allowed to log on to this virtual server depends on the total number of user licenses.

icaOnly

User can log on in basic mode only, through either Citrix Receiver or a browser. Users are not allowed to connect by using the Access Gateway Plug-in. Possible values: ON, OFF Default value: OFF

downStateFlush

Close existing connections when the virtual server is marked DOWN, which means the server might have timed out. Disconnecting existing connections frees resources and in certain cases speeds recovery of overloaded load balancing setups. Enable this setting on servers whose connections can safely be closed when they are marked DOWN. Do not enable DOWN state flush on servers that must complete their transactions. Possible values: ENABLED, DISABLED Default value: ENABLED

Listenpolicy

String specifying the listen policy for the Access Gateway virtual server. Can be either a named expression or a default syntax expression. The Access Gateway virtual server processes only the traffic for which the expression evaluates to true. Default value: "none"

Listenpriority

Integer specifying the priority of the listen policy. A higher number specifies a lower priority. If a request matches the listen policies of more than one virtual server, the virtual server whose listen policy has the highest priority (the lowest priority number) accepts the request. Default value: 101 Maximum value: 100

tcpProfileName

Name of the TCP profile to assign to this virtual server.

httpProfileName

Name of the HTTP profile to assign to this virtual server.

comment

Any comments associated with the virtual server.

appflowLog

Log AppFlow records that contain standard NetFlow or IPFIX information, such as time stamps for the beginning and end of a flow, packet count, and byte count. Also log records that contain application-level information, such as HTTP web addresses, HTTP request methods and response status codes, server response time, and latency. Possible values: ENABLED, DISABLED Default value: DISABLED

icmpVsrResponse

Criterion for responding to PING requests sent to this virtual server. If this parameter is set to ACTIVE, respond only if the virtual server is available. With the PASSIVE setting, respond even if the virtual server is not available. Possible values: PASSIVE, ACTIVE Default value: NS_VSR_PASSIVE

netProfile

The name of the network profile.

cginfraHomePageRedirect

When client requests for Sharefile resource and AGEE finds that the user is unauthenticated or the user-session has expired then, disabling this option will take the user to the originally requested Sharefile resource after authentication (instead of taking the user to the default vpn homepage) Possible values: ENABLED, DISABLED Default value: ENABLED

maxLoginAttempts

Maximum Number of login Attempts Minimum value: 1 Maximum value: 255

Example

```
The following example creates a VPN vserver named  
myvpnvip which supports SSL portocol and with AAA  
functionality enabled:  
vserver myvpnvip SSL 65.219.17.34 443 -aaa ON
```

[Top](#)

rm vpn vserver**Synopsis**

```
rm vpn vserver <name>@ ...
```

Description

Removes an Access Gateway virtual server. Policies that are bound to the virtual server are automatically unbound.

Parameters**name**

Name of the virtual server to remove.

Example

```
rm vserver vpn_vip
```

[Top](#)

set vpn vsrver

Synopsis

```
set vpn vsrver <name> [-IPAddress <ip_addr|ipv6_addr|*>] [-authentication ( ON |
OFF )] [-doubleHop ( ENABLED | DISABLED )] [-icaOnly ( ON | OFF )] [-maxAAAUsers
<positive_integer>] [-downStateFlush ( ENABLED | DISABLED )] [-Listenpolicy
<expression>] [-Listenpriority <positive_integer>] [-tcpProfileName <string>] [-
httpProfileName <string>] [-comment <string>] [-appflowLog ( ENABLED | DISABLED )] [-
icmpVsrResponse ( PASSIVE | ACTIVE )] [-netProfile <string>] [-cginfraHomePageRedirect
( ENABLED | DISABLED )] [-maxLoginAttempts <positive_integer>] [-failedLoginTimeout
<positive_integer>]
```

Description

Modifies the specified parameters of an Access Gateway virtual server.

Parameters

name

Name of the virtual server to modify.

IPAddress

IPv4 or IPv6 address of the Access Gateway virtual server. Usually a public IP address. User devices send connection requests to this IP address.

authentication

Require authentication for users connecting to Access Gateway. Possible values: ON, OFF Default value: ON

doubleHop

Use the Access Gateway appliance in a double-hop configuration. A double-hop deployment provides an extra layer of security for the internal network by using three firewalls to divide the demilitarized zone (DMZ) into two stages. Such a deployment can have one appliance in the DMZ and one appliance in the secure network. Possible values: ENABLED, DISABLED Default value: DISABLED

icaOnly

User can log on in basic mode only, through either Citrix Receiver or a browser. Users are not allowed to connect by using the Access Gateway Plug-in. Possible values: ON, OFF Default value: OFF

maxAAAUsers

Maximum number of concurrent user sessions allowed on this virtual server. The actual number of users allowed to log on to this virtual server depends on the total number of user licenses.

downStateFlush

Close existing connections when the virtual server is marked DOWN, which means the server might have timed out. Disconnecting existing connections frees resources and in certain cases speeds recovery of overloaded load balancing setups. Enable this setting on servers whose connections can safely be closed when they are marked DOWN. Do not enable DOWN state flush on servers that must complete their transactions. Possible values: ENABLED, DISABLED Default value: ENABLED

Listenpolicy

String specifying the listen policy for the Access Gateway virtual server. Can be either a named expression or a default syntax expression. The Access Gateway virtual server processes only the traffic for which the expression evaluates to true. Default value: "none"

Listenpriority

Integer specifying the priority of the listen policy. A higher number specifies a lower priority. If a request matches the listen policies of more than one virtual server, the virtual server whose listen policy has the highest priority (the lowest priority number) accepts the request. Default value: 101 Maximum value: 100

tcpProfileName

Name of the TCP profile to assign to this virtual server.

httpProfileName

Name of the HTTP profile to assign to this virtual server.

comment

Any comments associated with the virtual server.

appflowLog

Log AppFlow records that contain standard NetFlow or IPFIX information, such as time stamps for the beginning and end of a flow, packet count, and byte count. Also log records that contain application-level information, such as HTTP web addresses, HTTP request methods and response status codes, server response time, and latency. Possible values: ENABLED, DISABLED Default value: DISABLED

icmpVsrResponse

Criterion for responding to PING requests sent to this virtual server. If this parameter is set to ACTIVE, respond only if the virtual server is available. With the PASSIVE setting, respond even if the virtual server is not available. Possible values: PASSIVE, ACTIVE Default value: NS_VSR_PASSIVE

netProfile

The name of the network profile.

cginfraHomePageRedirect

When client requests for Sharefile resource and AGEE finds that the user is unauthenticated or the user-session has expired then, disabling this option will take the user to the originally requested Sharefile resource after authentication (instead of taking the user to the default vpn homepage) Possible values: ENABLED, DISABLED Default value: ENABLED

maxLoginAttempts

Maximum Number of login Attempts Minimum value: 1 Maximum value: 255

failedLoginTimeout

Failed Login timeout Minimum value: 1

[Top](#)

unset vpn vserver

Synopsis

unset vpn vserver <name> [-authentication] [-doubleHop] [-icaOnly] [-maxAAAUUsers] [-downStateFlush] [-Listenpolicy] [-Listenpriority] [-tcpProfileName] [-httpProfileName] [-comment] [-appflowLog] [-icmpVsrResponse] [-netProfile] [-cginfraHomePageRedirect] [-maxLoginAttempts]

Description

Use this command to remove vpn vserver settings. Refer to the set vpn vserver command for meanings of the arguments.

[Top](#)

bind vpn vserver

Synopsis

bind vpn vserver <name> [-policy <string> [-priority <positive_integer>] [-secondary] [-groupExtraction] [-gotoPriorityExpression <expression>] [-type <type>]] [-intranetApplication <string>] [-nextHopServer <string>] [-urlName <string>] [-intranetIP <ip_addr> <netmask>] [-staServer <URL>] [-appController <URL>] [-sharefile <string>]

Description

Binds attributes to the specified Access Gateway virtual server.

Parameters

name

Name of the virtual server.

policy

Name of a policy to bind to the virtual server (for example, the name of an authentication, session, or endpoint analysis policy).

intranetApplication

Name of the application to bind to the virtual server. Intranet applications are used to enable access to selected applications located in the internal network. They are required for any user connecting with the Access Gateway Plug-in for Java.

nextHopServer

Name of the next hop server to bind to the virtual server.

urlName

Web address of the next hop virtual server to bind to the virtual server.

intranetIP

The network id for the range of intranet IP addresses or individual intranet ip to be bound to the vserver.

staServer

Web address of the Secure Ticket Authority (STA) server, in the following format:
'http(s)://FQDN/URLPATH'

appController

AppController server, in the format 'http(s)://IP/FQDN'

sharefile

Sharefile server, in the format 'IP:PORT / FQDN:PORT'

[Top](#)

unbind vpn vserver

Synopsis

unbind vpn vserver <name> [-policy <string> [-secondary] [-groupExtraction] [-type <type>]] [-intranetApplication <string>] [-nextHopServer <string>] [-urlName <string>] [-intranetIP <ip_addr> <netmask>] [-staServer <URL>] [-appController <URL>] [-sharefile <string>]

Description

Unbinds the specified attributes from a virtual server.

Parameters

name

Name of the virtual server from which to unbind an attribute.

policy

Name of the policy to unbind from the virtual server.

intranetApplication

Name of intranet application to unbind from the virtual server.

nextHopServer

Name of the next hop server to remove.

urlName

Web address of the next hop virtual server to unbind.

intranetIP

The range of IP addresses to unbind from the virtual server.

staServer

Web address of the Secure Ticket Authority (STA) server to remove, in the following format: 'http(s)://FQDN/URLPATH'

appController

AppController server to be removed, in the format 'http(s)://IP/FQDN'

sharefile

Sharefile server to be removed, in the format 'IP:PORT / FQDN:PORT'

[Top](#)

enable vpn vserver

Synopsis

enable vpn vserver <name>@

Description

Enables an Access Gateway virtual server. Note: Virtual servers, when added, are enabled by default.

Parameters

name

Name of the virtual server to be enabled.

Example

```
enable vserver vpn1
```

[Top](#)

disable vpn vserver

Synopsis

disable vpn vserver <name>@

Description

Disables an Access Gateway virtual server. The virtual server is taken out of service.

Parameters

name

Name of the virtual server to be disabled. The Access Gateway still responds to ARP and/or ping requests for the IP address of the virtual server. You can enable the Access Gateway virtual server again at any time, because the virtual server is still configured.

Example

```
disable vserver lb_vip
```

[Top](#)

show vpn vserver

Synopsis

show vpn vserver [<name>] show vpn vserver stats - alias for 'stat vpn vserver'

Description

Displays information about all the configured Access Gateway virtual servers, or displays detailed information about the specified Access Gateway virtual server.

Parameters

name

Name of the Access Gateway virtual server for which to show detailed information.

Example

```
show vpn vserver
```

[Top](#)

stat vpn vserver

Synopsis

```
stat vpn vserver [<name>] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile  
<input_filename>] [-clearstats ( basic | full )]
```

Description

Displays statistics for all Access Gateway virtual servers, or displays detailed statistics for the specified Access Gateway virtual server.

Parameters

name

Name of the virtual server for which to show detailed statistics.

clearstats

Clear the statistics / counters Possible values: basic, full

[Top](#)

rename vpn vserver

Synopsis

```
rename vpn vserver <name>@ <newName>@
```

Description

Renames an Access Gateway virtual server.

Parameters

name

Name of the Access Gateway virtual server.

newName

New name for the Access Gateway virtual server. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my server" or 'my server').

Example

```
rename vpn vserver vpn1 vpn1new
```

[Top](#)

vpn intranetApplication

[[add](#) | [rm](#) | [show](#)]

add vpn intranetApplication

Synopsis

```
add vpn intranetApplication <intranetApplication> [<protocol>] ((<destIP> [-netmask
<netmask>]) | <IPRange> | <hostName> | (-clientApplication <string> ... [-spoofIIP ( ON
| OFF )])) [-destPort <port[-port]>] [-interception ( PROXY | TRANSPARENT ) [-srcIP
<ip_addr>] [-srcPort <port>]]
```

Description

Defines intranet applications to be made accessible through the Access Gateway.

Parameters

intranetApplication

Name of the intranet application.

protocol

Protocol used by the intranet application. If protocol is set to BOTH, TCP and UDP traffic is allowed. Possible values: TCP, UDP, ANY

destIP

Destination IP address, IP range, or host name of the intranet application. This address is the server IP address.

clientApplication

Names of the client applications, such as PuTTY and Xshell.

destPort

Destination TCP or UDP port number for the intranet application. Use a hyphen to specify a range of port numbers, for example 90-95. Minimum value: 1

interception

Interception mode for the intranet application or resource. Correct value depends on the type of client software used to make connections. If the interception mode is set to TRANSPARENT, users connect with the Access Gateway Plug-in for Windows. With the PROXY setting, users connect with the Access Gateway Plug-in for Java. Possible values: PROXY, TRANSPARENT

srcIP

Source IP address. Required if interception mode is set to PROXY. Default is the loopback address, 127.0.0.1.

srcPort

Source port for the application for which the Access Gateway virtual server proxies the traffic. If users are connecting from a device that uses the Access Gateway Plug-in for Java, applications must be configured manually by using the source IP address and TCP port values specified in the intranet application profile. If a port value is not set, the destination port value is used. Minimum value: 1

[Top](#)

rm vpn intranetApplication

Synopsis

rm vpn intranetApplication <intranetApplication>

Description

Removes a configured intranet resource.

Parameters

intranetApplication

Name of the intranet resource to remove.

