APPENDIX A

Active Directory Agent Command Reference

This appendix contains an alphabetical listing of commands specific to the Active Directory Agent. The commands comprise these modes:

- adactrl—Used to start, stop, and restart the AD Agent, and to monitor its running status.
- adacfg—Used to configure the Active Directory Agent with client devices, Active Directory domain controllers, and Syslog servers.

Each of the commands in this appendix is followed by a brief description of its use, command syntax, usage guidelines, and an example.

This appendix contains the following sections:

AD Agent Control Commands

This section describes the following commands:

- **adactrl help**
- **adactrl restart**
- **adactrl show running**
- **adactrl start**
- **adactrl stop**
- **adactrl version**

Note All the adactrl commands are case-sensitive.

adactrl help

To view a list of adactrl commands and their syntax.

Syntax

adactrl help

Example

```
C:\IBF\CLI>adactrl help
Cisco AD Agent adctrl -- version 1.0.0.32, build 539
    Usage: adactrl COMMAND
    where COMMAND can be:
        start        - to start the AD Agent
        stop         - to stop the AD Agent
        restart      - to restart the AD Agent
        show running - to show the running status of the AD Agent
        version      - to view info on AD Agent version currently installed
        help         - to view this help
```

adactrl restart

To stop and restart the AD Agent.

Syntax

adactrl restart

Example

```
C:\IBF\CLI>adactrl restart
OK
```

adactrl show running

To view the status of the AD Agent's internal components: radiusServer and adObserver.

Syntax

adactrl show running

Example

```
C:\IBF\CLI>adactrl show running
running C:\\IBF\\watchdog\\radiusServer.bat since 2011- 1- 5 T10:25:44
running C:\\IBF\\watchdog\\adObserver.bat since 2011- 1- 5 T10:25:44
```

adactrl start

To start the AD Agent.

Syntax

adactrl start

Example

```
C:\IBF\CLI>adactrl start
OK
```

adactrl stop

To stop the AD Agent.

Syntax

adactrl stop

Example

```
C:\IBF\CLI>adactrl stop
OK
```

adactrl version

To view the version of AD Agent that is installed on your Windows machine.

Syntax

adactrl version

Example

```
C:\IBF\CLI>adactrl version
Cisco AD Agent adactrl -- version 1.0.0.32, build 539
(Built from sources last modified 2011-04-21 12:20:17 +0300)
```

AD Agent Configuration Commands

This section describes the following commands:

- **adacfg help**
- **adacfg help client**
- **adacfg client create**
- **adacfg client erase**
- **adacfg client list**
- **adacfg client status**
- **adacfg help dc**
- **adacfg dc create**
- **adacfg dc erase**
- **adacfg dc list**
- **adacfg help cache**
- **adacfg cache list**
- **adacfg cache clear**
- **adacfg help options**
- **adacfg options list**
- **adacfg options set**

- adacfg help syslog
- adacfg syslog create
- adacfg syslog erase
- adacfg syslog list
- adacfg version

Note The adacfg commands are not case-sensitive.

adacfg help

To view the top-level summary of the **adacfg** command syntax.

Syntax

adacfg help

Example

```
C:\IBF\CLI>adacfg help
Cisco AD Agent adacfg -- version 1.0.0.32, build 539
    Usage: adacfg [COMMAND]
    where COMMAND can be:
        client       - to manage client-devices of AD Agent
        dc           - to manage AD domain-controller machines monitored by AD Agent
        syslog       - to manage syslog-targets of AD Agent
        options      - to manage configurable settings for AD Agent
        cache        - to manage cache of identity-mappings maintained by AD Agent
        version      - to view info on AD Agent version currently installed
        help         - to view this help
        help COMMAND - to view the help for specified COMMAND
```

adacfg help client

To view a detailed syntax summary of the client-related **adacfg** commands.

Syntax

adacfg help client

Example

```
C:\IBF\CLI>adacfg help client
Cisco AD Agent adacfg -- version 1.0.0.32, build 539
    Usage:  adacfg client [SUBCOMMAND] [ARGS]
    where SUBCOMMAND can be:
            create  - to configure a new client
            list    - to list all previously configured clients
            erase   - to erase a previously configured client
            status  - to view status of clients subscribed for notification
            help    - to view this help
    detailed syntax (write command on a single line!):
            adacfg client create -name <client-nickname>
                                 -ip <IP-address>[/<prefix-length-for-IP-range>]
                                 -secret <RADIUS-shared-secret>
```

```
adacfg client list
adacfg client erase -name <client-nickname>
adacfg client status
```

adacfg client create

To configure a new client device.

