Command Reference

This appendix contains necessary information on disk space management for all types of deployments and an alphabetical listing of the commands specific to the . The comprise the following modes:

- EXEC
    - System-level
    - Show
- Configuration
    - configuration submode

      Use EXEC mode system-level **config** or **configure** command to access configuration mode.

Each of the commands in this appendix is followed by a brief description of its use, command syntax, any command defaults, command modes, usage guidelines, and one or more examples. Throughout this appendix, the server uses the name *ncs* in place of the server's hostname.

Note If an error occurs in any command usage, use the **debug** command to determine the cause of the error.

EXEC Commands

This section lists each EXEC command and each command page includes a brief description of its use, command syntax, any command defaults, command modes, usage guidelines, and an example of the command and any related commands.

application start

To start the application process, use the **application start** command in EXEC mode. There is **no** form of this command.

Note This command does not work in FIPS release.

application start *application-name*

Syntax Description

application-name	Name of the predefined application that you want to enable. Up to 255 alphanumeric characters.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Enables an application.

You cannot use this command to start the application. If you use this command to start the application, you can see that the is already running.

Examples

```
pi-system-117/admin# application start ncs
% Application failed to start
pi-system-117/admin#
```

Related Commands

Command	Description
application stop	Stops or disables an application.
application upgrade	Upgrades an application bundle.
show application	Shows application information for the installed application packages on the system.

application stop

To stop the PI process, use the **application stop** command in EXEC mode. There is no **No** form of this command.

Note This command does not work in FIPS release.

application stop *application-name*

Syntax Description

application-name	Name of the predefined application that you want to disable. Up to 255 alphanumeric characters.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Disables an application.

Examples

```
pi-system-117/admin# application stop ncs
% Application failed to stop
pi-system-117/admin#
```

Related Commands

	Description
application start	Starts or enables an application.
application upgrade	Upgrades an application bundle.
show application	Shows application information for the installed application packages on the system.

application upgrade

To upgrade lower version to higher version (supported version), use the **application upgrade** command in EXEC mode.

application upgrade *application-bundle repository-name*

Syntax Description

application-bundle	Enter the upgrade bundle name.
remote-repository-name	Remote repository name (up to 80 alphanumeric characters).

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Upgrades an application bundle, and preserves any application configuration data.

If you enter the **application upgrade** command when another application upgrade operation is in progress, you will see the following warning message:

```
An existing application install, remove, or upgrade is in progress. Try again shortly.
```

Caution Do not enter the **backup** or **restore** commands when the upgrade is in progress. This action might cause the database to be corrupted.

Related Commands

Command	Description
application start	Starts or enables an application.
application stop	Stops or disables an application.
show application	Shows application information for the installed application packages on the system.

backup

Appliance Backup: To perform a backup (including the and Cisco ADE OS data) and place the backup in a repository, use the **backup** command in EXEC mode.

Application Backup: To perform a backup of only the application data without the Cisco ADE OS data, use the **application** keyword command.

Command for Appliance Backup:

backup *backup-name* **repository** *repository-name*

Command for Application Backup

backup *backup-name* **repository** *repository-name* **application** *application-name*

Syntax Description

backup-name	Name of the backup file. Up to 26 alphanumeric characters is recommended.
repository-name	Name of the location where the files should be backed up to. Up to 80 alphanumeric characters.
application-name	Application name. Up to 255 alphanumeric characters. **Note** Enter the application name as 'NCS' in uppercase.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Performs a backup of the and Cisco ADE OS data and places the backup in a repository.

To perform a backup of only the application data without the Cisco ADE OS data, use the **application** command.