[Top](#)

show vpn intranetApplication

Synopsis

show vpn intranetApplication [<intranetApplication>]

Description

Displays information about all the configured intranet resources, or displays detailed information about the specified intranet resource.

Parameters

intranetApplication

Name of the intranet resource for which to display detailed information.

[Top](#)

vpn nextHopServer

[[add](#) | [rm](#) | [show](#)]

add vpn nextHopServer

Synopsis

add vpn nextHopServer <name> <nextHopIP> <nextHopPort> [-secure (ON | OFF)]

Description

Enables an Access Gateway appliance in the first DMZ to communicate with one or more Access Gateway appliances in the second DMZ.

Parameters

name

Name for the Access Gateway appliance in the first DMZ. Maximum value: 32

nextHopIP

IP address or FQDN of the Access Gateway proxy in the second DMZ.

nextHopPort

Port number of the Access Gateway proxy in the second DMZ.

secure

Use of a secure port, such as 443, for the double-hop configuration. Possible values: ON, OFF Default value: OFF

Example

```
add vpn nexthopserver dh1 10.1.1.1 80 -secure OFF
```

[Top](#)

rm vpn nextHopServer

Synopsis

```
rm vpn nextHopServer <name>
```

Description

Removes a configured next hop server.

Parameters

name

Name of the next hop server to remove. Maximum value: 32

Example

```
rm vpn nexthopserver dh1
```

[Top](#)

show vpn nextHopServer

Synopsis

```
show vpn nextHopServer [<name>]
```

Description

Displays information about all the configured next Access Gateway hop servers, or detailed information about the specified Access Gateway next hop server.

Parameters

name

Name of the Access Gateway next hop server for which to display detailed information. Maximum value: 32

Example

```
show vpn nexthopserver dh1
```

[Top](#)

vpn trafficPolicy

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add vpn trafficPolicy

Synopsis

add vpn trafficPolicy <name> <rule> <action>

Description

Creates a traffic policy. A traffic policy conditionally sets Access Gateway traffic characteristics at run time. For an intranet resource, for example, the traffic policy parameters define the destination IP address, destination port, amount of time a user can stay logged on to the application, and HTTP compression.

Parameters

name

Name for the traffic policy. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the policy is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy').

rule

Expression, or name of a named expression, against which traffic is evaluated. Written in the classic or default syntax. Note: Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>". The following requirements apply only to the NetScaler CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action

Action to apply to traffic that matches the policy.

[Top](#)

rm vpn trafficPolicy**Synopsis**

rm vpn trafficPolicy <name>

Description

Removes an existing traffic policy from Access Gateway.

Parameters**name**

Name of the traffic policy to remove.

[Top](#)

set vpn trafficPolicy**Synopsis**

set vpn trafficPolicy <name> [-rule <expression>] [-action <string>]

Description

Modifies the specified parameters of an existing traffic policy.

Parameters**name**

Name of the traffic policy to modify.

rule

Expression, or name of a named expression, against which traffic is evaluated. Written in the classic or default syntax. Note: Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>". The following requirements apply only to the NetScaler CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action

Action to apply to traffic that matches the policy.

[Top](#)

unset vpn trafficPolicy

Synopsis

unset vpn trafficPolicy <name> [-rule] [-action]

Description

Use this command to remove vpn trafficPolicy settings. Refer to the set vpn trafficPolicy command for meanings of the arguments.

[Top](#)

show vpn trafficPolicy

Synopsis

show vpn trafficPolicy [<name>]

Description

Displays information about all Access Gateway traffic policies, or detailed information about the specified policy.

Parameters

name

Name of the traffic policy for which to display detailed information.

[Top](#)

vpn trafficAction

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add vpn trafficAction

Synopsis

add vpn trafficAction <name> <qual> [-appTimeout <mins>] [(-SSO (ON | OFF) [-formSSOAction <string>]) | -wanscaler (ON | OFF)] [-fta (ON | OFF)] [-kcdAccount <string>] [-samlSSOProfile <string>]

Description

Creates an action to be applied by a policy that matches the traffic being processed.

Parameters

name

Name for the traffic action. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after a traffic action is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

qual

Protocol, either HTTP or TCP, to be used with the action. If you specify TCP, single sign-on cannot be configured. Possible values: http, tcp

appTimeout

Maximum amount of time, in minutes, a user can stay logged on to the web application. Minimum value: 1 Maximum value: 715827

SSO

Provide single sign-on to the web application. Possible values: ON, OFF

formSSOAction

Name of the form-based single sign-on profile. Form-based single sign-on allows users to log on one time to all protected applications in your network, instead of requiring them to log on separately to access each one.

fta

Specify file type association, which is a list of file extensions that users are allowed to open. Possible values: ON, OFF

wanscaler

Use the Repeater Plug-in to optimize network traffic. Possible values: ON, OFF

kcdAccount

Kerberos constrained delegation account name

samlSSOProfile

Profile to be used for doing SAML SSO to remote relying party

[Top](#)

rm vpn trafficAction

Synopsis

```
rm vpn trafficAction <name>
```

Description

Removes a previously created traffic policy action.

Parameters

name

Name of the traffic policy action to remove.

[Top](#)

set vpn trafficAction

Synopsis

```
set vpn trafficAction <name> [-appTimeout <mins>] [-SSO ( ON | OFF ) | -wanscaler  
( ON | OFF )] [-formSSOAction <string>] [-fta ( ON | OFF )] [-kcdAccount <string>] [-  
samlSSOProfile <string>]
```

Description

Modifies a traffic policy action to be applied by the policy if the rule criteria are met.

Parameters

name

Name of the traffic policy action to modify.

appTimeout

Maximum amount of time, in minutes, a user can stay logged on to the web application. Minimum value: 1 Maximum value: 715827

SSO

Provide single sign-on to the web application. Possible values: ON, OFF

formSSOAction

Name of the form-based single sign-on profile. Form-based single sign-on allows users to log on one time to all protected applications in your network, instead of requiring them to log on separately to access each one.

fta

Specify file type association, which is a list of file extensions that users are allowed to open. Possible values: ON, OFF

wanscaler

Use the Repeater Plug-in to optimize network traffic. Possible values: ON, OFF

kcdAccount

Kerberos constrained delegation account name

samlSSOProfile

Profile to be used for doing SAML SSO to remote relying party

[Top](#)

unset vpn trafficAction

Synopsis

```
unset vpn trafficAction <name> [-wanscaler] [-kcdAccount]
```

Description

Use this command to remove vpn trafficAction settings. Refer to the set vpn trafficAction command for meanings of the arguments.

[Top](#)

show vpn trafficAction

Synopsis

```
show vpn trafficAction [<name>]
```

Description

Displays information about all the configured traffic actions, or displays detailed information about the specified traffic action.

Parameters

name

Name of the traffic policy action for which to display detailed information.

[Top](#)

vpn formSSOAction

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add vpn formSSOAction

Synopsis

```
add vpn formSSOAction <name> -actionURL <URL> -userField <string> -passwdField
<string> -ssoSuccessRule <expression> [-nameValuePair <string>] [-responsesize
<positive_integer>] [-nvtype ( STATIC | DYNAMIC )] [-submitMethod ( GET | POST )]
```

Description

Creates a form-based single sign-on profile. Form based single sign-on allows users to log on one time to all protected applications in your network. Users can access web applications that require an HTML form-based logon without having to type their password again.

Parameters

name

Name for the form based single sign-on profile.

actionURL

Root-relative URL to which the completed form is submitted.

userField

Name of the form field in which the user types in the user ID.

passwdField

Name of the form field in which the user types in the password.

ssoSuccessRule

Use a frequently used expression or create a custom expression describing the action that the form-based single sign-on profile takes when invoked by a policy. Used for verifying successful single sign-on.

nameValuePair

Other name-value pair attributes to send to the server, in addition to sending the user name and password. Value names are separated by an ampersand (&), such as in name1=value1&name2=value2.

responsesize

Maximum number of bytes to allow in the response size. Specifies the number of bytes in the response to be parsed for extracting the forms. Default value: 8096

nvtype

How to process the name-value pair. Available settings function as follows: * STATIC - The administrator-configured values are used. * DYNAMIC - The response is parsed,

the form is extracted, and then submitted. Possible values: STATIC, DYNAMIC Default value: NS_ACT_FSSO_NV_DYNAMIC

submitMethod

HTTP method (GET or POST) used by the single sign-on form to send the logon credentials to the logon server. Possible values: GET, POST Default value: NS_ACT_FSSO_SUBMIT_GET

[Top](#)

rm vpn formSSOAction

Synopsis

rm vpn formSSOAction <name>

Description

Removes a configured form-based single sign-on profile.

Parameters

name

Name of the form-based single sign-on profile to remove.

[Top](#)

set vpn formSSOAction

Synopsis

set vpn formSSOAction <name> [-actionURL <URL>] [-userField <string>] [-passwdField <string>] [-ssoSuccessRule <expression>] [-responsesize <positive_integer>] [-nameValuePair <string>] [-nvtype (STATIC | DYNAMIC)] [-submitMethod (GET | POST)]

Description

Modifies the parameters of an existing form-based single sign-on profile (or action).

Parameters

name

Name for the form based single sign-on profile.

actionURL

Root-relative URL to which the completed form is submitted.

userField

Name of the form field in which the user types in the user ID.

passwdField

Name of the form field in which the user types in the password.

ssoSuccessRule

Use a frequently used expression or create a custom expression describing the action that the form-based single sign-on profile takes when invoked by a policy. Used for verifying successful single sign-on.

responsesize

Maximum number of bytes to allow in the response size. Specifies the number of bytes in the response to be parsed for extracting the forms. Default value: 8096

nameValuePair

Other name-value pair attributes to send to the server, in addition to sending the user name and password. Value names are separated by an ampersand (&), such as in name1=value1&name2=value2.

nvtype

How to process the name-value pair. Available settings function as follows: * STATIC - The administrator-configured values are used. * DYNAMIC - The response is parsed, the form is extracted, and then submitted. Possible values: STATIC, DYNAMIC Default value: NS_ACT_FSSO_NV_DYNAMIC

submitMethod

HTTP method (GET or POST) used by the single sign-on form to send the logon credentials to the logon server. Possible values: GET, POST Default value: NS_ACT_FSSO_SUBMIT_GET

[Top](#)

unset vpn formSSOAction

Synopsis

```
unset vpn formSSOAction <name> [-responsesize] [-nameValuePair] [-nvtype] [-submitMethod]
```

Description

Use this command to remove vpn formSSOAction settings. Refer to the set vpn formSSOAction command for meanings of the arguments.

[Top](#)

show vpn formSSOAction

Synopsis

```
show vpn formSSOAction [<name>]
```

Description

Displays the attributes of a form-based single sign-on profile.

Parameters**name**

Name of the form-based single sign-on profile.

[Top](#)

vpn samlSSOProfile

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add vpn samlSSOProfile

Synopsis

```
add vpn samlSSOProfile <name> -samlSigningCertName <string> -  
assertionConsumerServiceURL <URL> -relaystateRule <expression> [-sendPassword ( ON  
| OFF )] [-samlIssuerName <string>]
```

Description

Creates a SAML single sign-on profile. This profile is employed in triggering saml assertion to a target service based on traffic profile.

Parameters

name

Name for the new saml single sign-on profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an SSO action is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

samlSigningCertName

Name of the signing authority as given in the SAML server's SSL certificate.

assertionConsumerServiceURL

URL to which the assertion is to be sent.

relaystateRule

Expression to extract relaystate to be sent along with assertion.

sendPassword

Option to send password in assertion. Possible values: ON, OFF Default value: OFF

samlIssuerName

The name to be used in requests sent from Netscaler to IdP to uniquely identify Netscaler.

[Top](#)

rm vpn samlSSOProfile

Synopsis

```
rm vpn samlSSOProfile <name>
```

Description

Deletes an existing saml single sign-on traffic profile.

Parameters

name

Name for the new saml single sign-on profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an SSO action is created. The following requirement applies

only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

[Top](#)

set vpn samlSSOProfile

Synopsis

```
set vpn samlSSOProfile <name> [-samlSigningCertName <string>] [-
assertionConsumerServiceURL <URL>] [-sendPassword ( ON | OFF )] [-samlIssuerName
<string>] [-relaystateRule <expression>]
```

Description

Modifies the specified attributes of a saml single sign-on traffic profile.

Parameters

name

Name for the new saml single sign-on profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an SSO action is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

samlSigningCertName

Name of the signing authority as given in the SAML server's SSL certificate.

assertionConsumerServiceURL

URL to which the assertion is to be sent.

sendPassword

Option to send password in assertion. Possible values: ON, OFF Default value: OFF

samlIssuerName

The name to be used in requests sent from Netscaler to IdP to uniquely identify Netscaler.

relaystateRule

Expression to extract relaystate to be sent along with assertion.

[Top](#)

unset vpn samlSSOProfile

Synopsis

```
unset vpn samlSSOProfile <name> [-samlSigningCertName] [-sendPassword] [-
samlIssuerName]
```

Description

Use this command to remove vpn samlSSOProfile settings. Refer to the set vpn samlSSOProfile command for meanings of the arguments.

[Top](#)

show vpn samlSSOProfile

Synopsis

show vpn samlSSOProfile [<name>]

Description

Displays information about all configured saml single sign-on profiles, or displays detailed information about the specified action.

Parameters

name

Name for the new saml single sign-on profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an SSO action is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

[Top](#)

vpn url

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add vpn url

Synopsis

add vpn url <urlName> <linkName> <actualURL> [-clientlessAccess (ON | OFF)] [-comment <string>]

Description

Creates a bookmark link to an external or internal resource that appears on the Access Interface, according to type, as a web site link or file share link.