Syntax

adacfg client create -name <*client-nickname*> **-ip** <*IP-address*>*[/<prefix-length-for-IP-range>]* **-secret** <*RADIUS-shared-secret*>

where

- *client-nickname*—Any friendly name that you can assign to the client device.
- *IP-address*—The IP address of the client device.
- *prefix-length-for-IP-range*—You can optionally define an IP subnet range.
- *RADIUS-shared-secret*—The shared secret that the RADIUS protocol uses to communicate with the client device. This *secret* is the key that is configured on the client device.

Example

```
C:\IBF\CLI>adacfg client create -name asa1 -ip 10.77.202.1/32 -secret cisco123
Reply: Command completed successfully!
```

adacfg client erase

To erase a previously configured client.

Syntax

adacfg client erase -name <*client-nickname*>

where *client-nickname* is the name of the client device.

Example

```
C:\IBF\CLI>adacfg client erase -name asa1
Reply: Command completed successfully!
```

adacfg client list

To list all previously configured client devices.

Syntax

adacfg client list

Example

```
C:\IBF\CLI>adacfg client list
Name  IP/Range
----  ---------
asa1  10.77.204.2
asa2  10.77.101.3
asa3  10.77.101.4
```

adacfg client status

To view the sync status of the clients that are subscribed for notification (on-demand queries that also include a request for notification, or requests to register for replication).

Syntax

adacfg client status

Example

```
C:\IBF\CLI>adacfg client status
Subscribed-IP  Sync Status
-------------  ------------
10.77.101.2    In-Sync
10.77.101.3    Out-Of-Sync
10.77.101.4    Out-Of-Sync
10.77.101.5    In-Sync
```

adacfg help dc

To view a detailed syntax summary of the DC-related **adacfg** commands.

Syntax

adacfg help dc

Example

```
C:\IBF\CLI>adacfg help dc
Cisco AD Agent adacfg -- version 1.0.0.32, build 539
    Usage:  adacfg dc [SUBCOMMAND] [ARGS]
    where SUBCOMMAND can be:
            create  - to configure a new AD domain-controller machine
            list    - to list all previously configured AD domain-controller machines
            erase   - to erase a previously configured AD domain-controller machine
            help    - to view this help
    detailed syntax (write command on a single line!):
            adacfg dc create -name <DC-nickname>
                             -host <DC-hostname-or-FQDN>
                             -domain <full-DNS-name-of-AD-domain>
                             -user <username-member-of-Domain-Admins-group>
                             -password <password-of-user>
            adacfg dc list
            adacfg dc erase -name <DC-nickname>
```

adacfg dc create

To configure a new AD domain controller machine.

Syntax

adacfg dc create -name <*DC-nickname*> **-host** <*DC-hostname-or-FQDN*> **-domain** <*full-DNS-name-of-AD-domain*> **-user** <*username-member-of-Domain-Admins-group*> **-password** <*password-of-user*>

where

- *DC-nickname*—Name of the Active Directory domain controller.
- *DC-hostname-or-FQDN*—The hostname of the AD domain controller or the fully qualified domain name (FQDN) of the Active Directory domain controller.
- *full-DNS-name-of-AD-domain*—The full DNS name of the AD domain.
- *username-member-of-Domain-Admins-group*—The username of an existing account through which the security log of the domain controller machine will be monitored.

  This account must have the necessary privileges for reading the Security Log of the domain controller machine. You can easily and conveniently ensure this by specifying an account that belongs to the “Domain Admins” AD group for the domain specified with the “-domain” option.

  Alternatively, it is possible for nonmembers of the “Domain Admins” group to have the necessary privileges by satisfying all of the following requirements:

  – The account must belong to the “Distributed COM Users” AD group.

  – The account must have permission to access WMI namespaces (in particular, the “CIMV2” namespace) on the domain controller machine. You can configure this permission using the ‘wmimgmt.msc’ snap-in, or through Group Policy (to affect all domain controller machines). See http://blogs.msdn.com/b/spatdsg/archive/2007/11/21/set-wmi-namespace-security-via-gpo-script.aspx for more information.