Examples

```
pi-system-117/admin# backup MySysBkp repository defaultRepo

DO NOT press ^C while the backup is in progress
Aborting backup with a ^C may terminate the backup operation or the backup file may \
be corrupted

To restore this backup you will have to enter this password

Password :
Password Again :
  Backup Started at : 02/28/18 00:48:51
  Stage 1 of 7: Database backup ...
  Database size: 16G
  -- completed at  02/28/18 00:50:12
  Stage 2 of 7: Database copy ...
  -- completed at  02/28/18 00:50:12
  Stage 3 of 7: Backing up support files ...
  -- completed at  02/28/18 00:50:12
  Stage 4 of 7: Compressing Backup ...
  -- completed at  02/28/18 00:50:17
  Stage 5 of 7: Building backup file ...
  -- completed at  02/28/18 00:50:54
  Stage 6 of 7: Encrypting backup file ...
  -- completed at  02/28/18 00:51:04
  Stage 7 of 7: Transferring backup file ...
  -- completed at 02/28/18 00:51:06
% Backup file created is:                                                           \
MySysBkp-180228-0048__VER3.2.50.0.70_BKSZ13G_FIPS_ON_CPU20_MEM16G_RAM62G_SWAP15G_SYS\
_CK1677401767.tar.gpg
  Total Backup duration is: 0h:2m:15s
pi-system-117/admin#
pi-system-117/admin# backup MyApplicationBkp repository defaultRepo application NCS

DO NOT press ^C while the backup is in progress
Aborting backup with a ^C may terminate the backup operation or the backup file may \
be corrupted

To restore this backup you will have to enter this password

Password :
Password Again :
  Backup Started at : 02/28/18 00:52:37
  Stage 1 of 7: Database backup ...
  Database size: 16G
  -- completed at  02/28/18 00:53:45
  Stage 2 of 7: Database copy ...
  -- completed at  02/28/18 00:53:45
  Stage 3 of 7: Backing up support files ...
  -- completed at  02/28/18 00:53:45
  Stage 4 of 7: Compressing Backup ...
  -- completed at  02/28/18 00:53:50
  Stage 5 of 7: Building backup file ...
  -- completed at  02/28/18 00:54:25
  Stage 6 of 7: Encrypting backup file ...
  -- completed at  02/28/18 00:54:35
  Stage 7 of 7: Transferring backup file ...
  -- completed at 02/28/18 00:54:38
% Backup file created is:                                                           \
MyApplicationBkp-180228-0052__VER3.2.50.0.70_BKSZ13G_FIPS_ON_CPU20_MEM16G_RAM62G_SWA\
P15G_APP_CK4137329745.tar.gpg
  Total Backup duration is: 0h:2m:1s
pi-system-117/admin#
```

Related Commands

Command	Description
delete	Deletes a file from the server.
repository	Enters the repository submode for configuration of backups.
restore	Restores from backup the file contents of a specific repository.
show backup history	Displays the backup history of the system.
show repository	Displays the available backup files located on a specific repository.

backup-logs

To back up system logs, use the **backup-logs** command in EXEC mode. There is no **no** form of this command.

backup-logs *backup-name* **repository** *repository-name*

Syntax Description

backup-name	Name of one or more files to back up. Up to 100 alphanumeric characters.
repository-name	Location where files should be backed up to. Up to 80 alphanumeric characters.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Backs up system logs.

Examples

```
pi-admin/admin# backup-logs log-backup repository defaultRepo
% Creating log backup with timestamped filename: log-backup-150621-1618.tar.gz
  Transferring file ...
  -- complete.
pi-system/admin#
```

Related Commands

Command	Description
repository	Enters the repository submode for configuration of backups.
show repository	Shows the available backup files located on a specific repository.

banner

To set up messages while logging (pre-login) in to CLI, use the **banner install pre-login** command.

banner install pre-login *banner-text-filename* **repository** *Repository-name*

Syntax Description

banner-text-filename	Banner text file name.
repository-name	Repository name.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

```
admin#  banner install pre-login test.txt repository defaultRepo
```

Related Commands

Command	Description
show banner pre-login, on page 120	Enables you to display a pre-login banner.

clock

To set the system clock, use the **clock** command in EXEC mode. You cannot remove this function but reset the clock.

clock set *[mmm dd hh:mm:ss yyyy]*

Syntax Description

mmm	Current month of the year by name. Up to three alphabetic characters. For example, Jan for January.
dd	Current day (by date) of the month. Value = 0 to 31. Up to two numbers.
hh:mm:ss	Current time in hours (24-hour format), minutes, and seconds.
yyyy	Current year (no abbreviation).

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Sets the system clock. You must restart the server after you reset the clock for the change to take effect.

Examples

```
pi-system/admin# clock set nov 16 18:00:00 2017
pi-system-81/admin# show clock
Thu Nov 16 18:00:05 IST 2017
pi-system/admin#
```

Related Commands

Command	Description
show clock	Displays the time and date set on the system software clock.

configure

To enter configuration mode, use the **configure** command in EXEC mode. If the **replace** option is used with this command, copies a remote configuration to the system which overwrites the existing configuration.

configure terminal

Syntax Description

terminal	Executes configuration commands from the terminal.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Use this command to enter configuration mode. Note that commands in this mode write to the running configuration file as soon as you enter them (press **Enter**).

To exit configuration mode and return to EXEC mode, enter **end**, **exit**, or press**Ctrl-z**.

To view the changes that you have made to the configuration, use the **show running-config** command in EXEC mode.

