



Send documentation comments to n5kdocfeedback@cisco.com



Cisco Nexus 5000 Series NX-OS SAN Operations Guide, Release 5.2(1)N1(1)

For Cisco Nexus 5000 Platform Switches
and Cisco Nexus 5500 Platform Switches

December 5, 2011

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-28444-01

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 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.

Cisco Nexus 5000 Series NX-OS SAN Operations Guide, Release 5.2(1)N1(1)
© 2010-2011 Cisco Systems, Inc. All rights reserved.

Send documentation comments to n5kdocfeedback@cisco.com



CONTENTS

Preface 3

Audience 3

Document Conventions 3

Related Documentation 5

Obtaining Documentation and Submitting a Service Request 5

CHAPTER 1

Using the Predefined SAN Administrator Role 1-1

Information About the Predefined SAN Administrator Role 1-1

SAN Administrator Role 1-1

Role-Feature Mapping 1-2

Examples 1-2

Configuring a User with the SAN Administrator Role 1-3

Verifying the SAN Administrator Role Configuration 1-3

Enabling the FCoE Feature for the SAN Administrator User 1-4

Modifying the SAN Administrator Default Role 1-4

Verifying the New SAN Administrator Role Configuration 1-5

Displaying the User Role Configurations 1-5

Send documentation comments to n5kdocfeedback@cisco.com



Preface

This preface describes the audience, organization, and conventions of the *Cisco Nexus 5000 Series NX-OS SAN Operations Guide, Release 5.2(1)N1(1)*. It also provides information on how to obtain related documentation.

This chapter includes the following topics:

- [Audience, page 3](#)
- [Document Conventions, page 3](#)
- [Related Documentation, page 5](#)
- [Obtaining Documentation and Submitting a Service Request, page 5](#)

Audience

This publication is for experienced network administrators who configure and maintain Cisco NX-OS on Cisco Nexus 5000 Platform switches and Cisco Nexus 5500 Platform switches.

Document Conventions

Command descriptions use the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.
<i>Italic</i>	Italic text indicates arguments for which the user supplies the values.
[x]	Square brackets enclose an optional element(keyword or argument).
[x y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.

Send documentation comments to n5kdocfeedback@cisco.com

[x {y z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
variable	Indicates a variable for which you supply values, in context where italics cannot be used.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Screen examples use the following conventions::

Convention	Description
screen font	Terminal sessions and information the switch displays are in screen font.
boldface screen font	Information you must enter is in boldface screen font.
<i>italic screen font</i>	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.



Note

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.



Caution

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Send documentation comments to n5kdocfeedback@cisco.com

Related Documentation

Documentation for Cisco Nexus 5000 Series Switches and Cisco Nexus 2000 Series Fabric Extenders is available at the following URL:

http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

Send documentation comments to n5kdocfeedback@cisco.com



CHAPTER 1

Using the Predefined SAN Administrator Role

This chapter describes how to use the predefined SAN administrator (san-admin) role on the Cisco Nexus 5000 Series devices.

This chapter includes the following sections:

- [Information About the Predefined SAN Administrator Role, page 1-1](#)
- [Examples, page 1-2](#)

Information About the Predefined SAN Administrator Role

The current Role-Based Access Control (RBAC) model in the Cisco Nexus 5000 Series device allows you to configure custom access roles that are based on rules. A rule can permit or deny access to a certain feature, interface, or command. For more information about RBAC, see the *Cisco Nexus 5000 Series NX-OS System Management Configuration Guide, Release 5.x*.

Limitations with the RBAC implementation previous to Release 5.2(1)N1(1) prompted the creation of a predefined SAN administrator role. These limitations were as follows:

- Some RBAC features that could be used for rule creation were not defined. This restriction caused the user to have to configure multiple rules for permitting or denying access to a certain feature.
- Mapping between the System Network Management Protocol (SNMP) object ID and the RBAC feature was missing for certain storage-area network (SAN) features. This restriction blocked SNMP management even if the role was configured to allow it.
- There was no role separation between LAN and SAN administrators.

To allow separation between SAN and local-area network (LAN) administrator responsibility, a new predefined SAN administrator role, called san-admin, has been created. You cannot modify this role, but you can use it to create your own custom role with custom defined rules that are appropriate for your specific organization. The RBAC model has also been enhanced and some new RBAC features have been defined to make rule creation easier.