Parameters

urlName

Name of the bookmark link.

linkName

Description of the bookmark link. The description appears in the Access Interface.

actualURL

Web address for the bookmark link.

clientlessAccess

If clientless access to the resource hosting the link is allowed, also use clientless access for the bookmarked web address in the Secure Client Access based session. Allows single sign-on and other HTTP processing on Access Gateway for HTTPS resources. Possible values: ON, OFF Default value: OFF

comment

Any comments associated with the bookmark link.

Example

```
add vpn url ggl search www.google.com.
```

[Top](#)

rm vpn url**Synopsis**

```
rm vpn url <urlName>
```

Description

Removes a bookmark link to an internal resource that appears in the Access Interface.

Parameters**urlName**

Name of the bookmark link to remove.

Example

```
rm vpn url ggl
```

[Top](#)

set vpn url**Synopsis**

```
set vpn url <urlName> [-linkName <string>] [-actualURL <string>] [-clientlessAccess  
( ON | OFF )] [-comment <string>]
```

Description

Modifies the specified parameters of a bookmark link to an internal resource that appears in the Access Interface.

Parameters**urlName**

Name of the bookmark link.

linkName

Description of the bookmark link. The description appears in the Access Interface.

actualURL

Web address for the bookmark link.

clientlessAccess

If clientless access to the resource hosting the link is allowed, also use clientless access for the bookmarked web address in the Secure Client Access based session. Allows single sign-on and other HTTP processing on Access Gateway for HTTPS resources. Possible values: ON, OFF Default value: OFF

comment

Any comments associated with the bookmark link.

Example

```
set vpn url wiurl -clientlessAccess on
```

[Top](#)

unset vpn url**Synopsis**

```
unset vpn url <urlName> [-clientlessAccess] [-comment]
```

Description

Use this command to remove vpn url settings. Refer to the set vpn url command for meanings of the arguments.

[Top](#)

show vpn url**Synopsis**

```
show vpn url [<urlName>]
```

Description

Displays information about all the configured bookmark links to internal resources that appear in the Access Interface, or displays detailed information about the specified bookmark link.

Parameters**urlName**

Name of the bookmark link for which to display detailed information.

[Top](#)

vpn sessionPolicy

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add vpn sessionPolicy

Synopsis

add vpn sessionPolicy <name> <rule> <action>

Description

Creates a new session policy that, if bound, is applied after the user logs on to Access Gateway, and that determines the properties of the user session.

Parameters

name

Name for the new session policy that is applied after the user logs on to Access Gateway.

rule

Expression, or name of a named expression, specifying the traffic that matches the policy. Can be written in either default or classic syntax. Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>". The following requirements apply only to the NetScaler CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action

Action to be applied by the new session policy if the rule criteria are met.

[Top](#)

rm vpn sessionPolicy

Synopsis

rm vpn sessionPolicy <name>

Description

Removes the session policy that is applied after the user logs on to Access Gateway.

Parameters

name

Name of the session policy to remove.

[Top](#)

set vpn sessionPolicy

Synopsis

set vpn sessionPolicy <name> [-rule <expression>] [-action <string>]

Description

Modifies the rule or action of a session policy.

Parameters

name

Name of the session policy to modify.

rule

Expression, or name of a named expression, specifying the traffic that matches the policy. Can be written in either default or classic syntax. Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>". The following requirements apply only to the NetScaler CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action

Action to be applied by the new session policy if the rule criteria are met.

[Top](#)

unset vpn sessionPolicy

Synopsis

```
unset vpn sessionPolicy <name> [-rule] [-action]
```

Description

Use this command to remove vpn sessionPolicy settings. Refer to the set vpn sessionPolicy command for meanings of the arguments.

[Top](#)

show vpn sessionPolicy

Synopsis

```
show vpn sessionPolicy [<name>]
```

Description

Displays a session policy.

Parameters

name

Name of the session policy to display.

[Top](#)

vpn sessionAction

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add vpn sessionAction

Synopsis

```
add vpn sessionAction <name> [-httpPort <port> ...] [-winsIP <ip_addr>] [-
dnsVserverName <string>] [-splitDns <splitDns>] [-sessTimeout <mins>] [-clientSecurity
<expression>] [-clientSecurityGroup <string>] [-clientSecurityMessage <string>]] [-
clientSecurityLog ( ON | OFF )] [-splitTunnel <splitTunnel>] [-localLanAccess ( ON |
OFF )] [-rfc1918 ( ON | OFF )] [-spoofIP ( ON | OFF )] [-killConnections ( ON | OFF )] [-
transparentInterception ( ON | OFF )] [-defaultAuthorizationAction ( ALLOW | DENY )]
[-authorizationGroup <string>] [-clientIdleTimeout <mins>] [-proxy <proxy>] [-
allProtocolProxy <string> | -httpProxy <string> | -ftpProxy <string> | -socksProxy
<string> | -gopherProxy <string> | -sslProxy <string>] [-proxyException <string>] [-
proxyLocalBypass ( ENABLED | DISABLED )] [-clientCleanupPrompt ( ON | OFF )] [-
forceCleanup <forceCleanup> ...] [-clientOptions <clientOptions> ...] [-
clientConfiguration <clientConfiguration> ...] [-SSO ( ON | OFF )] [-ssoCredential
( PRIMARY | SECONDARY )] [-windowsAutoLogon ( ON | OFF )] [-useMIP ( NS | OFF )] [-
useIIP <useIIP>] [-clientDebug <clientDebug>] [-loginScript <input_filename>] [-
logoutScript <input_filename>] [-homePage <URL>] [-icaProxy ( ON | OFF )] [-wihome
<URL>] [-citrixReceiverHome <URL>] [-wiPortalMode ( NORMAL | COMPACT )] [-
ClientChoices ( ON | OFF )] [-iipDnsSuffix <string>] [-forcedTimeout <mins>] [-
forcedTimeoutWarning <mins>] [-ntDomain <string>] [-clientlessVpnMode
<clientlessVpnMode>] [-emailHome <URL>] [-clientlessModeUrlEncoding
<clientlessModeUrlEncoding>] [-clientlessPersistentCookie <clientlessPersistentCookie>]
[-allowedLoginGroups <string>] [-SecureBrowse ( ENABLED | DISABLED )] [-storefronturl
<string>] [-kcdAccount <string>]
```

Description

Adds a session profile (action) to bind to a session policy that is applied to a user session if the policy expression conditions are met.

Parameters

name

Name for the Access Gateway profile (action). Must begin with an ASCII alphabetic or underscore (_) character, and must consist only of ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the profile is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

httpPort

Destination port numbers other than port 80, added as a comma-separated list. Traffic to these ports is processed as HTTP traffic, which allows functionality, such as HTTP authorization and single sign-on to a web application to work. Minimum value: 1

winsIP

WINS server IP address to add to Access Gateway for name resolution.

dnsVserverName

Name of the DNS virtual server for the user session.

splitDns

Route the DNS requests to the local DNS server configured on the user device, or Access Gateway (remote), or both. Possible values: LOCAL, REMOTE, BOTH

sessTimeout

Number of minutes after which the session times out. Minimum value: 1

clientSecurity

Specify the client security check for the user device to permit an Access Gateway session. The web address or IP address is not included in the expression for the client security check.

clientSecurityLog

Set the logging of client security checks. Possible values: ON, OFF

splitTunnel

Send, through the tunnel, traffic only for intranet applications that are defined in Access Gateway. Route all other traffic directly to the Internet. The OFF setting routes all traffic through Access Gateway. With the REVERSE setting, intranet applications define the network traffic that is not intercepted. All network traffic directed to internal IP addresses bypasses the VPN tunnel, while other traffic goes through Access Gateway. Reverse split tunneling can be used to log all non-local LAN traffic. For example, if users have a home network and are logged on through the Access Gateway Plug-in, network traffic destined to a printer or another device within the home network is not intercepted. Possible values: ON, OFF, REVERSE

localLanAccess

Set local LAN access. If split tunneling is OFF, and you set local LAN access to ON, the local client can route traffic to its local interface. When the local area network switch is specified, this combination of switches is useful. The client can allow local LAN access to devices that commonly have non-routable addresses, such as local printers or local file servers. Possible values: ON, OFF

rfc1918

As defined in the local area network, allow only the following local area network addresses to bypass the VPN tunnel when the local LAN access feature is enabled: * 10.*.*, * 172.16.*.*, * 192.168.*.* Possible values: ON, OFF

spoofIP

IP address that the intranet application uses to route the connection through the virtual adapter. Possible values: ON, OFF

killConnections

Specify whether the Access Gateway Plug-in should disconnect all preexisting connections, such as the connections existing before the user logged on to Access Gateway, and prevent new incoming connections on the Access Gateway Plug-in for Windows and MAC when the user is connected to Access Gateway and split tunneling is disabled. Possible values: ON, OFF

transparentInterception

Allow access to network resources by using a single IP address and subnet mask or a range of IP addresses. The OFF setting sets the mode to proxy, in which you configure

destination and source IP addresses and port numbers. If you are using the Access Gateway Plug-in for Windows, set this parameter to ON, in which the mode is set to transparent. If you are using the Access Gateway Plug-in for Java, set this parameter to OFF. Possible values: ON, OFF

windowsClientType

Choose between two types of Windows Client\ a) Application Agent - which always runs in the task bar as a standalone application and also has a supporting service which runs permanently when installed\ b) Activex Control - ActiveX control run by Microsoft's Internet Explorer. Possible values: AGENT, PLUGIN

defaultAuthorizationAction

Specify the network resources that users have access to when they log on to the internal network. The default setting for authorization is to deny access to all network resources. Citrix recommends using the default global setting and then creating authorization policies to define the network resources users can access. If you set the default authorization policy to DENY, you must explicitly authorize access to any network resource, which improves security. Possible values: ALLOW, DENY

authorizationGroup

Comma-separated list of groups in which the user is placed when none of the groups that the user is a part of is configured on Access Gateway. The authorization policy can be bound to these groups to control access to the resources.

clientIdleTimeout

Time, in minutes, after which to time out the user session if Access Gateway does not detect mouse or keyboard activity. Minimum value: 1 Maximum value: 9999

proxy

Set options to apply proxy for accessing the internal resources. Available settings function as follows: * BROWSER - Proxy settings are configured only in Internet Explorer and Firefox browsers. * NS - Proxy settings are configured on the NetScaler appliance. * OFF - Proxy settings are not configured. Possible values: BROWSER, NS, OFF

allProtocolProxy

IP address of the proxy server to use for all protocols supported by Access Gateway.

httpProxy

IP address of the proxy server to be used for HTTP access for all subsequent connections to the internal network.

ftpProxy

IP address of the proxy server to be used for FTP access for all subsequent connections to the internal network.

socksProxy

IP address of the proxy server to be used for SOCKS access for all subsequent connections to the internal network.

gopherProxy

IP address of the proxy server to be used for GOPHER access for all subsequent connections to the internal network.

sslProxy

IP address of the proxy server to be used for SSL access for all subsequent connections to the internal network.

proxyException

Proxy exception string that will be configured in the browser for bypassing the previously configured proxies. Allowed only if proxy type is Browser.

proxyLocalBypass

Bypass proxy server for local addresses option in Internet Explorer and Firefox proxy server settings. Possible values: ENABLED, DISABLED

clientCleanupPrompt

Prompt for client-side cache clean-up when a client-initiated session closes. Possible values: ON, OFF

forceCleanup

Force cache clean-up when the user closes a session. You can specify all, none, or any combination of the client-side items.

clientOptions

Display only the configured menu options when you select the "Configure Access Gateway" option in the Access Gateway Plug-in's system tray icon for Windows.

clientConfiguration

Display only the configured tabs when you select the "Configure Access Gateway" option in the Access Gateway Plug-in's system tray icon for Windows.