Examples

```
ncs/admin# configure
Enter configuration commands, one per line.  End with CNTL/Z.
ncs/admin(config)#

ncs/admin# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ncs/admin(config)#
```

Related Commands

Command	Description
show running-config	Displays the contents of the currently running configuration file or the configuration.
show startup-config	Displays the contents of the startup configuration file or the configuration.

copy

To copy any file from a source to a destination, use the **copy** command in EXEC mode.

Syntax Description

running-config	Represents the current running configuration file.
startup-config	Represents the configuration file used during initialization (startup).
protocol	See Table 1: Protocol Prefix Keywords for protocol keyword options.
hostname	Hostname of destination.
location	Location of disk:/<dirpath>.
logs	The system log files.
all	Copies all log files from the system to another location. All logs are packaged as ncslogs.tar.gz and transferred to the specified directory on the remote host.
filename	Allows you to copy a single log file and transfer it to the specified directory on the remote host, with its original name.
log_filename	Name of the log file, as displayed by the **show logs** command (up to 255 characters).
mgmt	Copies the management debug logs and Tomcat logs from the system, bundles them as mgmtlogs.tar.gz, and transfers them to the specified directory on the remote host.
runtime	Copies the runtime debug logs from the system, bundles them as runtimelogs.tar.gz, and transfers them to the specified directory on the remote host.

Command Default

No default behavior or values.

Command Modes

EXEC

The fundamental function of the **copy** command allows you to copy a file (such as a system image or configuration file) from one location to another location. The source and destination for the file specified uses the file system, through which you can specify any supported local or remote file location. The file system being used (a local memory source or a remote system) dictates the syntax used in the command.

You can enter on the command line all of the necessary source and destination information and the username and password to use; or, you can enter the **copy** command and have the server prompt you for any missing information. You can enter up to a maximum of 2048 characters of source and destination URL information on the command line.

The **copy** command in the copies a configuration (running or startup).

The active configuration stores itself in the RAM. Every configuration command you enter resides in the running configuration. If you reboot your server, you lose the running configuration. If you make changes that you want to save, you must copy the running configuration to a safe location, such as a network server, or save it as the server startup configuration.

You cannot edit a startup configuration directly. All commands that you enter store themselves in the running configuration, which you can copy into the startup configuration.

In other words, when you boot a server, the startup configuration becomes the initial running configuration. As you modify the configuration, the two diverge: the startup configuration remains the same; the running configuration reflects the changes that you have made. If you want to make your changes permanent, you must save the running configuration to the startup configuration using the **write memory** command. The **write memory** command makes the current running configuration permanent.

Note If you do not save the running configuration, you will lose all your configuration changes during the next reboot of the server. You can also save a copy of the running and startup configurations using the following commands, to recover in case of loss of configuration:

copy startup-config *location*

copy running-config *location*

Note The **copy** command is supported only for the local disk and not for a repository.

Tip Aliases reduce the amount of typing that you need to do. For example, type **copy run start** (the abbreviated form of the **copy running-config startup-config** command).

The entire copying process might take several minutes and differs from protocol to protocol and from network to network.

Use the filename relative to the directory for file transfers.

Possible error is the standard FTP error message.

Table 1: Protocol Prefix Keywords

Keyword	Destination
ftp	URL for FTP network server. The syntax for this alias: **ftp:**//*location*/*directory*

Keyword	Destination
sftp	URL for an SFTP network server. The syntax for this alias: sftp://location/directory SFTP Repositories may require the // between the IP address/FQDN and the physical path on the SFTP store. If you find that you cannot access the SFTP repository with single slashes, add the additional slash and try the operation again. For example: url sftp://server//path **Note** The remote sftp servers need to be enabled for 'password authentication' (keyboard-interactive mode does not work for sftp transfers). See the documentation on sshd server used at the remote end, to enable password authentication. Depending on the SFTP software used with the remote server, you may need to enable "password authentication" instead of "keyboard-interactive mode". Enabling "password authentication" is required; copy to remote SFTP servers will not work unless it is enabled. For example: With OpenSSH 6.6x, "keyboard-interactive mode" is the default. To enable "password authentication", edit the OpenSSH sshd_config file to set the PasswordAuthentication parameter to "yes", as follows: PasswordAuthentication yes.
tftp	URL for a TFTP network server. The syntax for this alias: **tftp:**//*location*/*directory*

Examples

```
ncs/admin# copy run start
Generating configuration...
ncs/admin#

ncs/admin# copy running-config startup-config
Generating configuration...
ncs/admin#

ncs/admin# copy start run
ncs/admin#

ncs/admin# copy startup-config running-config
ncs/admin#

ncs/admin# copy logs disk:/
 Collecting logs...
ncs/admin#
```