SAN Administrator Role

The SAN administrator (san-admin) role allows a separation of SAN and LAN administrative tasks. With this role you can perform only Fibre Channel (FC) and Fibre Channel over Ethernet (FCoE) configuration tasks using SNMP or the command line interface (CLI), without impact any Ethernet capabilities.

With the san-admin role, you can do the following tasks:

Send documentation comments to n5kdocfeedback@cisco.com

- Configure all interfaces. There is no restriction to only Fibre Channel (FC) interfaces.
- Configure all attributes of FC unified ports other than creating or deleting ports
- Configure all virtual SAN (VSAN) information, including database and membership
- Map preconfigured virtual LANs (VLANs) for FCoE to VSANs
- Configure zoning
- Configure and manage the following SAN features:
 - FC-SP
 - FC-PORT-SECURITY
 - FCoE
 - FCoE-NPV
 - FPORT-CHANNEL-TRUNK
 - PORT-TRACK
 - FABRIC-BINDING
- Configure SNMP-related parameters, except SNMP community and SNMP users.
- Save the entire running configuration, including FC/FCoE, Ethernet interface, and other non-default configurations.
- View all other configurations (read-only privileges).

Role-Feature Mapping

The san-admin role has role-feature mapping capabilities that you can use to permit or deny access to that feature. The features that can be mapped are as follows:

- copy (copy-related commands)
- trapRegEntry (SNMP trap registry command)
- snmpTargetAddrEntry (SNMP trap target command)
- snmpTargetParamsEntry (SNMP trap target parameters command)
- fcfe (FC fe related commands)
- fcoe (FCoE related commands)
- trunk (FC port channel trunk related commands)
- fcmgmt (FC management related commands)
- port-track (Port-track related commands)
- port-security (FC port security related commands)
- fabric-binding (Fabric binding commands)

Examples

The examples in the following sections show you how to perform various tasks for the SAN administrator role:

- [Configuring a User with the SAN Administrator Role, page 1-3](#)

Send documentation comments to n5kdocfeedback@cisco.com

- [Verifying the SAN Administrator Role Configuration, page 1-3](#)
- [Enabling the FCoE Feature for the SAN Administrator User, page 1-4](#)
- [Modifying the SAN Administrator Default Role, page 1-4](#)
- [Verifying the New SAN Administrator Role Configuration, page 1-5](#)
- [Displaying the User Role Configurations, page 1-5](#)

Configuring a User with the SAN Administrator Role

This example shows how to create a new user-id called “mynewuser” and assign that user to the san-admin role.

```
switch# configuration terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# username mynewuser role san-admin password cisco123
switch(config)# show user-account
user:admin
    this user account has no expiry date
    roles:network-admin
user:mynewuser
    this user account has no expiry date
    roles:san-admin
```

Verifying the SAN Administrator Role Configuration

This example shows how to verify the “mynewuser” SAN administrator role. It also shows this user’s restricted command list, compared with the default command list.

```
Nexus 5000 Switch
login: mynewuser
Password:
Bad terminal type: "xterm-256color". Will assume vt100.
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2012, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
switch# ?
  clear      Reset functions
  configure  Enter configuration mode
  copy       Copy from one file to another
  debug      Debugging functions
  show       Show running system information
  end        Go to exec mode
  exit       Exit from command interpreter
```

Send documentation comments to n5kdocfeedback@cisco.com

Enabling the FCoE Feature for the SAN Administrator User

This example shows how to enable the FCoE feature for the “mynewuser” SAN administrator user. (You can enable only FC-related features for a SAN administrator user role.)

```
switch# configuration terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# feature ?
    fcoe          Enable/Disable FCoE/FC feature
    fcoe-npv      Enable/Disable FCoE NPV feature
switch(config)# feature fcoe
FC license checked out successfully
fc_plugin extracted successfully
FC plugin loaded successfully
FCoE manager enabled successfully
FC enabled on all modules successfully
Enabled FCoE QoS policies successfully
```

Modifying the SAN Administrator Default Role

The san-admin role is a predefined system-based role that cannot be modified. However, you can use it as a model to create a new SAN administrator role.