SSO

Set single sign-on (SSO) for the session. When the user accesses a server, the user's logon credentials are passed to the server for authentication. Possible values: ON, OFF

ssoCredential

Specify whether to use the primary or secondary authentication credentials for single sign-on to the server. Possible values: PRIMARY, SECONDARY

windowsAutoLogon

Enable or disable the Windows Auto Logon for the session. If a VPN session is established after this setting is enabled, the user is automatically logged on by using Windows credentials after the system is restarted. Possible values: ON, OFF

useMIP

Enable or disable the use of a unique IP address alias, or a mapped IP address, as the client IP address for each client session. Allow Access Gateway to use the mapped IP address as an intranet IP address when all other IP addresses are not available. When IP pooling is configured and the mapped IP is used as an intranet IP address, the mapped IP address is used when an intranet IP address cannot be assigned. Possible values: NS, OFF

useIP

Define IP address pool options. Available settings function as follows: * SPILLOVER - When an address pool is configured and the mapped IP is used as an intranet IP address, the mapped IP address is used when an intranet IP address cannot be assigned. * NOSPILOVER - When intranet IP addresses are enabled and the mapped

IP address is not used, the Transfer Login page appears for users who have used all available intranet IP addresses. * OFF - Address pool is not configured. Possible values: NOSPILLOVER, SPILLOVER, OFF

clientDebug

Set the trace level on Access Gateway. Technical support technicians use these debug logs for in-depth debugging and troubleshooting purposes. Available settings function as follows: * DEBUG - Detailed debug messages are collected and written into the specified file. * STATS - Application audit level error messages and debug statistic counters are written into the specified file. * EVENTS - Application audit-level error messages are written into the specified file. * OFF - Only critical events are logged into the Windows Application Log. Possible values: debug, stats, events, OFF

loginScript

Path to the logon script that is run when a session is established. Separate multiple scripts by using comma. A "\$" in the path signifies that the word following the "\$" is an environment variable.

logoutScript

Path to the logout script. Separate multiple scripts by using comma. A "\$" in the path signifies that the word following the "\$" is an environment variable.

homePage

Web address of the home page that appears when users log on. Otherwise, users receive the default home page for Access Gateway, which is the Access Interface.

icaProxy

Enable ICA proxy to configure secure Internet access to servers running Citrix XenApp or XenDesktop by using Citrix Receiver instead of the Access Gateway Plug-in. Possible values: ON, OFF

wihome

Web address of the Web Interface server, such as `http://<ipAddress>/Citrix/XenApp`, or Receiver for Web, which enumerates the virtualized resources, such as XenApp, XenDesktop, and cloud applications. This web address is used as the home page in ICA proxy mode. If Client Choices is ON, you must configure this setting. Because the user can choose between FullClient and ICAProxy, the user may see a different home page. An Internet web site may appear if the user gets the FullClient option, or a Web Interface site if the user gets the ICAProxy option. If the setting is not configured, the XenApp option does not appear as a client choice.

citrixReceiverHome

Web address for the Citrix Receiver home page. Configure Access Gateway so that when users log on to the appliance, the Access Gateway Plug-in opens a web browser that allows single sign-on to the Citrix Receiver home page.

wiPortalMode

Layout on the Access Interface. The COMPACT value indicates the use of small icons. Possible values: NORMAL, COMPACT

ClientChoices

Provide users with multiple logon options. With client choices, users have the option of logging on by using the Access Gateway Plug-in for Windows, Access Gateway Plug-in for Java, the Web Interface, or clientless access from one location. Depending on

how Access Gateway is configured, users are presented with up to three icons for logon choices. The most common are the Access Gateway Plug-in for Windows, Web Interface, and clientless access. Possible values: ON, OFF

epaClientType

Choose between two types of End point Windows Client a) Application Agent - which always runs in the task bar as a standalone application and also has a supporting service which runs permanently when installed b) Activex Control - ActiveX control run by Microsoft's Internet Explorer. Possible values: AGENT, PLUGIN

iipDnsSuffix

An intranet IP DNS suffix. When a user logs on to Access Gateway and is assigned an IP address, a DNS record for the user name and IP address combination is added to Access Gateway DNS cache. You can configure a DNS suffix to append to the user name when the DNS record is added to the cache. You can reach to the host from where the user is logged on by using the user's name, which can be easier to remember than an IP address. When the user logs off from Access Gateway, the record is removed from the DNS cache.

forcedTimeout

Force a disconnection from the Access Gateway Plug-in with Access Gateway after a specified number of minutes. If the session closes, the user must log on again. Minimum value: 1 Maximum value: 3000

forcedTimeoutWarning

Number of minutes to warn a user before the user session is disconnected. Minimum value: 1 Maximum value: 255

ntDomain

Single sign-on domain to use for single sign-on to applications in the internal network. This setting can be overwritten by the domain that users specify at the time of logon or by the domain that the authentication server returns.

clientlessVpnMode

Enable clientless access for web, XenApp or XenDesktop, and FileShare resources without installing the Access Gateway Plug-in. Available settings function as follows: * ON - Allow only clientless access. * OFF - Allow clientless access after users log on with the Access Gateway Plug-in. * DISABLED - Do not allow clientless access. Possible values: ON, OFF, DISABLED

emailHome

Web address for the web-based email, such as Outlook Web Access.

clientlessModeUrlEncoding

When clientless access is enabled, you can choose to encode the addresses of internal web applications or to leave the address as clear text. Available settings function as follows: * OPAQUE - Use standard encoding mechanisms to make the domain and protocol part of the resource unclear to users. * CLEAR - Do not encode the web address and make it visible to users. * ENCRYPT - Allow the domain and protocol to be encrypted using a session key. When the web address is encrypted, the URL is different for each user session for the same web resource. If users bookmark the encoded web address, save it in the web browser and then log off, they cannot connect to the web address when they log on and use the bookmark. If users save the

encrypted bookmark in the Access Interface during their session, the bookmark works each time the user logs on. Possible values: TRANSPARENT, OPAQUE, ENCRYPT

clientlessPersistentCookie

State of persistent cookies in clientless access mode. Persistent cookies are required for accessing certain features of SharePoint, such as opening and editing Microsoft Word, Excel, and PowerPoint documents hosted on the SharePoint server. A persistent cookie remains on the user device and is sent with each HTTP request. Access Gateway encrypts the persistent cookie before sending it to the plug-in on the user device, and refreshes the cookie periodically as long as the session exists. The cookie becomes stale if the session ends. Available settings function as follows: * ALLOW - Enable persistent cookies. Users can open and edit Microsoft documents stored in SharePoint. * DENY - Disable persistent cookies. Users cannot open and edit Microsoft documents stored in SharePoint. * PROMPT - Prompt users to allow or deny persistent cookies during the session. Persistent cookies are not required for clientless access if users do not connect to SharePoint. Possible values: ALLOW, DENY, PROMPT

allowedLoginGroups

Specify groups that have permission to log on to Access Gateway. Users who do not belong to this group or groups are denied access even if they have valid credentials.

SecureBrowse

Allow users to connect through Access Gateway to network resources from iOS and Android mobile devices with Citrix Receiver. Users do not need to establish a full VPN tunnel to access resources in the secure network. Possible values: ENABLED, DISABLED

storefronturl

Web address for StoreFront to be used in this session for enumeration of resources from XenApp or XenDesktop.

kcdAccount

The kcd account details to be used in SSO

[Top](#)

rm vpn sessionAction

Synopsis

```
rm vpn sessionAction <name>
```

Description

Removes an action that was previously added to a session policy.

Parameters

name

Name of the action to remove.

[Top](#)

set vpn sessionAction

Synopsis

```
set vpn sessionAction <name> [-httpPort <port> ...] [-winsIP <ip_addr>] [-  
dnsVserverName <string>] [-splitDns <splitDns>] [-sessTimeout <mins>] [-clientSecurity  
<expression>] [-clientSecurityGroup <string>] [-clientSecurityMessage <string>]] [-  
clientSecurityLog ( ON | OFF )] [-splitTunnel <splitTunnel>] [-localLanAccess ( ON |  
OFF )] [-rfc1918 ( ON | OFF )] [-spoofIIP ( ON | OFF )] [-killConnections ( ON | OFF )] [-  
transparentInterception ( ON | OFF )] [-defaultAuthorizationAction ( ALLOW | DENY )]  
[-authorizationGroup <string>] [-clientIdleTimeout <mins>] [-proxy <proxy>] [-  
allProtocolProxy <string> | -httpProxy <string> | -ftpProxy <string> | -socksProxy  
<string> | -gopherProxy <string> | -sslProxy <string>] [-proxyException <string>] [-  
proxyLocalBypass ( ENABLED | DISABLED )] [-clientCleanupPrompt ( ON | OFF )] [-  
forceCleanup <forceCleanup> ...] [-clientOptions <clientOptions> ...] [-  
clientConfiguration <clientConfiguration> ...] [-SSO ( ON | OFF )] [-ssoCredential  
( PRIMARY | SECONDARY )] [-windowsAutoLogon ( ON | OFF )] [-useMIP ( NS | OFF )] [-  
useIIP <useIIP>] [-clientDebug <clientDebug>] [-loginScript <input_filename>] [-  
logoutScript <input_filename>] [-homePage <URL>] [-icaProxy ( ON | OFF )] [-wihome  
<URL>] [-citrixReceiverHome <URL>] [-wiPortalMode ( NORMAL | COMPACT )] [-  
ClientChoices ( ON | OFF )] [-iipDnsSuffix <string>] [-forcedTimeout <mins>] [-  
forcedTimeoutWarning <mins>] [-ntDomain <string>] [-clientlessVpnMode  
<clientlessVpnMode>] [-emailHome <URL>] [-clientlessModeUrlEncoding  
<clientlessModeUrlEncoding>] [-clientlessPersistentCookie <clientlessPersistentCookie>]  
[-allowedLoginGroups <string>] [-SecureBrowse ( ENABLED | DISABLED )] [-storefronturl  
<string>] [-kcdAccount <string>]
```

Description

Modifies an action that was previously added to a session policy that is applied to a user session if the policy expression conditions are met.

Parameters

name

The name of the vpn session action.

httpPort

Destination port numbers other than port 80, added as a comma-separated list.

Traffic to these ports is processed as HTTP traffic, which allows functionality, such as HTTP authorization and single sign-on to a web application to work. Minimum value:

1

winsIP

The WINS server ip address.

dnsVserverName

Name of the DNS virtual server for the user session.

splitDns

Route the DNS requests to the local DNS server configured on the user device, or Access Gateway (remote), or both. Possible values: LOCAL, REMOTE, BOTH

sessTimeout

Number of minutes after which the session times out. Minimum value: 1

clientSecurity

Specify the client security check for the user device to permit an Access Gateway session. The web address or IP address is not included in the expression for the client security check.

clientSecurityLog

Set the logging of client security checks. Possible values: ON, OFF

splitTunnel

Send, through the tunnel, traffic only for intranet applications that are defined in Access Gateway. Route all other traffic directly to the Internet. The OFF setting routes all traffic through Access Gateway. With the REVERSE setting, intranet applications define the network traffic that is not intercepted. All network traffic directed to internal IP addresses bypasses the VPN tunnel, while other traffic goes through Access Gateway. Reverse split tunneling can be used to log all non-local LAN traffic. For example, if users have a home network and are logged on through the Access Gateway Plug-in, network traffic destined to a printer or another device within the home network is not intercepted. Possible values: ON, OFF, REVERSE

localLanAccess

Set local LAN access. If split tunneling is OFF, and you set local LAN access to ON, the local client can route traffic to its local interface. When the local area network switch is specified, this combination of switches is useful. The client can allow local LAN access to devices that commonly have non-routable addresses, such as local printers or local file servers. Possible values: ON, OFF

rfc1918

As defined in the local area network, allow only the following local area network addresses to bypass the VPN tunnel when the local LAN access feature is enabled: * 10.*.*, * 172.16.*.*, * 192.168.*.* Possible values: ON, OFF

spoofIP

IP address that the intranet application uses to route the connection through the virtual adapter. Possible values: ON, OFF

killConnections

Specify whether the Access Gateway Plug-in should disconnect all preexisting connections, such as the connections existing before the user logged on to Access Gateway, and prevent new incoming connections on the Access Gateway Plug-in for Windows and MAC when the user is connected to Access Gateway and split tunneling is disabled. Possible values: ON, OFF

transparentInterception

Allow access to network resources by using a single IP address and subnet mask or a range of IP addresses. The OFF setting sets the mode to proxy, in which you configure destination and source IP addresses and port numbers. If you are using the Access Gateway Plug-in for Windows, set this parameter to ON, in which the mode is set to transparent. If you are using the Access Gateway Plug-in for Java, set this parameter to OFF. Possible values: ON, OFF

windowsClientType

Choose between two types of Windows Client\ a) Application Agent - which always runs in the task bar as a standalone application and also has a supporting service which runs permanently when installed\ b) Activex Control - ActiveX control run by Microsoft's Internet Explorer. Possible values: AGENT, PLUGIN

defaultAuthorizationAction

Specify the network resources that users have access to when they log on to the internal network. The default setting for authorization is to deny access to all network resources. Citrix recommends using the default global setting and then creating authorization policies to define the network resources users can access. If you set the default authorization policy to DENY, you must explicitly authorize access to any network resource, which improves security. Possible values: ALLOW, DENY

authorizationGroup

Comma-separated list of groups in which the user is placed when none of the groups that the user is a part of is configured on Access Gateway. The authorization policy can be bound to these groups to control access to the resources.

clientIdleTimeout

Time, in minutes, after which to time out the user session if Access Gateway does not detect mouse or keyboard activity. Minimum value: 1 Maximum value: 9999

proxy

Set options to apply proxy for accessing the internal resources. Available settings function as follows: * BROWSER - Proxy settings are configured only in Internet Explorer and Firefox browsers. * NS - Proxy settings are configured on the NetScaler appliance. * OFF - Proxy settings are not configured. Possible values: BROWSER, NS, OFF

allProtocolProxy

IP address of the proxy server to use for all protocols supported by Access Gateway.

httpProxy

IP address of the proxy server to be used for HTTP access for all subsequent connections to the internal network.

ftpProxy

IP address of the proxy server to be used for FTP access for all subsequent connections to the internal network.

socksProxy

IP address of the proxy server to be used for SOCKS access for all subsequent connections to the internal network.

gopherProxy

IP address of the proxy server to be used for GOPHER access for all subsequent connections to the internal network.

sslProxy

IP address of the proxy server to be used for SSL access for all subsequent connections to the internal network.

proxyException

Proxy exception string that will be configured in the browser for bypassing the previously configured proxies. Allowed only if proxy type is Browser.

proxyLocalBypass

Bypass proxy server for local addresses option in Internet Explorer and Firefox proxy server settings. Possible values: ENABLED, DISABLED

clientCleanupPrompt

Prompt for client-side cache clean-up when a client-initiated session closes. Possible values: ON, OFF

forceCleanup

Force cache clean-up when the user closes a session. You can specify all, none, or any combination of the client-side items.

clientOptions

Display only the configured menu options when you select the "Configure Access Gateway" option in the Access Gateway Plug-in's system tray icon for Windows.

clientConfiguration

Display only the configured tabs when you select the "Configure Access Gateway" option in the Access Gateway Plug-in's system tray icon for Windows.