This command is used to copy the certificate from ftp tp pnp.

```
copy tftp://<PI Server IP Address>/server.key disk:/
copy tftp://<PI Server IP Address>/server.crt disk:/
 copy tftp://<PI Server IP Address>/ncs_server_certificate.crt disk:/
```

Related Commands

Command	Description
delete	Deletes a file from the server.
dir	Lists a file from the server.

debug

To display errors or events for command situations, use the **debug** command in EXEC mode.

debug{all | application | backup-restore | cdp | config | icmp | copy | locks | logging | snmp | system | transfer | user | utils}

Syntax Description

all	Enables all debugging.
application	Application files. • *all*—Enables all application debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • *install*—Enables application install debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • *operation*—Enables application operation debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • *uninstall*—Enables application uninstall debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
backup-restore	Backs up and restores files. • *all*—Enables all debug output for backup-restore. Set level between 0 and 7, with 0 being severe and 7 being all. • *backup*—Enables backup debug output for backup-restore. Set level between 0 and 7, with 0 being severe and 7 being all. • *backup-logs*—Enables backup-logs debug output for backup-restore. Set level between 0 and 7, with 0 being severe and 7 being all. • *history*—Enables history debug output for backup-restore. Set level between 0 and 7, with 0 being severe and 7 being all. • *restore*—Enables restore debug output for backup-restore. Set level between 0 and 7, with 0 being severe and 7 being all.
cdp	Cisco Discovery Protocol configuration files. • *all*—Enables all Cisco Discovery Protocol configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • *config*—Enables configuration debug output for Cisco Discovery Protocol. Set level between 0 and 7, with 0 being severe and 7 being all. • *infra*—Enables infrastructure debug output for Cisco Discovery Protocol. Set level between 0 and 7, with 0 being severe and 7 being all.

config	Configuration files. • *all*—Enables all configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • *backup*—Enables backup configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • *clock*—Enables clock configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • *infra*—Enables configuration infrastructure debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • *kron*—Enables command scheduler configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • *network*—Enables network configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • *repository*—Enables repository configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • *service*—Enables service configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
icmp	Internet Control Message Protocol (ICMP) echo response configuration. *all*—Enable all debug output for ICMP echo response configuration. Set level between 0 and 7, with 0 being severe and 7 being all.
copy	Copy commands. Set level between 0 and 7, with 0 being severe and 7 being all.
locks	Resource locking. • *all*—Enables all resource locking debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • *file*—Enables file locking debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
logging	Logging configuration files. *all*—Enables all logging configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
snmp	SNMP configuration files. *all*—Enables all SNMP configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.

system	System files. • *all*—Enables all system files debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • *id*—Enables system ID debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • *info*—Enables system info debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • *init*—Enables system init debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
transfer	File transfer. Set level between 0 and 7, with 0 being severe and 7 being all.
user	User management. • *all*—Enables all user management debug output. Set level between 0 and 7, with 0 being severe and 7 being all. • *password-policy*—Enables user management debug output for password-policy. Set level between 0 and 7, with 0 being severe and 7 being all.
utils	Utilities configuration files. *all*—Enables all utilities configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Use the **debug** command to identify various failures within the server; for example, setup failures or configuration failures.

Examples

```
ncs/admin# debug all
ncs/admin# mkdir disk:/1
ncs/admin# 6 [15347]: utils: vsh_root_stubs.c[2742] [admin]: mkdir operation success

ncs/admin# rmdir disk:/1
6 [15351]: utils: vsh_root_stubs.c[2601] [admin]: Invoked Remove Directory disk:/1 command
6 [15351]: utils: vsh_root_stubs.c[2663] [admin]: Remove Directory operation success
ncs/admin#

ncs/admin# undebug all
ncs/admin#
```

Related Commands

Command	Description
undebug	Disables the output (display of errors or events) of the **debug** command for various command situations.

delete

To delete a file from the server, use the **delete** command in EXEC mode. There is no **no** form of this command.

delete *filename [disk:/path]*

Syntax Description

filename	Filename.
disk:/path	Location.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

If you attempt to delete the configuration file or image, the system prompts you to confirm the deletion. Also, if you attempt to delete the last valid system image, the system prompts you to confirm the deletion.

Examples

```
ncs/admin# delete disk:/hs_err_pid19962.log
ncs/admin#
```

Related Commands

Command	Description
dir	Lists all of the files on the server.

dir

To list a file from the server, use the **dir** command in EXEC mode. To remove this function, use the **no** form of this command.

dir *[word]***[recursive]**

Syntax Description

word	Directory name. Up to 80 alphanumeric characters. Requires **disk:/** preceding the directory name.
recursive	Lists a local directory or filename recursively.