  – The account must have permission to read the Security Event Log on the domain controller machine. You can configure this permission by setting the CustomSD key in the registry, or through the Group Policy (to affect all domain controller machines). See http://msdn.microsoft.com/en-us/library/aa363648%28v=vs.85%29.aspx for more information.
- *password-of-user*—The password corresponding to the username specified above.

Example

```
C:\IBF\CLI>adacfg dc create -name abc-dc1 -host amer.acs.com -domain acs.com -user xyz
-password axbycz
Warning: please make sure that this DC machine has:
  [1] all necessary patches installed, and
  [2] a properly configured Audit Policy.
  For more details, visit:
  http://www.cisco.com/en/US/docs/security/asa/asa84/release/notes/README_FIRST.html

Command completed successfully!
```

adacfg dc erase

To erase a previously configured AD domain controller machine.

Syntax

adacfg dc erase -name <*DC-nickname*>

Example

```
C:\IBF\CLI>adacfg dc erase -name abc-dc1
Reply: Command completed successfully!
```

adacfg dc list

To list all previously configured AD domain controller machines.

Syntax

adacfg dc list

Example

```
C:\IBF\CLI>adacfg dc list
C:\IBF\CLI>adacfg dc list
Name     Host/IP       Username     Domain-Name   Latest Status
----     -------       --------     -----------   -------------
abc-dc1  amer.acs.com  domainAdmin  ACS           up
abc-dc2  amer2.acs.com domainAdmin                down
abc-dc3  amer3.acs.com domainAdmin                down(no-retry)
```

adacfg help cache

To view a detailed syntax summary of the cache-related **adacfg** commands.

Syntax

adacfg help cache

Example

```
C:\IBF\CLI>adacfg help cache
Cisco AD Agent adacfg -- version 1.0.0.32, build 539
    Usage:  adacfg cache [SUBCOMMAND]
    where SUBCOMMAND can be:
            list  - to view the currently cached mappings
            clear - to clear the currently cached mappings
            help  - to view this help
    detailed syntax:
            adacfg cache list
            adacfg cache clear
```

adacfg cache list

To view the currently cached mappings.

Syntax

adacfg cache list

Example

```
C:\IBF\CLI>adacfg cache list
IP           User-Name Domain Response-to-Probe Mapping-Type Mapping-Origin Create-Time
--           --------- ------ ----------------- ------------ -------------- -----------
10.77.100.1  User1     AD1    true              DC           AD1  2011-01-05T09:37:17Z
10.77.100.2  User2     AD1    true              DC           AD1  2011-01-05T09:37:21Z
```

adacfg cache clear

To clear the currently cached mappings.

Syntax

adacfg cache clear

Example

```
C:\IBF\CLI>adacfg cache clear
Removed 10 records.
```

Note You must allow some time for the cache to be completely cleared internally, depending on the number of mappings that are currently cached.

A very large number of mappings in the cache can take a minute or so to be completely cleared. Meanwhile, interim invocations of the **adacfg cache list** command might appear to show that mappings still exist, or even return an SQL error that states the "database is locked," but you can safely ignore these results. Once the clear cache operation ultimately completes internally, the **adacfg cache list** command will return a "Total mappings count" of 0.

adacfg help options

To view a detailed syntax summary of the options-related **adacfg** commands.

Syntax

adacfg help options

Example

```
C:\IBF\CLI>adacfg help options
Cisco AD Agent adacfg -- version 1.0.0.32, build 539
    Usage:  adacfg options [SUBCOMMAND] [ARGS]
    where SUBCOMMAND can be:
            list - to view the current settings of the configurable options
            set  - to configure one or more of the configurable options
```

```
        help - to view this help
detailed syntax:
        adacfg options list
        adacfg options set [-<optionName> <optionValue>] [...]

      an <optionName>/<optionValue> pair can be:

        [-userLogonTTL <number-of-minutes>]
          Time duration after which logged-in user is marked as being logged-out.

        [-dcStatusTime <number-of-seconds>]
          Time span between consecutive monitorings of DC-machine up/down status.

        [-dcHistoryTime <number-of-seconds>]
          Amount of time before the present from which to start reading
          the security logs of DC-machines that are configured
          (via 'adacfg dc create') for the first time ever.

        [-notifyAttributes <text>]
          Comma-separated list of attributes to be sent in notifications to
          subscribed client-devices.

          Fully expanded list:
            domain,time-stamp,responds-to-probe,mapping-type,mapping-origin

          Wildcard equivalent to the fully expanded list:
            *

        [-logLevel <level>]
          Logging level for the customer logs (localStore and syslogs).

          Valid values: FATAL, ERROR, WARN, INFO, or DEBUG

          Default value: INFO
```

adacfg options list

To view the current settings of the configurable options.