SSO

Set single sign-on (SSO) for the session. When the user accesses a server, the user's logon credentials are passed to the server for authentication. Possible values: ON, OFF

ssoCredential

Specify whether to use the primary or secondary authentication credentials for single sign-on to the server. Possible values: PRIMARY, SECONDARY

windowsAutoLogon

Enable or disable the Windows Auto Logon for the session. If a VPN session is established after this setting is enabled, the user is automatically logged on by using Windows credentials after the system is restarted. Possible values: ON, OFF

useMIP

Enable or disable the use of a unique IP address alias, or a mapped IP address, as the client IP address for each client session. Allow Access Gateway to use the mapped IP address as an intranet IP address when all other IP addresses are not available. When IP pooling is configured and the mapped IP is used as an intranet IP address, the mapped IP address is used when an intranet IP address cannot be assigned. Possible values: NS, OFF

useIP

Define IP address pool options. Available settings function as follows: * SPILLOVER - When an address pool is configured and the mapped IP is used as an intranet IP address, the mapped IP address is used when an intranet IP address cannot be assigned. * NOSPILLOVER - When intranet IP addresses are enabled and the mapped IP address is not used, the Transfer Login page appears for users who have used all available intranet IP addresses. * OFF - Address pool is not configured. Possible values: NOSPILLOVER, SPILLOVER, OFF

clientDebug

Set the trace level on Access Gateway. Technical support technicians use these debug logs for in-depth debugging and troubleshooting purposes. Available settings function as follows: * DEBUG - Detailed debug messages are collected and written into the specified file. * STATS - Application audit level error messages and debug statistic counters are written into the specified file. * EVENTS - Application audit-level error messages are written into the specified file. * OFF - Only critical events are logged into the Windows Application Log. Possible values: debug, stats, events, OFF

loginScript

Path to the logon script that is run when a session is established. Separate multiple scripts by using comma. A "\$" in the path signifies that the word following the "\$" is an environment variable.

logoutScript

Path to the logout script. Separate multiple scripts by using comma. A "\$" in the path signifies that the word following the "\$" is an environment variable.

homePage

Web address of the home page that appears when users log on. Otherwise, users receive the default home page for Access Gateway, which is the Access Interface.

icaProxy

Enable ICA proxy to configure secure Internet access to servers running Citrix XenApp or XenDesktop by using Citrix Receiver instead of the Access Gateway Plug-in. Possible values: ON, OFF Default value: OFF

wihome

Web address of the Web Interface server, such as `http://<ipAddress>/Citrix/XenApp`, or Receiver for Web, which enumerates the virtualized resources, such as XenApp, XenDesktop, and cloud applications. This web address is used as the home page in ICA proxy mode. If Client Choices is ON, you must configure this setting. Because the user can choose between FullClient and ICAProxy, the user may see a different home page. An Internet web site may appear if the user gets the FullClient option, or a Web Interface site if the user gets the ICAProxy option. If the setting is not configured, the XenApp option does not appear as a client choice.

citrixReceiverHome

Web address for the Citrix Receiver home page. Configure Access Gateway so that when users log on to the appliance, the Access Gateway Plug-in opens a web browser that allows single sign-on to the Citrix Receiver home page.

wiPortalMode

Layout on the Access Interface. The COMPACT value indicates the use of small icons. Possible values: NORMAL, COMPACT

ClientChoices

Provide users with multiple logon options. With client choices, users have the option of logging on by using the Access Gateway Plug-in for Windows, Access Gateway Plug-in for Java, the Web Interface, or clientless access from one location. Depending on how Access Gateway is configured, users are presented with up to three icons for logon choices. The most common are the Access Gateway Plug-in for Windows, Web Interface, and clientless access. Possible values: ON, OFF

epaClientType

Choose between two types of End point Windows Client a) Application Agent - which always runs in the task bar as a standalone application and also has a supporting service which runs permanently when installed b) Activex Control - ActiveX control run by Microsoft's Internet Explorer. Possible values: AGENT, PLUGIN

iipDnsSuffix

An intranet IP DNS suffix. When a user logs on to Access Gateway and is assigned an IP address, a DNS record for the user name and IP address combination is added to Access Gateway DNS cache. You can configure a DNS suffix to append to the user name when the DNS record is added to the cache. You can reach to the host from where the user is logged on by using the user's name, which can be easier to remember than an IP address. When the user logs off from Access Gateway, the record is removed from the DNS cache.

forcedTimeout

Force a disconnection from the Access Gateway Plug-in with Access Gateway after a specified number of minutes. If the session closes, the user must log on again. Minimum value: 1 Maximum value: 3000

forcedTimeoutWarning

Number of minutes to warn a user before the user session is disconnected. Minimum value: 1 Maximum value: 255

ntDomain

Single sign-on domain to use for single sign-on to applications in the internal network. This setting can be overwritten by the domain that users specify at the time of logon or by the domain that the authentication server returns.

clientlessVpnMode

Enable clientless access for web, XenApp or XenDesktop, and FileShare resources without installing the Access Gateway Plug-in. Available settings function as follows: * ON - Allow only clientless access. * OFF - Allow clientless access after users log on with the Access Gateway Plug-in. * DISABLED - Do not allow clientless access. Possible values: ON, OFF, DISABLED Default value: VPN_SESS_ACT_CVPNMODE_OFF

emailHome

Web address for the web-based email, such as Outlook Web Access.

clientlessModeUrlEncoding

When clientless access is enabled, you can choose to encode the addresses of internal web applications or to leave the address as clear text. Available settings function as follows: * OPAQUE - Use standard encoding mechanisms to make the domain and protocol part of the resource unclear to users. * CLEAR - Do not encode the web address and make it visible to users. * ENCRYPT - Allow the domain and protocol to be encrypted using a session key. When the web address is encrypted, the URL is different for each user session for the same web resource. If users bookmark the encoded web address, save it in the web browser and then log off, they cannot connect to the web address when they log on and use the bookmark. If users save the encrypted bookmark in the Access Interface during their session, the bookmark works each time the user logs on. Possible values: TRANSPARENT, OPAQUE, ENCRYPT

clientlessPersistentCookie

State of persistent cookies in clientless access mode. Persistent cookies are required for accessing certain features of SharePoint, such as opening and editing Microsoft Word, Excel, and PowerPoint documents hosted on the SharePoint server. A persistent cookie remains on the user device and is sent with each HTTP request. Access Gateway encrypts the persistent cookie before sending it to the plug-in on the user device, and refreshes the cookie periodically as long as the session exists. The cookie becomes stale if the session ends. Available settings function as follows: * ALLOW - Enable persistent cookies. Users can open and edit Microsoft documents stored in SharePoint. * DENY - Disable persistent cookies. Users cannot open and edit Microsoft documents stored in SharePoint. * PROMPT - Prompt users to allow or deny persistent cookies during the session. Persistent cookies are not required for clientless access if users do not connect to SharePoint. Possible values: ALLOW, DENY, PROMPT Default value: VPN_SESS_ACT_CVPN_PERSCookie_DENY

allowedLoginGroups

Specify groups that have permission to log on to Access Gateway. Users who do not belong to this group or groups are denied access even if they have valid credentials.

SecureBrowse

Allow users to connect through Access Gateway to network resources from iOS and Android mobile devices with Citrix Receiver. Users do not need to establish a full VPN tunnel to access resources in the secure network. Possible values: ENABLED, DISABLED

storefronturl

Web address for StoreFront to be used in this session for enumeration of resources from XenApp or XenDesktop.

kcdAccount

The kcd account details to be used in SSO

[Top](#)

unset vpn sessionAction

Synopsis

```
unset vpn sessionAction <name> [-httpPort] [-winsIP] [-dnsVserverName] [-splitDns] [-sessTimeout] [-clientSecurity] [-clientSecurityGroup] [-clientSecurityMessage] [-clientSecurityLog] [-splitTunnel] [-localLanAccess] [-rfc1918] [-spoofIIP] [-killConnections] [-transparentInterception] [-defaultAuthorizationAction] [-authorizationGroup] [-clientIdleTimeout] [-proxy] [-allProtocolProxy] [-httpProxy] [-ftpProxy] [-socksProxy] [-gopherProxy] [-sslProxy] [-proxyException] [-proxyLocalBypass] [-clientCleanupPrompt] [-forceCleanup] [-clientOptions] [-clientConfiguration] [-SSO] [-ssoCredential] [-windowsAutoLogon] [-useMIP] [-useIIP] [-clientDebug] [-loginScript] [-logoutScript] [-homePage] [-icaProxy] [-wihome] [-citrixReceiverHome] [-wiPortalMode] [-ClientChoices] [-iipDnsSuffix] [-forcedTimeout] [-forcedTimeoutWarning] [-ntDomain] [-clientlessVpnMode] [-emailHome] [-clientlessModeUrlEncoding] [-clientlessPersistentCookie] [-allowedLoginGroups] [-SecureBrowse] [-storefronturl] [-kcdAccount]
```

Description

Use this command to remove vpn sessionAction settings. Refer to the set vpn sessionAction command for meanings of the arguments.

[Top](#)

show vpn sessionAction

Synopsis

show vpn sessionAction [<name>]

Description

Displays a session action that is applied to a user session if the policy expression conditions are met.

Parameters

name

Name of the session action to display.

[Top](#)

vpn clientlessAccessPolicy

[[add](#) | [rm](#) | [set](#) | [show](#)]

add vpn clientlessAccessPolicy

Synopsis

add vpn clientlessAccessPolicy <name> <rule> <profileName>

Description

Adds a clientless access policy, which enables users to log on using a web browser and connect to the bookmarked web address without requiring the user to install a software plug-in.

Parameters

name

Name of the new clientless access policy.

rule

Expression, or name of a named expression, specifying the traffic that matches the policy. Can be written in either default or classic syntax. Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>". The following requirements apply only to the NetScaler CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the \ character. *

Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

profileName

Name of the profile to invoke for the clientless access.

[Top](#)

rm vpn clientlessAccessPolicy

Synopsis

```
rm vpn clientlessAccessPolicy <name>
```

Description

Removes a clientless access policy.

Parameters

name

Name of the clientless access policy to remove.

[Top](#)

set vpn clientlessAccessPolicy

Synopsis

```
set vpn clientlessAccessPolicy <name> [-rule <expression>] [-profileName <string>]
```

Description

Adds a new rule to be used by an existing clientless access policy that includes a simple expression that specifies the conditions for which the policy is enforced.

Parameters

name

Name of the existing clientless access policy to modify.

rule

Expression, or name of a named expression, specifying the traffic that matches the policy. Can be written in either default or classic syntax. Maximum length of a string literal in the expression is 255 characters. A longer string can be split into smaller strings of up to 255 characters each, and the smaller strings concatenated with the + operator. For example, you can create a 500-character string as follows: "<string of 255 characters>" + "<string of 245 characters>". The following requirements apply only to the NetScaler CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

profileName

Name of the profile to invoke for the clientless access.

[Top](#)

show vpn clientlessAccessPolicy

Synopsis

show vpn clientlessAccessPolicy [<name>]

Description

Displays a clientless access policy.

Parameters

name

Name of the clientless access policy to display.

[Top](#)

vpn clientlessAccessProfile

[[add](#) | [rm](#) | [set](#) | [unset](#) | [show](#)]

add vpn clientlessAccessProfile

Synopsis

add vpn clientlessAccessProfile <profileName>

Description

Adds a collection of settings that allows clientless access to a given application. Settings include the policies to specify whether to rewrite a URL, rules to find the URLs within various web content-types, and a set of cookies that are required to be present on the client machine.

Parameters

profileName

Name for the Access Gateway clientless access profile. Must begin with an ASCII alphabetic or underscore (_) character, and must consist only of ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the profile is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my profile" or 'my profile').

[Top](#)

rm vpn clientlessAccessProfile

Synopsis

rm vpn clientlessAccessProfile <profileName>

Description

Removes a clientless access profile.

Parameters

profileName

Name of the clientless access profile to remove.

[Top](#)

set vpn clientlessAccessProfile

Synopsis

```
set vpn clientlessAccessProfile <profileName> [-URLRewritePolicyLabel <string>] [-  
JavaScriptRewritePolicyLabel <string>] [-ReqHdrRewritePolicyLabel <string>] [-  
ResHdrRewritePolicyLabel <string>] [-RegexForFindingURLinJavaScript <string>] [-  
RegexForFindingURLinCSS <string>] [-RegexForFindingURLinXComponent <string>] [-  
RegexForFindingURLinXML <string>] [-RegexForFindingCustomURLs <string>] [-  
ClientConsumedCookies <string>] [-requirePersistentCookie ( ON | OFF )]
```

Description

Modifies the settings for an existing clientless access profile.

Parameters

profileName

Name of the clientless access profile to modify.

URLRewritePolicyLabel

Name of the configured URL rewrite policy label. If you do not specify a policy label name, then URLs are not rewritten.

JavaScriptRewritePolicyLabel

Name of the configured JavaScript rewrite policy label. If you do not specify a policy label name, then JAVA scripts are not rewritten.

ReqHdrRewritePolicyLabel

Name of the configured Request rewrite policy label. If you do not specify a policy label name, then requests are not rewritten.

ResHdrRewritePolicyLabel

Name of the configured Response rewrite policy label.

RegexForFindingURLinJavaScript

Name of the pattern set that contains the regular expressions, which match the URL in Java script.

RegexForFindingURLinCSS

Name of the pattern set that contains the regular expressions, which match the URL in the CSS.