Command Default

No default behavior or values.

Command Modes

EXEC

Related Commands

Command	Description
delete	Deletes a file from the server.

exit

To close an active terminal session by logging out of the server or to move up one mode level from configuration mode, use the **exit** command in EXEC mode.

exit

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Use the **exit** command in EXEC mode to exit an active session (log out of the server) or to move up from configuration mode.

Examples

```
ncs/admin# exit
```

Related Commands

Command	Description
end	Exits configuration mode.
exit	Exits configuration mode or EXEC mode.
Ctrl-z	Exits configuration mode.

forceout

To force users out of an active terminal session by logging them out of the server, use the **forceout** command in EXEC mode.

forceout *username*

Syntax Description

username	The name of the user. Up to 31 alphanumeric characters.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

```
ncs/admin# forceout user1
ncs/admin#
```

halt

To shut down and power off the system, use the **halt** command in EXEC mode.

halt

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Before you enter the **halt** command, ensure that the is not performing any backup, restore, installation, upgrade, or remove operation. If you enter the **halt** command while the is performing any of these operations, you will get one of the following warning messages:

```
WARNING: A backup or restore is currently in progress! Continue with halt?
```

```
WARNING: An install/upgrade/remove is currently in progress! Continue with halt?
```

If you get any of these warnings, enter **YEs** to halt the operation, or enter **NO** to cancel the halt.

If no processes are running when you use the **halt** command or if you enter **Yes** in response to the warning message displayed, the asks you to respond to the following option:

```
Do you want to save the current configuration ?
```

Enter YES to save the existing configuration. The displays the following message:

```
Saved the running configuration to startup successfully
```

Examples

```
pi-system/admin# halt
Save the current ADE-OS running configuration? (yes/no) [yes] ? yes
Generating configuration...
Saved the ADE-OS running configuration to startup successfully
Continue with shutdown? [y/n] y
Broadcast message from root (pts/0) (Wed May  5 18:37:02 2010):
The system is going down for system halt NOW!
Server is shutting down...
```

Related Commands

Command	Description
reload	Reboots the system.

lms

To migrate data from lms server to PI server, use **lms** command in EXEC mode.

lms migrate repository *repository-name*

Syntax Description

repository-name	Name of the PI repository.

Command Default

No default values or behaviour.

Command Modes

EXEC

Examples

```
pi-system-117/admin# lms migrate repository test
Repository name : test
 ERROR: Restore is not supported in FIPS enabled server.
INFO: LMS Migration will not proceed with FIPS enabled Server.
pi-system-117/admin#
```

mkdir

To create a new directory on the server, use the **mkdir** command in EXEC mode.

mkdir *directory-name [disk:/path]*

Syntax Description

directory-name	The name of the directory to create. Up to 80 alphanumeric characters.
disk:/path	Use *disk:/path* with the directory name.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Use *disk***:/***path* with the directory name; otherwise, an error appears that indicates that the *disk***:/***path* must be included.

Examples

```
ncs/admin# mkdir disk:/test
ncs/admin# dir

Directory of disk:/

       4096 May 06 2010 13:34:49  activemq-data/
       4096 May 06 2010 13:40:59  logs/
      16384 Mar 01 2010 16:07:27  lost+found/
       4096 May 06 2010 13:42:53  target/
       4096 May 07 2010 12:26:04  test/

           Usage for disk: filesystem
                  181067776 bytes total used
                19084521472 bytes free
                20314165248 bytes available
ncs/admin#
```

Related Commands

Command	Description
dir	Displays a list of files on the server.
rmdir	Removes an existing directory.

ncs run client-auth

You can enable client certificate authentication on your Prime Infrastructure application using **ncs run client-auth** command.

ncs run client-auth enable

ncs run client-auth disable

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

```
pi-system-117/admin# ncs run client-auth enable

WARNING :

This feature requires the CA certificate to be installed on the system.
Please use the command 'ncs key importcacert ..." to
import the certificate of the CA used to sign the client certificates.
Ignore this warning if the CA certificate is already installed.

Use the 'disable' option of this command, to disable client authentication,
if not required.

client_auth status : enabled
pi-system-117/admin#

pi-system-117/admin# ncs run client-auth disable
client_auth status : disabled
pi-system-117/admin#
```

ncs run list

To display the list of commands associated with NCS, use **ncs run list** command in EXEC mode.