This example shows how to create a new SAN administrator role, called “newsan-admin” and modify the role to allow the following capabilities:

- Upgrade and downgrade of the Cisco NX-OS system and kickstart image.
- Configuration of the 5548UP base ports to Ethernet or native FC type. (A reload of the module is still required to change the port-type assignment.)

```
switch# configuration terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# role name newsan-admin
switch(config-role)# rule 1 permit read-write feature snmp
switch(config-role)# rule 2 permit read-write feature snmpTargetParamsEntry
switch(config-role)# rule 3 permit read-write feature snmpTargetAddrEntry
switch(config-role)# rule 4 permit read-write feature trapRegEntry
switch(config-role)# rule 5 permit read-write feature interface
switch(config-role)# rule 6 permit read-write feature fabric-binding
switch(config-role)# rule 7 permit read-write feature vsanIfvsan
switch(config-role)# rule 8 permit read-write feature vsan
switch(config-role)# rule 9 permit read-write feature wwnm
switch(config-role)# rule 10 permit read-write feature zone
switch(config-role)# rule 11 permit read-write feature span
switch(config-role)# rule 12 permit read-write feature fcns
switch(config-role)# rule 13 permit read-write feature fcsp
switch(config-role)# rule 14 permit read-write feature fdmi
switch(config-role)# rule 15 permit read-write feature fspf
switch(config-role)# rule 16 permit read-write feature rscn
switch(config-role)# rule 17 permit read-write feature rmon
switch(config-role)# rule 18 permit read-write feature copy
switch(config-role)# rule 19 permit read-write feature port-security
switch(config-role)# rule 20 permit read-write feature fcoe
switch(config-role)# rule 21 permit read-write feature port-track
switch(config-role)# rule 22 permit read-write feature fcfe
switch(config-role)# rule 23 permit read-write feature fcmgmt
switch(config-role)# rule 24 permit read-write feature trunk
switch(config-role)# rule 25 permit read-write feature rdl
switch(config-role)# rule 26 permit read-write feature fcdomain
```

Send documentation comments to n5kdocfeedback@cisco.com

```
switch(config-role)# rule 27 permit read-write feature install
switch(config-role)# rule 28 permit command configuration terminal; slot 1
switch(config-role)# rule 29 permit read
```

Verifying the New SAN Administrator Role Configuration

This example assumes that a new user was created called “newsanadmin” and it was assigned the newsan-admin role. This example shows how to verify the newsan-admin RBAC role using the newsanadmin user:

```
Nexus 5000 Switch
login: newsanadmin
Password:
Bad terminal type: "xterm-256color". Will assume vt100.
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2012, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
switch# configuration terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# slot 1
switch(config-slot)# port 16-32 type fc
switch(config-slot)# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...
switch(config-slot)# install all kickstart
bootflash:n5000-uk9-kickstart.5.2.1.N1.0.211.bin system
bootflash:n5000-uk9.5.2.1.N1.0.211.bin

Verifying image bootflash:/n5000-uk9-kickstart.5.2.1.N1.0.211.bin for boot variable
"kickstart".
[#####] 100% -- SUCCESS

Verifying image bootflash:/n5000-uk9.5.2.1.N1.0.211.bin for boot variable "system".
```

Displaying the User Role Configurations

This example shows how to display the user roles and their configurations:

```
switch# show role

Role: network-admin
Description: Predefined network admin role has access to all commands
on the switch
-----
Rule      Perm      Type      Scope      Entity
-----
1         permit   read-write

Role: network-operator
```

Send documentation comments to n5kdocfeedback@cisco.com

Description: Predefined network operator role has access to all read commands on the switch

Rule	Perm	Type	Scope	Entity
1	permit	read		

Role: vdc-admin

Description: Predefined vdc admin role has access to all commands within a VDC instance

Rule	Perm	Type	Scope	Entity
1	permit	read-write		

Role: vdc-operator

Description: Predefined vdc operator role has access to all read commands within a VDC instance

Rule	Perm	Type	Scope	Entity
1	permit	read		

Role: san-admin

Description: Predefined system role for san administrators. This role cannot be modified.

vsan policy: permit (default)

Vlan policy: permit (default)

Interface policy: permit (default)

Vrf policy: permit (default)

Rule	Perm	Type	Scope	Entity
27	permit	read		
26	permit	read-write	feature	fcdomain
25	permit	read-write	feature	rdl
24	permit	read-write	feature	trunk
23	permit	read-write	feature	fcmgmt
22	permit	read-write	feature	fcfe
21	permit	read-write	feature	port-track
20	permit	read-write	feature	fcoe
19	permit	read-write	feature	port-security
18	permit	read-write	feature	copy
17	permit	read-write	feature	rmon
16	permit	read-write	feature	rscn
15	permit	read-write	feature	fspf
14	permit	read-write	feature	fdmi
13	permit	read-write	feature	fcsp
12	permit	read-write	feature	fcns
11	permit	read-write	feature	span
10	permit	read-write	feature	zone
9	permit	read-write	feature	wwnm
8	permit	read-write	feature	vsan
7	permit	read-write	feature	vsanIfvsan
6	permit	read-write	feature	fabric-binding
5	permit	read-write	feature	interface
4	permit	read-write	feature	trapRegEntry
3	permit	read-write	feature	snmpTargetAddrEntry
2	permit	read-write	feature	snmpTargetParamsEntry
1	permit	read-write	feature	snmp