RegexForFindingURLinXComponent

Name of the pattern set that contains the regular expressions, which match the URL in X Component.

RegexForFindingURLinXML

Name of the pattern set that contains the regular expressions, which match the URL in XML.

RegexForFindingCustomURLs

Name of the pattern set that contains the regular expressions, which match the URLs in the custom content type other than HTML, CSS, XML, XCOMP, and JavaScript. The custom content type should be included in the patset ns_cvpn_custom_content_types.

ClientConsumedCookies

Specify the name of the pattern set containing the names of the cookies, which are allowed between the client and the server. If a pattern set is not specified, Access Gateway does not allow any cookies between the client and the server. A cookie that is not specified in the pattern set is handled by Access Gateway on behalf of the client.

requirePersistentCookie

Specify whether a persistent session cookie is set and accepted for clientless access. If this parameter is set to ON, COM objects, such as MSOffice, which are invoked by the browser can access the files using clientless access. Use caution because the persistent cookie is stored on the disk. Possible values: ON, OFF Default value: OFF

[Top](#)

unset vpn clientlessAccessProfile**Synopsis**

```
unset vpn clientlessAccessProfile <profileName> [-URLRewritePolicyLabel] [-
JavaScriptRewritePolicyLabel] [-ReqHdrRewritePolicyLabel] [-
ResHdrRewritePolicyLabel] [-RegexForFindingURLinJavaScript] [-
RegexForFindingURLinCSS] [-RegexForFindingURLinXComponent] [-
RegexForFindingURLinXML] [-RegexForFindingCustomURLs] [-ClientConsumedCookies] [-
requirePersistentCookie]
```

Description

Resets the attributes of the specified clientless access profile. Attributes for which a default value is available revert to their default values. Refer to the set vpn clientlessAccessProfile command for a description of the parameters..Refer to the set vpn clientlessAccessProfile command for meanings of the arguments.

[Top](#)

show vpn clientlessAccessProfile**Synopsis**

```
show vpn clientlessAccessProfile [<profileName>]
```

Description

Displays information about all the configured clientless access profiles, or displays detailed information about the specified clientless access profile.

Parameters**profileName**

Name of the clientless access profile for which to display detailed information.

[Top](#)

vpn stats

show vpn stats

Synopsis

show vpn stats - alias for 'stat vpn'

Description

show vpn stats is an alias for stat vpn

vpn icaConnection

show vpn icaConnection

Synopsis

show vpn icaConnection [-userName <string>]

Description

Displays active connections that use the ICA proxy.

Parameters

userName

User name for which to display connections.

vpn global

[[bind](#) | [unbind](#) | [show](#)]

bind vpn global

Synopsis

bind vpn global [-policyName <string> [-priority <positive_integer>] [-secondary] [-groupExtraction]] [-intranetDomain <string>] [-intranetApplication <string>] [-nextHopServer <string>] [-urlName <string>] [-intranetIP <ip_addr> <netmask>] [-staServer <URL>] [-appController <URL>] [-sharefile <string>]

Description

Binds Access Gateway entities, including policies, globally.

Parameters

policyName

Name of the policy to bind globally.

intranetDomain

Intranet domain name for single sign-on.

intranetApplication

Name of the intranet application to bind globally.

nextHopServer

Name of the next hop server to bind globally.

urlName

Name of the URL of the virtual server to bind globally.

intranetIP

Range of IP addresses in an address pool or individual IP addresses to bind globally.

staServer

Web address of the Secure Ticketing Authority (STA) server to be bound globally, in the following format: 'http(s)://FQDN/URLPATH'

appController

AppController server, in the format 'http(s)://IP/FQDN'

sharefile

Sharefile server, in the format 'IP:PORT / FQDN:PORT'

[Top](#)

unbind vpn global

Synopsis

```
unbind vpn global [-policyName <string> [-secondary] [-groupExtraction]] [-intranetDomain <string>] [-intranetApplication <string>] [-nextHopServer <string>] [-urlName <string>] [-intranetIP <ip_addr> <netmask>] [-staServer <URL>] [-appController <URL>] [-sharefile <string>]
```

Description

Unbinds Access Gateway policies to the virtual server globally.

Parameters

policyName

Name of the policy to unbind globally.

intranetDomain

A conflicting intranet domain name to be unbound.

intranetApplication

The name of a vpn intranet application to be unbound.

nextHopServer

The name of the next hop server to be unbound globally.

urlName

The name of a vpn url to be unbound from vpn global.

intranetIP

The intranet ip address or range to be unbound.

staServer

Secure Ticketing Authority (STA) server to be removed, in the format 'http(s)://IP/FQDN/URLPATH'

appController

AppController server to be removed, in the format 'http(s)://IP/FQDN'

sharefile

Sharefile server to be removed, in the format 'IP:PORT / FQDN:PORT'

[Top](#)

show vpn global

Synopsis

show vpn global

Description

Shows the Access Gateway policies that are bound to the virtual server globally.

[Top](#)

vpn parameter

[[set](#) | [unset](#) | [show](#)]

set vpn parameter

Synopsis

```
set vpn parameter [-httpPort <port> ...] [-winsIP <ip_addr>] [-dnsVserverName
<string>] [-splitDns <splitDns>] [-sessTimeout <mins>] [-clientSecurity <expression> [-
clientSecurityGroup <string>] [-clientSecurityMessage <string>]] [-clientSecurityLog
( ON | OFF )] [-splitTunnel <splitTunnel>] [-localLanAccess ( ON | OFF )] [-rfc1918 ( ON
| OFF )] [-spoofIP ( ON | OFF )] [-killConnections ( ON | OFF )] [-
transparentInterception ( ON | OFF )] [-defaultAuthorizationAction ( ALLOW | DENY )]
[-authorizationGroup <string>] [-clientIdleTimeout <mins>] [-proxy <proxy>] [-
allProtocolProxy <string> | -httpProxy <string> | -ftpProxy <string> | -socksProxy
<string> | -gopherProxy <string> | -sslProxy <string>] [-proxyException <string>] [-
proxyLocalBypass ( ENABLED | DISABLED )] [-clientCleanupPrompt ( ON | OFF )] [-
forceCleanup <forceCleanup> ...] [-clientOptions <clientOptions> ...] [-
clientConfiguration <clientConfiguration> ...] [-SSO ( ON | OFF )] [-ssoCredential
( PRIMARY | SECONDARY )] [-windowsAutoLogon ( ON | OFF )] [-useMIP ( NS | OFF )] [-
useIP <useIP>] [-clientDebug <clientDebug>] [-loginScript <input_filename>] [-
logoutScript <input_filename>] [-homePage <URL>] [-icaProxy ( ON | OFF )] [-wihome
<URL>] [-citrixReceiverHome <URL>] [-wiPortalMode ( NORMAL | COMPACT )] [-
ClientChoices ( ON | OFF )] [-iipDnsSuffix <string>] [-forcedTimeout <mins>] [-
forcedTimeoutWarning <mins>] [-ntDomain <string>] [-clientlessVpnMode
<clientlessVpnMode>] [-clientlessModeUrlEncoding <clientlessModeUrlEncoding>] [-
clientlessPersistentCookie <clientlessPersistentCookie>] [-emailHome <URL>] [-
allowedLoginGroups <string>] [-encryptCsecExp ( ENABLED | DISABLED )] [-
appTokenTimeout <positive_integer>] [-mdxTokenTimeout <positive_integer>] [-
```

```
UITHEME <UITHEME>] [-SecureBrowse ( ENABLED | DISABLED )] [-storefronturl <string>]  
[-kcdAccount <string>]
```

Description

Sets global parameters for Access Gateway.

Parameters

httpPort

Destination port numbers other than port 80, added as a comma-separated list. Traffic to these ports is processed as HTTP traffic, which allows functionality, such as HTTP authorization and single sign-on to a web application to work. Minimum value: 1

winsIP

WINS server IP address to add to Access Gateway for name resolution.

dnsVserverName

Name of the DNS virtual server for the user session.

splitDns

Route the DNS requests to the local DNS server configured on the user device, or Access Gateway (remote), or both. Possible values: LOCAL, REMOTE, BOTH

sessTimeout

Number of minutes after which the session times out. Default value: 30 Minimum value: 1

clientSecurity

Specify the client security check for the user device to permit an Access Gateway session. The web address or IP address is not included in the expression for the client security check.

clientSecurityLog

Set the logging of client security checks. Possible values: ON, OFF Default value: VPN_SESS_ACT_ON

splitTunnel

Send, through the tunnel, traffic only for intranet applications that are defined in Access Gateway. Route all other traffic directly to the Internet. The OFF setting routes all traffic through Access Gateway. With the REVERSE setting, intranet applications define the network traffic that is not intercepted. All network traffic directed to internal IP addresses bypasses the VPN tunnel, while other traffic goes through Access Gateway. Reverse split tunneling can be used to log all non-local LAN traffic. For example, if users have a home network and are logged on through the Access Gateway Plug-in, network traffic destined to a printer or another device within the home network is not intercepted. Possible values: ON, OFF, REVERSE Default value: VPN_SESS_ACT_OFF

localLanAccess

Set local LAN access. If split tunneling is OFF, and you set local LAN access to ON, the local client can route traffic to its local interface. When the local area network switch is specified, this combination of switches is useful. The client can allow local LAN access to devices that commonly have non-routable addresses, such as local

printers or local file servers. Possible values: ON, OFF Default value: VPN_SESS_ACT_OFF

rfc1918

As defined in the local area network, allow only the following local area network addresses to bypass the VPN tunnel when the local LAN access feature is enabled: * 10.*.*, * 172.16.*.*, * 192.168.*.* Possible values: ON, OFF Default value: VPN_SESS_ACT_OFF

spoofIP

Indicate whether or not the application requires IP spoofing, which routes the connection to the intranet application through the virtual adapter. Possible values: ON, OFF Default value: ON

killConnections

Specify whether the Access Gateway Plug-in should disconnect all preexisting connections, such as the connections existing before the user logged on to Access Gateway, and prevent new incoming connections on the Access Gateway Plug-in for Windows and MAC when the user is connected to Access Gateway and split tunneling is disabled. Possible values: ON, OFF Default value: VPN_SESS_ACT_OFF

transparentInterception

Allow access to network resources by using a single IP address and subnet mask or a range of IP addresses. The OFF setting sets the mode to proxy, in which you configure destination and source IP addresses and port numbers. If you are using the Access Gateway Plug-in for Windows, set this parameter to ON, in which the mode is set to transparent. If you are using the Access Gateway Plug-in for Java, set this parameter to OFF. Possible values: ON, OFF Default value: VPN_SESS_ACT_ON

windowsClientType

The Windows client type. Choose between two types of Windows Client\ a) Application Agent - which always runs in the task bar as a standalone application and also has a supporting service which runs permanently when installed\ b) Activex Control - ActiveX control run by Microsoft's Internet Explorer. Possible values: AGENT, PLUGIN Default value: VPN_SESS_ACT_CLT_AGENT

defaultAuthorizationAction

Specify the network resources that users have access to when they log on to the internal network. The default setting for authorization is to deny access to all network resources. Citrix recommends using the default global setting and then creating authorization policies to define the network resources users can access. If you set the default authorization policy to DENY, you must explicitly authorize access to any network resource, which improves security. Possible values: ALLOW, DENY

authorizationGroup

Comma-separated list of groups in which the user is placed when none of the groups that the user is a part of is configured on Access Gateway. The authorization policy can be bound to these groups to control access to the resources.

clientIdleTimeout

Time, in minutes, after which to time out the user session if Access Gateway does not detect mouse or keyboard activity. Minimum value: 1 Maximum value: 9999

proxy

Set options to apply proxy for accessing the internal resources. Available settings function as follows: * BROWSER - Proxy settings are configured only in Internet Explorer and Firefox browsers. * NS - Proxy settings are configured on the NetScaler appliance. * OFF - Proxy settings are not configured. Possible values: BROWSER, NS, OFF

allProtocolProxy

IP address of the proxy server to use for all protocols supported by Access Gateway.

httpProxy

IP address of the proxy server to be used for HTTP access for all subsequent connections to the internal network.

ftpProxy

IP address of the proxy server to be used for FTP access for all subsequent connections to the internal network.

socksProxy

IP address of the proxy server to be used for SOCKS access for all subsequent connections to the internal network.

gopherProxy

IP address of the proxy server to be used for GOPHER access for all subsequent connections to the internal network.

sslProxy

IP address of the proxy server to be used for SSL access for all subsequent connections to the internal network.

proxyException

Proxy exception string that will be configured in the browser for bypassing the previously configured proxies. Allowed only if proxy type is Browser.

proxyLocalBypass

Bypass proxy server for local addresses option in Internet Explorer and Firefox proxy server settings. Possible values: ENABLED, DISABLED Default value: VPN_SESS_ACT_DISABLED

clientCleanupPrompt

Prompt for client-side cache clean-up when a client-initiated session closes. Possible values: ON, OFF Default value: VPN_SESS_ACT_ON

forceCleanup

Force cache clean-up when the user closes a session. You can specify all, none, or any combination of the client-side items.

clientOptions

Display only the configured menu options when you select the "Configure Access Gateway" option in the Access Gateway Plug-in's system tray icon for Windows.

clientConfiguration

Display only the configured tabs when you select the "Configure Access Gateway" option in the Access Gateway Plug-in's system tray icon for Windows.