ncs run list

Command Default

No default behavior or arguments

Command Modes

EXEC

Examples

```
pi-system-61/admin# ncs run list
commands :
list - prints this list

test iops - tests the disk write performance
reset [db|keys] - reset database and keys to default factory settings

csrf [disable|enable] - enable or disable CSRF protection
client-auth [disable|enable] - enable or disable client certificate based authentication
jms [disable|enable] - enable or disable message bus connectivity (port 61617)

sshclient-nonfips-ciphers [disable|enable] - enable or disable non fips compliant ciphers
for outgoing ssh client connections to devices
ssh-server-dh1key [disable|enable] - enable or disable DH group1 for SSH service.
tls-server-versions <tls_versions> - set the TLS versions to be enabled for TLS service -
TLSv1.2 TLSv1.1 TLSv1
tls-server-ciphers <tls_cipher_groups> - set the TLS cipher group to be enabled for TLS
service - tls-ecdhe tls-dhe tls-static ssl-static

livelogs [all|secure|ade|messages] - view live audit logs
loghistory [all|secure|ade|messages] - view audit logs
```

ncs run test iops

To test and view details of the input output operations on your Prime Infrastructure, use **ncs run test iops** command in EXEC mode.

ncs run test iops

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

```
pi-242/admin# ncs run test iops
Testing disk write speed ...
8388608+0 records in
8388608+0 records out
8589934592 bytes (8.6 GB) copied, 33.4561 s, 257 MB/s
```

ncs run reset

You can use **ncs run reset** command to delete all private keys from your Prime Infrastructure server and to clean a corrupted Database. Resetting the DB clears all existing data and replaces it with empty data.

ncs run reset { db | keys }

Syntax Description

db	Resets DB wth empty data.
keys	Deletes all private keys from Prime Infrastructure server.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

```
pi-system-61/admin# ncs run reset db
```

Examples

This example shows how to delete all private keys in server:

```
pi-system-61/admin# ncs run reset keys
This will delete all the private keys and may impact webserver, SSH service etc.
Do you want to proceed [yes/no] [no]? yes
```

ncs run csrf

The cross-site request forgery check can be disabled (not recommended). The CLI provided only for backward compatibility with API clients which are not programmed for CSRF protection. For CSRF protection, this option should be enabled using the following command.

ncs run csrf enable

To disable, use the following command:

ncs run csrf disable

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

```
pi-cluster-93/admin# ncs run csrf enable
```

```
pi-cluster-93/admin# ncs run csrf disable
```

ncs run livelogs

You can run **ncs run livelogs** command to view live audit logs.