Syntax

adacfg options list

Example

```
C:\IBF\CLI>adacfg options list
Option           Value
---------------  -----
userLogonTTL     1440
dcHistoryTime    86400
dcStatusTime     60
notifyAttributes *
logLevel         INFO
```

adacfg options set

To configure one or more of the configurable options.

Syntax

adacfg options set [-<optionName> <optionValue>] [...]

where optionName and optionValue pairs could be any or all of the following:

- **[userLogonTTL** <*number-of-minutes*>**]**—Time duration after which logged-in user is marked as being logged-out.
- **[dcStatusTime** <*number-of-seconds*>**]**—Time span between consecutive monitorings of DC-machine up/down status.
- **[dcHistoryTime** <*number-of-seconds*>**]**—Amount of time before the present from which to start reading the security logs of DC-machines that are configured (via 'adacfg dc create') for the first time ever.
- **[notifyAttributes** <*text*>**]**—Comma-separated list of attributes to be sent in notifications to subscribed client-devices, which could be any or all of the following attributes:
  - **domain, time-stamp, responds-to-probe, mapping-type, mapping-origin**
  - ***** (wildcard equivalent of all the attributes)
- **[logLevel** <*level*>**]**—Logging level for the customer logs (localStore and syslogs). Valid values include FATAL, ERROR, WARN, INFO, and DEBUG. The default level is INFO.

Note The AD Agent generates some of its Customer Log messages using the “NOTICE” logging level (which falls between the “INFO” and “WARN” levels), but you cannot explicitly choose “NOTICE” as a setting for ‘logLevel’ using the **adacfg options set -logLevel** command. See Appendix B, “Customer Log Messages,” for more details.

adacfg help syslog

To view a detailed syntax summary of the syslog-related **adacfg** commands.

Syntax

adacfg help syslog

Example

```
C:\IBF\CLI>adacfg help syslog

Cisco AD Agent adacfg -- version 1.0.0.32, build 539
    Usage:  adacfg syslog [SUBCOMMAND] [ARGS]
    where SUBCOMMAND can be:
            create  - to configure a new syslog-target
            list    - to list all previously configured syslog-targets
            erase   - to erase a previously configured syslog-target
            help    - to view this help
    detailed syntax (write command on a single line!):
            adacfg syslog create -name <syslog-target-nickname>
                                 -ip <IP-address>
                                [-facility <syslog-facility>]
              valid syslog facility values:  LOCAL0 - LOCAL7
              default syslog facility value: LOCAL6
```

```
adacfg syslog list
adacfg syslog erase -name <syslog-target-nickname>
```

adacfg syslog create

To configure a new syslog target.

Syntax

adacfg syslog create -name <*syslog-target-nickname*> **-ip** <*IP-address*> [**-facility** <*syslog-facility*>]

where

- *syslog-target-nickname*—Name of the syslog server.
- *IP-address*—IP address of the syslog server.
- *syslog-facility*—Facility values range from LOCAL0 to LOCAL7. The default is LOCAL6.

Example

```
C:\IBF\CLI>adacfg syslog create -name mysyslog -ip 10.77.202.1 -facility LOCAL6
Reply: Command completed successfully!
```

adacfg syslog erase

To erase a previously configured syslog target.

Syntax

adacfg syslog erase -name <*syslog-target-nickname*>

where *syslog-target-nickname* is the name of the syslog target connected to the AD Agent.

Example

```
C:\IBF\CLI>adacfg syslog erase -name mysyslog
Reply: Command completed successfully.
```

adacfg syslog list

To list all the previously configured syslog targets.

Syntax

adacfg syslog list

Example

```
C:\IBF\CLI>adacfg syslog list
Name      IP           Facility
-----     ---          ---------
mysyslog  10.77.202.4  LOCAL6
```

adacfg version

To view the version of the AD Agent installed on your Windows machine.

Syntax

adacfg version

Example

```
C:\IBF\CLI>adacfg version
Cisco AD Agent adacfg -- version 1.0.0.32, build 539
<Built from sources last modified 2011-04-21 12:20:17 +0300>
```