SSO

Set single sign-on (SSO) for the session. When the user accesses a server, the user's logon credentials are passed to the server for authentication. Possible values: ON, OFF Default value: VPN_SESS_ACT_OFF

ssoCredential

Specify whether to use the primary or secondary authentication credentials for single sign-on to the server. Possible values: PRIMARY, SECONDARY Default value: VPN_SESS_ACT_USE_PRIMARY_CREDENTIALS

windowsAutoLogon

Enable or disable the Windows Auto Logon for the session. If a VPN session is established after this setting is enabled, the user is automatically logged on by using Windows credentials after the system is restarted. Possible values: ON, OFF Default value: VPN_SESS_ACT_OFF

useMIP

Enable or disable the use of a unique IP address alias, or a mapped IP address, as the client IP address for each client session. Allow Access Gateway to use the mapped IP address as an intranet IP address when all other IP addresses are not available. When IP pooling is configured and the mapped IP is used as an intranet IP address, the mapped IP address is used when an intranet IP address cannot be assigned. Possible values: NS, OFF Default value: VPN_SESS_ACT_NS

useIP

Define IP address pool options. Available settings function as follows: * SPILLOVER - When an address pool is configured and the mapped IP is used as an intranet IP address, the mapped IP address is used when an intranet IP address cannot be assigned. * NOSPILLOVER - When intranet IP addresses are enabled and the mapped IP address is not used, the Transfer Login page appears for users who have used all available intranet IP addresses. * OFF - Address pool is not configured. Possible values: NOSPILLOVER, SPILLOVER, OFF Default value: VPN_SESS_ACT_NOSPILLOVER

clientDebug

Set the trace level on Access Gateway. Technical support technicians use these debug logs for in-depth debugging and troubleshooting purposes. Available settings function as follows: * DEBUG - Detailed debug messages are collected and written into the specified file. * STATS - Application audit level error messages and debug statistic counters are written into the specified file. * EVENTS - Application audit-level error messages are written into the specified file. * OFF - Only critical events are logged into the Windows Application Log. Possible values: debug, stats, events, OFF Default value: VPN_FLAG_TRACE_OFF

loginScript

Path to the logon script that is run when a session is established. Separate multiple scripts by using comma. A "\$" in the path signifies that the word following the "\$" is an environment variable.

logoutScript

Path to the logout script. Separate multiple scripts by using comma. A "\$" in the path signifies that the word following the "\$" is an environment variable.

homePage

Web address of the home page that appears when users log on. Otherwise, users receive the default home page for Access Gateway, which is the Access Interface.

icaProxy

Enable ICA proxy to configure secure Internet access to servers running Citrix XenApp or XenDesktop by using Citrix Receiver instead of the Access Gateway Plug-in.

Possible values: ON, OFF Default value: VPN_SESS_ACT_OFF

wihome

Web address of the Web Interface server, such as `http://<ipAddress>/Citrix/XenApp`, or Receiver for Web, which enumerates the virtualized resources, such as XenApp, XenDesktop, and cloud applications. This web address is used as the home page in ICA proxy mode. If Client Choices is ON, you must configure this setting. Because the user can choose between FullClient and ICAProxy, the user may see a different home page. An Internet web site may appear if the user gets the FullClient option, or a Web Interface site if the user gets the ICAProxy option. If the setting is not configured, the XenApp option does not appear as a client choice.

citrixReceiverHome

Web address for the Citrix Receiver home page. Configure Access Gateway so that when users log on to the appliance, the Access Gateway Plug-in opens a web browser that allows single sign-on to the Citrix Receiver home page.

wiPortalMode

Layout on the Access Interface. The COMPACT value indicates the use of small icons.

Possible values: NORMAL, COMPACT

ClientChoices

Provide users with multiple logon options. With client choices, users have the option of logging on by using the Access Gateway Plug-in for Windows, Access Gateway Plug-in for Java, the Web Interface, or clientless access from one location. Depending on how Access Gateway is configured, users are presented with up to three icons for logon choices. The most common are the Access Gateway Plug-in for Windows, Web Interface, and clientless access. Possible values: ON, OFF Default value:

VPN_SESS_ACT_OFF

epaClientType

Choose between two types of End point Windows Client a) Application Agent - which always runs in the task bar as a standalone application and also has a supporting service which runs permanently when installed b) Activex Control - ActiveX control run by Microsoft's Internet Explorer. Possible values: AGENT, PLUGIN

iipDnsSuffix

An intranet IP DNS suffix. When a user logs on to Access Gateway and is assigned an IP address, a DNS record for the user name and IP address combination is added to Access Gateway DNS cache. You can configure a DNS suffix to append to the user name when the DNS record is added to the cache. You can reach to the host from where the user is logged on by using the user's name, which can be easier to remember than an IP address. When the user logs off from Access Gateway, the record is removed from the DNS cache.

forcedTimeout

Force a disconnection from the Access Gateway Plug-in with Access Gateway after a specified number of minutes. If the session closes, the user must log on again.

Minimum value: 1 Maximum value: 3000

forcedTimeoutWarning

Number of minutes to warn a user before the user session is disconnected. Minimum value: 1 Maximum value: 255

ntDomain

Single sign-on domain to use for single sign-on to applications in the internal network. This setting can be overwritten by the domain that users specify at the time of logon or by the domain that the authentication server returns.

clientlessVpnMode

Enable clientless access for web, XenApp or XenDesktop, and FileShare resources without installing the Access Gateway Plug-in. Available settings function as follows: * ON - Allow only clientless access. * OFF - Allow clientless access after users log on with the Access Gateway Plug-in. * DISABLED - Do not allow clientless access.

Possible values: ON, OFF, DISABLED Default value: VPN_SESS_ACT_CVPNMODE_OFF

clientlessModeUrlEncoding

When clientless access is enabled, you can choose to encode the addresses of internal web applications or to leave the address as clear text. Available settings function as follows: * OPAQUE - Use standard encoding mechanisms to make the domain and protocol part of the resource unclear to users. * CLEAR - Do not encode the web address and make it visible to users. * ENCRYPT - Allow the domain and protocol to be encrypted using a session key. When the web address is encrypted, the URL is different for each user session for the same web resource. If users bookmark the encoded web address, save it in the web browser and then log off, they cannot connect to the web address when they log on and use the bookmark. If users save the encrypted bookmark in the Access Interface during their session, the bookmark works each time the user logs on. Possible values: TRANSPARENT, OPAQUE, ENCRYPT Default value: VPN_SESS_ACT_CVPN_ENC_OPAQUE

clientlessPersistentCookie

State of persistent cookies in clientless access mode. Persistent cookies are required for accessing certain features of SharePoint, such as opening and editing Microsoft Word, Excel, and PowerPoint documents hosted on the SharePoint server. A persistent cookie remains on the user device and is sent with each HTTP request. Access Gateway encrypts the persistent cookie before sending it to the plug-in on the user device, and refreshes the cookie periodically as long as the session exists. The cookie becomes stale if the session ends. Available settings function as follows: * ALLOW - Enable persistent cookies. Users can open and edit Microsoft documents stored in SharePoint. * DENY - Disable persistent cookies. Users cannot open and edit Microsoft documents stored in SharePoint. * PROMPT - Prompt users to allow or deny persistent cookies during the session. Persistent cookies are not required for clientless access if users do not connect to SharePoint. Possible values: ALLOW, DENY, PROMPT Default value: VPN_SESS_ACT_CVPN_PERSCookie_DENY

emailHome

Web address for the web-based email, such as Outlook Web Access.

allowedLoginGroups

Specify groups that have permission to log on to Access Gateway. Users who do not belong to this group or groups are denied access even if they have valid credentials.

encryptCsecExp

Enable encryption of client security expressions. Possible values: ENABLED, DISABLED
Default value: VPN_SESS_ACT_DISABLED

appTokenTimeout

The timeout value in seconds for tokens to access cloud gateway applications Default value: 100 Minimum value: 1 Maximum value: 255

mdxTokenTimeout

Validity of MDX Token in minutes. This token is used for mdx services to access backend and valid HEAD and GET request. Default value: 10 Minimum value: 1 Maximum value: 1440

UITHEME

Set VPN UI Theme to Green-Bubble, Caxton or Custom; default is Caxton. Possible values: DEFAULT, GREENBUBBLE, CUSTOM

SecureBrowse

Allow users to connect through Access Gateway to network resources from iOS and Android mobile devices with Citrix Receiver. Users do not need to establish a full VPN tunnel to access resources in the secure network. Possible values: ENABLED, DISABLED Default value: VPN_SESS_ACT_ENABLED

storefronturl

Web address for StoreFront to be used in this session for enumeration of resources from XenApp or XenDesktop.

kcdAccount

The kcd account details to be used in SSO

Example

```
set vpn parameter -httpport 80 90 -winsIP
192.168.0.220 -dnsVserverName mydns -sessTimeout
240
```

[Top](#)

unset vpn parameter**Synopsis**

```
unset vpn parameter [-httpPort] [-winsIP] [-dnsVserverName] [-splitDns] [-sessTimeout]
[-clientSecurity] [-clientSecurityGroup] [-clientSecurityMessage] [-clientSecurityLog] [-
authorizationGroup] [-clientIdleTimeout] [-allProtocolProxy | -httpProxy | -ftpProxy | -
socksProxy | -gopherProxy | -sslProxy] [-proxyException] [-forceCleanup] [-
clientOptions] [-clientConfiguration] [-loginScript] [-logoutScript] [-homePage] [-proxy]
[-wihome] [-citrixReceiverHome] [-wiPortalMode] [-iipDnsSuffix] [-forcedTimeout] [-
forcedTimeoutWarning] [-defaultAuthorizationAction] [-ntDomain] [-clientlessVpnMode]
```

[-emailHome] [-clientlessModeUrlEncoding] [-clientlessPersistentCookie] [-allowedLoginGroups] [-appTokenTimeout] [-mdxTokenTimeout] [-storefronturl] [-UITHEME] [-kcdAccount] [-splitTunnel] [-localLanAccess] [-rfc1918] [-spoofIP] [-killConnections] [-transparentInterception] [-proxyLocalBypass] [-clientCleanupPrompt] [-SSO] [-ssoCredential] [-windowsAutoLogon] [-useMIP] [-useIP] [-clientDebug] [-icaProxy] [-ClientChoices] [-encryptCsecExp] [-SecureBrowse]

Description

Removes global parameters for Access Gateway..Refer to the set vpn parameter command for meanings of the arguments.

[Top](#)

show vpn parameter

Synopsis

show vpn parameter

Description

Displays the configured Access Gateway parameters.

[Top](#)

WI Commands

This group of commands can be used to perform operations on the following entities:

- ♦ [wi site](#)
- ♦ [wi package](#)

wi site

[[add](#) | [rm](#) | [set](#) | [unset](#) | [bind](#) | [unbind](#) | [show](#)]

add wi site

Synopsis

add wi site <sitePath> [<agURL> [<staURL> [-secondSTAURL <string> [-useTwoTickets (ON | OFF)]] [-sessionReliability (ON | OFF)]] [-authenticationPoint (WebInterface | AccessGateway) [-agAuthenticationMethod (Explicit | SmartCard)]]] [-wiAuthenticationMethods (Explicit | Anonymous) ...] [-defaultCustomTextLocale <defaultCustomTextLocale>] [-webSessionTimeout <positive_integer>] [-defaultAccessMethod <defaultAccessMethod>] [-loginTitle <string>] [-appWelcomeMessage <string>] [-welcomeMessage <string>] [-footerText <string>] [-loginSysMessage <string>] [-preLoginButton <string>] [-preLoginMessage <string>] [-preLoginTitle <string>] [-domainSelection <string>] [-siteType (XenAppWeb | XenAppServices) [-ShowSearch (ON | OFF)] [-ShowRefresh (ON | OFF)] [-wiUserInterfaceModes (SIMPLE | ADVANCED)] [-UserInterfaceLayouts <UserInterfaceLayouts>]] [-userInterfaceBranding (Desktops | Applications)] [-publishedResourceType <publishedResourceType>] [-kioskMode (ON | OFF)]

Description

Creates a Web Interface site on the NetScaler appliance. The NetScaler Web Interface feature provides access to Citrix XenApp and Citrix XenDesktop applications. Users access resources through a standard web browser or by using the Citrix XenApp plug-in.