ncs run livelogs { *all* **|** *secure* **|** *ade* **|** *messages* **}**

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

```
pi-system-120/admin# ncs run livelogs
***Available filter options to limit logs - all  secure ade messages***
************Press Ctrl+C for stop logging*****************
2018-02-28T01:48:39.407787+05:30 pi-system-120 sshd[10309]: pam_unix(sshd:session): \
session closed for user admin
2018-02-28T01:50:14.109435+05:30 pi-system-120 sshd[32038]:                          \
pam_tally2(sshd:account): option unlock_time=60 allowed in auth phase only
2018-02-28T01:50:14.109456+05:30 pi-system-120 sshd[32038]:                          \
pam_tally2(sshd:account): unknown option: no_reset
2018-02-28T01:50:14.112152+05:30 pi-system-120 sshd[32038]: pam_unix(sshd:session): \
session opened for user admin by (uid=0)
2018-02-28T02:00:57.499844+05:30 pi-system-120 sshd[32038]: pam_unix(sshd:session): \
session closed for user admin
2018-02-28T02:04:28.870085+05:30 pi-system-120 su: pam_unix(su:session): session    \
opened for user oracle by (uid=0)
2018-02-28T02:04:28.976462+05:30 pi-system-120 su: pam_unix(su:session): session    \
closed for user oracle
2018-02-28T02:21:30.485537+05:30 pi-system-120 sshd[6381]:                           \
pam_tally2(sshd:account): option unlock_time=60 allowed in auth phase only
2018-02-28T02:21:30.485556+05:30 pi-system-120 sshd[6381]:                           \
pam_tally2(sshd:account): unknown option: no_reset
2018-02-28T02:21:30.488589+05:30 pi-system-120 sshd[6381]: pam_unix(sshd:session):  \
session opened for user admin by (uid=0)

2018-02-28T02:25:04.370446+05:30 pi-system-120 debugd[3229]: [7471]:                 \
config:network: sysconfig.c[1116] [admin]: Getting ipaddress for eth1
2018-02-28T02:25:04.377607+05:30 pi-system-120 debugd[3229]: [7471]:                 \
config:network: syscfg_cli.c[1098] [admin]: No ipaddress for interface eth1
2018-02-28T02:25:04.384642+05:30 pi-system-120 ADEOSShell[7471]: Change Audit        \
Details:SUCCESS:CARS                                                                 \
CLI:carsGetIfState::root:/opt/system/bin/carssh:NotFromTerminal:5:
2018-02-28T02:25:04.384720+05:30 pi-system-120 debugd[3229]: [7471]:                 \
config:network: syscfg_cli.c[1105] [admin]: Interface eth1 is down
2018-02-28T02:25:04.384777+05:30 pi-system-120 debugd[3229]: [7471]:                 \
config:network: syscfg_cli.c[1011] [admin]: Getting dhcpv6 enabled for eth1
2018-02-28T02:25:04.405866+05:30 pi-system-120 ADEOSShell[7471]: Change Audit        \
Details:SUCCESS:CARS                                                                 \
CLI:carsGetNameserver::root:/opt/system/bin/carssh:NotFromTerminal:6:
2018-02-28T02:25:04.412912+05:30 pi-system-120 ADEOSShell[7471]: Change Audit        \
Details:SUCCESS:CARS                                                                 \
CLI:carsGetNameserver::root:/opt/system/bin/carssh:NotFromTerminal:7:
2018-02-28T02:25:04.420049+05:30 pi-system-120 ADEOSShell[7471]: Change Audit        \
Details:SUCCESS:CARS                                                                 \
CLI:carsGetNameserver::root:/opt/system/bin/carssh:NotFromTerminal:8:
2018-02-28T02:25:04.427224+05:30 pi-system-120 ADEOSShell[7471]: Change Audit        \
Details:SUCCESS:CARS                                                                 \
CLI:carsGetGateway::root:/opt/system/bin/carssh:NotFromTerminal:9:
2018-02-28T02:28:16.411167+05:30 pi-system-120 ADEOSShell[8312]: Change Audit        \
Details:SUCCESS:CARS CLI:run_command::root:/opt/system/bin/carssh:/dev/pts/1:1:

2018-02-28T02:21:25.649026+05:30 pi-system-120 sshd[6381]: Operating in CiscoSSL     \
Common Criteria mode
2018-02-28T02:21:25.654950+05:30 pi-system-120 sshd[6381]: FIPS mode initialized
2018-02-28T02:21:25.806409+05:30 pi-system-120 sshd[6381]: Outbound-ReKey for        \
10.77.144.125:16285 [preauth]
2018-02-28T02:21:25.889051+05:30 pi-system-120 sshd[6381]: Inbound-ReKey for         \
10.77.144.125:16285 [preauth]
2018-02-28T02:21:30.487757+05:30 pi-system-120 sshd[6381]: Accepted password for     \
admin from 10.77.144.125 port 16285 ssh2
2018-02-28T02:21:30.490420+05:30 pi-system-120 sshd[6390]: Inbound-ReKey for         \
10.77.144.125:16285
2018-02-28T02:21:30.490437+05:30 pi-system-120 sshd[6390]: Outbound-ReKey for        \
10.77.144.125:16285
2018-02-28T02:21:32.124237+05:30 pi-system-120 rsyslogd: [origin                      \
software="rsyslogd" swVersion="5.8.10" x-pid="3216"                                   \
x-info="http://www.rsyslog.com ] rsyslogd was HUPed
2018-02-28T02:25:04.601075+05:30 pi-system-120 rsyslogd-2177: imuxsock begins to      \
drop messages from pid 3229 due to rate-limiting
2018-02-28T02:25:30.938945+05:30 pi-system-120 rsyslogd-2177: imuxsock lost 463       \
messages from pid 3229 due to rate-limiting
^CERROR: cmd '/opt/CSCOlumos/bin/run_command.sh livelogs' failed
pi-system-120/admin#
```

ncs run loghistory

You can run **ncs run loghistory** command to view a list of audit logs.