Role: priv-14

Description: This is a system defined privilege role.

vsan policy: permit (default)

Send documentation comments to n5kdocfeedback@cisco.com

```
Vlan policy: permit (default)
Interface policy: permit (default)
Vrf policy: permit (default)
```

```
-----
Rule      Perm      Type      Scope      Entity
-----
1          permit  read-write
```

Role: priv-13

```
Description: This is a system defined privilege role.
vsan policy: permit (default)
Vlan policy: permit (default)
Interface policy: permit (default)
Vrf policy: permit (default)
```

Role: priv-12

```
Description: This is a system defined privilege role.
vsan policy: permit (default)
Vlan policy: permit (default)
Interface policy: permit (default)
Vrf policy: permit (default)
```

Role: priv-11

```
Description: This is a system defined privilege role.
vsan policy: permit (default)
Vlan policy: permit (default)
Interface policy: permit (default)
Vrf policy: permit (default)
```

Role: priv-10

```
Description: This is a system defined privilege role.
vsan policy: permit (default)
Vlan policy: permit (default)
Interface policy: permit (default)
Vrf policy: permit (default)
```

Role: priv-9

```
Description: This is a system defined privilege role.
vsan policy: permit (default)
Vlan policy: permit (default)
Interface policy: permit (default)
Vrf policy: permit (default)
```

Role: priv-8

```
Description: This is a system defined privilege role.
vsan policy: permit (default)
Vlan policy: permit (default)
Interface policy: permit (default)
Vrf policy: permit (default)
```

Role: priv-7

```
Description: This is a system defined privilege role.
vsan policy: permit (default)
Vlan policy: permit (default)
Interface policy: permit (default)
Vrf policy: permit (default)
```

Role: priv-6

```
Description: This is a system defined privilege role.
vsan policy: permit (default)
Vlan policy: permit (default)
Interface policy: permit (default)
Vrf policy: permit (default)
```

Send documentation comments to n5kdocfeedback@cisco.com

```

Role: priv-5
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

```

```

Role: priv-4
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

```

```

Role: priv-3
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

```

```

Role: priv-2
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

```

```

Role: priv-1
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

```

```

Role: priv-0
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

```

Rule	Perm	Type	Scope	Entity
10	permit	command		traceroute6 *
9	permit	command		traceroute *
8	permit	command		telnet6 *
7	permit	command		telnet *
6	permit	command		ping6 *
5	permit	command		ping *
4	permit	command		ssh6 *
3	permit	command		ssh *
2	permit	command		enable *
1	permit	read		

```

Role: priv-15
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

```

Rule	Perm	Type	Scope	Entity
------	------	------	-------	--------

Send documentation comments to n5kdocfeedback@cisco.com

```
permit read-write
```

■ Examples

Send documentation comments to n5kdocfeedback@cisco.com



INDEX

A

administrator role [1-1](#)

C

configuring a user with SAN administrator role
example of [1-3](#)

D

displaying user role configurations
example of [1-5](#)

E

enabling FCoE feature for the SAN administrator role
example of [1-4](#)
examples
 configuring a user with SAN administrator role [1-3](#)
 displaying user role configurations [1-5](#)
 enabling FCoE feature for the SAN administrator role [1-4](#)
 modifying the SAN administrator default role [1-4](#)
 verifying the new SAN administrator role configuration [1-5](#)
 verifying the SAN administrator role configuration [1-3](#)

M

mapping
 features to roles [1-2](#)
modifying the SAN administrator default role

example of [1-4](#)

R

RBAC
 SAN administrator role [1-1](#)
Role-Based Access Control (RBAC)
 SAN administrator role [1-1](#)
role-feature mapping [1-2](#)

S

SAN administrator role
 description [1-1](#)
 overview [1-1](#)

V

verifying the new SAN administrator role configuration
 example of [1-5](#)
verifying the SAN administrator role configuration
 example of [1-3](#)

Send documentation comments to n5kdocfeedback@cisco.com

Send documentation comments to n5kdocfeedback@cisco.com

Send documentation comments to n5kdocfeedback@cisco.com