Parameters

sitePath

Path to the Web Interface site being created on the NetScaler appliance.

agURL

URL of the Access Gateway.

wiAuthenticationMethods

The method of authentication to be used at Web Interface Default value: WI_EXPLICIT

defaultCustomTextLocale

Default language for the Web Interface site. Possible values: German, English, Spanish, French, Japanese, Korean, Russian, Chinese_simplified, Chinese_traditional Default value: LANG_EN

webSessionTimeout

Time-out, in minutes, for idle Web Interface browser sessions. If a client's session is idle for a time that exceeds the time-out value, the NetScaler appliance terminates the connection. Default value: 20 Minimum value: 1 Maximum value: 1440

defaultAccessMethod

Default access method for clients accessing the Web Interface site. Note: Before you configure an access method based on the client IP address, you must enable USIP mode on the Web Interface service to make the client's IP address available with the Web Interface. Depending on whether the Web Interface site is configured to use an HTTP or HTTPS virtual server or to use access gateway, you can send clients or access gateway the IP address, or the alternate address, of a XenApp or XenDesktop server. Or, you can send the IP address translated from a mapping entry, which defines mapping of an internal address and port to an external address and port. Note: In the NetScaler command line, mapping entries can be created by using the bind wi site command. Possible values: Direct, Alternate, Translated, GatewayDirect, GatewayAlternate, GatewayTranslated

loginTitle

A custom login page title for the Web Interface site. Default value: "Welcome to Web Interface on NetScaler"

appWelcomeMessage

Specifies localized text to appear at the top of the main content area of the Applications screen. LanguageCode is en, de, es, fr, ja, or any other supported language identifier.

welcomeMessage

Localized welcome message that appears on the welcome area of the login screen.

footerText

Localized text that appears in the footer area of all pages.

loginSysMessage

Localized text that appears at the bottom of the main content area of the login screen.

preLoginButton

Localized text that appears as the name of the pre-login message confirmation button.

preLoginMessage

Localized text that appears on the pre-login message page.

preLoginTitle

Localized text that appears as the title of the pre-login message page.

domainSelection

Domain names listed on the login screen for explicit authentication.

siteType

Type of access to the Web Interface site. Available settings function as follows: * XenApp/XenDesktop web site - Configures the Web Interface site for access by a web browser. * XenApp/XenDesktop services site - Configures the Web Interface site for access by the XenApp plug-in. Possible values: XenAppWeb, XenAppServices Default value: WI_XENAPPWEB

userInterfaceBranding

Specifies whether the site is focused towards users accessing applications or desktops. Setting the parameter to Desktops changes the functionality of the site to improve the experience for XenDesktop users. Citrix recommends using this setting for any deployment that includes XenDesktop. Possible values: Desktops, Applications Default value: WI_UIBRAND_APP

publishedResourceType

Method for accessing the published XenApp and XenDesktop resources. Available settings function as follows: * Online - Allows applications to be launched on the XenApp and XenDesktop servers. * Offline - Allows streaming of applications to the client. * DualMode - Allows both online and offline modes. Possible values: Online, Offline, DualMode Default value: WI_ONLINE

kioskMode

User settings do not persist from one session to another. Possible values: ON, OFF Default value: OFF

ShowSearch

Enables search option on XenApp websites Possible values: ON, OFF Default value: OFF

ShowRefresh

Provides the Refresh button on the applications screen. Possible values: ON, OFF Default value: OFF

wiUserInterfaceModes

Appearance of the login screen. * Simple - Only the login fields for the selected authentication method are displayed. * Advanced - Displays the navigation bar, which provides access to the pre-login messages and preferences screens. Possible values: SIMPLE, ADVANCED Default value: WI_SIMPLE

UserInterfaceLayouts

Specifies whether or not to use the compact user interface. Possible values: AUTO, NORMAL, COMPACT Default value: WI_AUTO

Example

```
add wi site /Citrix/PNAgent -siteType
XenAppServices
```

[Top](#)

rm wi site**Synopsis**

```
rm wi site <sitePath>
```

Description

Removes a Web Interface site from the NetScaler appliance.

Parameters**sitePath**

Path to the Web Interface site being created on the NetScaler appliance.

Example

```
rm wi site /Citrix/PNAgent
```

[Top](#)

set wi site**Synopsis**

```
set wi site <sitePath> [-agURL <string>] [-staURL <string>] [-sessionReliability ( ON |
OFF )] [-useTwoTickets ( ON | OFF )] [-secondSTAURL <string>] [-
wiAuthenticationMethods ( Explicit | Anonymous ) ...] [-defaultAccessMethod
<defaultAccessMethod>] [-defaultCustomTextLocale <defaultCustomTextLocale>] [-
webSessionTimeout <positive_integer>] [-loginTitle <string>] [-appWelcomeMessage
<string>] [-welcomeMessage <string>] [-footerText <string>] [-loginSysMessage <string>]
[-preLoginButton <string>] [-preLoginMessage <string>] [-preLoginTitle <string>] [-
domainSelection <string>] [-userInterfaceBranding ( Desktops | Applications )] [-
authenticationPoint ( WebInterface | AccessGateway )] [-agAuthenticationMethod
( Explicit | SmartCard )] [-publishedResourceType <publishedResourceType>] [-
kioskMode ( ON | OFF )] [-ShowSearch ( ON | OFF )] [-ShowRefresh ( ON | OFF )] [-
wiUserInterfaceModes ( SIMPLE | ADVANCED )] [-UserInterfaceLayouts
<UserInterfaceLayouts>]
```

Description

Modifies the parameters of a Web Interface site configured on the NetScaler appliance.

Parameters

sitePath

Path to the Web Interface site being created on the NetScaler appliance.

agURL

URL of the Access Gateway.

staURL

URL of the Secure Ticket Authority (STA) server.

sessionReliability

Enable session reliability through Access Gateway. Possible values: ON, OFF Default value: OFF

useTwoTickets

Request tickets issued by two separate Secure Ticket Authorities (STA) when a resource is accessed. Possible values: ON, OFF Default value: OFF

secondSTAURL

URL of the second Secure Ticket Authority (STA) server.

wiAuthenticationMethods

The method of authentication to be used at Web Interface Default value: WI_EXPLICIT

defaultAccessMethod

Default access method for clients accessing the Web Interface site. Note: Before you configure an access method based on the client IP address, you must enable USIP mode on the Web Interface service to make the client's IP address available with the Web Interface. Depending on whether the Web Interface site is configured to use an HTTP or HTTPS virtual server or to use access gateway, you can send clients or access gateway the IP address, or the alternate address, of a XenApp or XenDesktop server. Or, you can send the IP address translated from a mapping entry, which defines mapping of an internal address and port to an external address and port. Note: In the NetScaler command line, mapping entries can be created by using the bind wi site command. Possible values: Direct, Alternate, Translated, GatewayDirect, GatewayAlternate, GatewayTranslated

defaultCustomTextLocale

Default language for the Web Interface site. Possible values: German, English, Spanish, French, Japanese, Korean, Russian, Chinese_simplified, Chinese_traditional Default value: LANG_EN

webSessionTimeout

Time-out, in minutes, for idle Web Interface browser sessions. If a client's session is idle for a time that exceeds the time-out value, the NetScaler appliance terminates the connection. Default value: 20 Minimum value: 1 Maximum value: 1440

loginTitle

A custom login page title for the Web Interface site. Default value: "Welcome to Web Interface on NetScaler"

appWelcomeMessage

Specifies localized text to appear at the top of the main content area of the Applications screen. LanguageCode is en, de, es, fr, ja, or any other supported language identifier.

welcomeMessage

Localized welcome message that appears on the welcome area of the login screen.

footerText

Localized text that appears in the footer area of all pages.

loginSysMessage

Localized text that appears at the bottom of the main content area of the login screen.

preLoginButton

Localized text that appears as the name of the pre-login message confirmation button.

preLoginMessage

Localized text that appears on the pre-login message page.

preLoginTitle

Localized text that appears as the title of the pre-login message page.

domainSelection

Domain names listed on the login screen for explicit authentication.

userInterfaceBranding

Specifies whether the site is focused towards users accessing applications or desktops. Setting the parameter to Desktops changes the functionality of the site to improve the experience for XenDesktop users. Citrix recommends using this setting for any deployment that includes XenDesktop. Possible values: Desktops, Applications
Default value: WI_UIBRAND_APP

authenticationPoint

Authentication point for the Web Interface site. Possible values: WebInterface, AccessGateway

agAuthenticationMethod

Method for authenticating a Web Interface site if you have specified Web Interface as the authentication point. Available settings function as follows: * Explicit - Users must provide a user name and password to log on to the Web Interface. * Anonymous - Users can log on to the Web Interface without providing a user name and password. They have access to resources published for anonymous users. Possible values: Explicit, SmartCard

publishedResourceType

Method for accessing the published XenApp and XenDesktop resources. Available settings function as follows: * Online - Allows applications to be launched on the XenApp and XenDesktop servers. * Offline - Allows streaming of applications to the

client. * DualMode - Allows both online and offline modes. Possible values: Online, Offline, DualMode Default value: WI_ONLINE

kioskMode

User settings do not persist from one session to another. Possible values: ON, OFF
Default value: OFF

ShowSearch

Enables search option on XenApp websites Possible values: ON, OFF Default value: OFF

ShowRefresh

Provides the Refresh button on the applications screen. Possible values: ON, OFF
Default value: OFF

wiUserInterfaceModes

Appearance of the login screen. * Simple - Only the login fields for the selected authentication method are displayed. * Advanced - Displays the navigation bar, which provides access to the pre-login messages and preferences screens. Possible values: SIMPLE, ADVANCED Default value: WI_SIMPLE

UserInterfaceLayouts

Specifies whether or not to use the compact user interface. Possible values: AUTO, NORMAL, COMPACT Default value: WI_AUTO

Example

```
set wi site /Citrix/PNAgent -staURL http://  
myStaServer
```

[Top](#)

unset wi site

Synopsis

unset wi site <sitePath> [-appWelcomeMessage] [-welcomeMessage] [-footerText] [-loginSysMessage] [-preLoginButton] [-preLoginMessage] [-preLoginTitle] [-userInterfaceBranding]

Description

Use this command to remove wi site settings. Refer to the set wi site command for meanings of the arguments.

[Top](#)

bind wi site

Synopsis

bind wi site <sitePath> (((<farmName> <xmlServerAddresses> [-groups <string>] [-recoveryFarm (ON | OFF)] [-xmlPort <positive_integer>] [-transport <transport> [-sslRelayPort <positive_integer>]] [-loadBalance (ON | OFF)]) | ((-accessMethod


```
<accessMethod> (-clientIpAddress <ip_addr> -clientNetMask <netmask>)) | (-
translationInternalIp <ip_addr> -translationInternalPort <port|*> -translationExternalIp
<ip_addr> -translationExternalPort <port|*> [-accessType <accessType>]))))
```

Description

Binds XenApp or XenDesktop farms to a Web Interface site and optionally, defines access methods for different client IP addresses or networks.

Parameters

sitePath

Path to the Web Interface site.

farmName

Name for the logical representation of a XenApp or XenDesktop farm to be bound to the Web Interface site. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

accessMethod

Secure access method to be applied to the IPv4 or network address of the client specified by the Client IP Address parameter. Depending on whether the Web Interface site is configured to use an HTTP or HTTPS virtual server or to use access gateway, you can send clients or access gateway the IP address, or the alternate address, of a XenApp or XenDesktop server. Or, you can send the IP address translated from a mapping entry, which defines mapping of an internal address and port to an external address and port. Possible values: Direct, Alternate, Translated, GatewayDirect, GatewayAlternate, GatewayTranslated

translationInternalIp

IP address of the server for which you want to associate an external IP address. (Clients access the server through the associated external address and port.)

Example

```
bind wi site /Citrix/XenApp Farm2 10.10.10.11
```

[Top](#)

unbind wi site

Synopsis

```
unbind wi site <sitePath> (<farmName> | ((-clientIpAddress <ip_addr> -clientNetMask
<netmask>) | (-translationInternalIp <ip_addr> -translationInternalPort <port|*> -
translationExternalIp <ip_addr> -translationExternalPort <port|*>)))
```

Description

Unbinds XenApp or XenDesktop farms from the Web Interface site and removes the existing access method definition for a client IP address or network.

Parameters

sitePath

Path to the Web Interface site.

farmName

Name of the XenApp farm to be unbound from the Web Interface site.

clientIpAddress

IPv4 address or network address of the client for which you want to remove the defined access method.

translationInternalIp

Internal IP address of a mapping entry to be removed.

Example

```
unbind wi site /Citrix/XenApp Farm2
```

[Top](#)

show wi site

Synopsis

show wi site [<sitePath>]

Description

Displays settings of all the Web Interface sites, or of a specified site. To display settings of all the Web Interface sites, run the command without any parameters.

Parameters

sitePath

Path of a Web Interface site whose details you want the NetScaler appliance to display.

Example

```
show wi site
```

[Top](#)

wi package

[[install](#) | [uninstall](#)]

install wi package

Synopsis

```
install wi package [-jre <URL>] [-wi <URL>] [-maxSites <maxSites>]
```

Description

Installs Web Interface and JRE tar files on the NetScaler appliance.

Parameters

jre

Complete path to the JRE tar file. You can use the Diablo Latte JRE version 1.6.0-7 for 64-bit FreeBSD 6.x/amd64 platform available on the FreeBSD Foundation web site. Alternatively, you can use OpenJDK6 package for FreeBSD 6.x/amd63. The Java package can be downloaded from http://ftp.riken.jp/pub/FreeBSD/ports/amd64/packages-6-stable/java/openjdk6-b17_2.tbz or <http://www.freebsdoundation.org/cgi-bin/download?download=diablo-jdk-freebsd6.amd64.1.6.0.07.02.tbz> Default value: "file:///tmp/diablo-jdk-freebsd6.amd64.1.6.0.07.02.tbz"

wi

Complete path to the Web Interface tar file for installing the Web Interface on the NetScaler appliance. This file includes Apache Tomcat Web server. The file name has the following format: nswi-<version number>.tgz (for example, nswi-1.5.tgz). Default value: "http://citrix.com/downloads/nswi-1.7.tgz"

maxSites

Maximum number of Web Interface sites that can be created on the NetScaler appliance; changes the amount of RAM reserved for Web Interface usage; changing its value results in restart of Tomcat server and invalidates any existing Web Interface sessions. Possible values: 3, 25, 50, 100, 200, 500

Example

```
install wi package -jre http://10.102.1.10/diablo-  
latte-freebsd6-amd64-1.6.0_07-b02.tar.bz2 -wi  
http://citrix.com/downloads/nswi-1.6.tgz -maxSites  
25
```

[Top](#)

uninstall wi package

Synopsis

```
uninstall wi package
```

Description

Removes the Web Interface and JRE tar files, and the entire Web Interface related configuration, from the NetScaler appliance.

Example

```
uninstall wi package
```

[Top](#)