ncs run loghistory { *all* | *secure* | *ade* | *messages* }

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

```
pi-system-120/admin# ncs run loghistory
***Available filter options to limit logs - all  secure ade messages***
::::::::::::::
/var/log/secure
::::::::::::::
2018-02-25T04:22:03.091312+05:30 pi-system-120 passwd: pam_unix(passwd:chauthtok):  \
password changed for scpuser
2018-02-25T05:47:52.693460+05:30 pi-system-120 su: pam_unix(su:session): session    \
opened for user oracle by (uid=0)
2018-02-25T05:47:52.746896+05:30 pi-system-120 su: pam_unix(su:session): session    \
closed for user oracle
2018-02-25T07:48:08.551061+05:30 pi-system-120 su: pam_unix(su:session): session    \
opened for user oracle by (uid=0)
2018-02-25T07:48:08.607276+05:30 pi-system-120 su: pam_unix(su:session): session    \
closed for user oracle
2018-02-25T09:48:29.616066+05:30 pi-system-120 su: pam_unix(su:session): session    \
opened for user oracle by (uid=0)
2018-02-25T09:48:29.675890+05:30 pi-system-120 su: pam_unix(su:session): session    \
closed for user oracle
2018-02-25T11:48:49.792055+05:30 pi-system-120 su: pam_unix(su:session): session    \
opened for user oracle by (uid=0)
2018-02-25T11:48:49.845594+05:30 pi-system-120 su: pam_unix(su:session): session    \
closed for user oracle
2018-02-25T13:49:13.712070+05:30 pi-system-120 su: pam_unix(su:session): session    \
opened for user oracle by (uid=0)
2018-02-25T13:49:13.764692+05:30 pi-system-120 su: pam_unix(su:session): session    \
closed for user oracle
2018-02-25T15:49:28.165108+05:30 pi-system-120 su: pam_unix(su:session): session    \
opened for user oracle by (uid=0)
2018-02-25T15:49:28.231362+05:30 pi-system-120 su: pam_unix(su:session): session    \
closed for user oracle
2018-02-25T17:49:46.089296+05:30 pi-system-120 su: pam_unix(su:session): session    \
opened for user oracle by (uid=0)
2018-02-25T17:49:46.143475+05:30 pi-system-120 su: pam_unix(su:session): session    \
closed for user oracle
2018-02-25T19:50:06.775083+05:30 pi-system-120 su: pam_unix(su:session): session    \
opened for user oracle by (uid=0)
2018-02-25T19:50:06.828332+05:30 pi-system-120 su: pam_unix(su:session): session    \
closed for user oracle
2018-02-25T21:50:33.338183+05:30 pi-system-120 su: pam_unix(su:session): session    \
opened for user oracle by (uid=0)
2018-02-25T21:50:33.393056+05:30 pi-system-120 su: pam_unix(su:session): session    \
closed for user oracle
2018-02-25T23:50:59.225069+05:30 pi-system-120 su: pam_unix(su:session): session    \
opened for user oracle by (uid=0)
2018-02-25T23:50:59.278849+05:30 pi-system-120 su: pam_unix(su:session): session    \
closed for user oracle
2018-02-26T01:51:23.433628+05:30 pi-system-120 su: pam_unix(su-l:session): session  \
opened for user oracle by (uid=0)
2018-02-26T01:52:00.541797+05:30 pi-system-120 su: pam_unix(su-l:session): session  \
closed for user oracle
2018-02-26T01:52:00.582068+05:30 pi-system-120 su: pam_unix(su:session): session    \
opened for user oracle by (uid=0)
2018-02-26T01:52:00.635314+05:30 pi-system-120 su: pam_unix(su:session): session    \
closed for user oracle
2018-02-26T03:30:00.737839+05:30 pi-system-120 su: pam_unix(su-l:session): session  \
opened for user oracle by (uid=0)
2018-02-26T03:30:01.308384+05:30 pi-system-120 su: pam_unix(su-l:session): session  \
closed for user oracle
2018-02-26T03:30:01.318405+05:30 pi-system-120 su: pam_unix(su-l:session): session  \
opened for user oracle by (uid=0)
2018-02-26T03:30:01.373111+05:30 pi-system-120 su: pam_unix(su-l:session): session  \
closed for user oracle
2018-02-26T03:30:01.411957+05:30 pi-system-120 su: pam_unix(su-l:session): session  \
opened for user oracle by (uid=0)
2018-02-26T03:30:03.176254+05:30 pi-system-120 su: pam_unix(su-l:session): session  \
closed for user oracle
2018-02-26T03:30:03.196829+05:30 pi-system-120 su: pam_unix(su-l:session): session  \
opened for user oracle by (uid=0)
2018-02-26T03:30:03.252549+05:30 pi-system-120 su: pam_unix(su-l:session): session  \
closed for user oracle
2018-02-26T03:30:06.105604+05:30 pi-system-120 su: pam_unix(su-l:session): session  \
opened for user oracle by (uid=0)
2018-02-26T03:30:07.126919+05:30 pi-system-120 su: pam_unix(su-l:session): session  \
closed for user oracle
2018-02-26T03:30:07.131747+05:30 pi-system-120 su: pam_unix(su-l:session): session  \
opened for user oracle by (uid=0)
2018-02-26T03:30:14.916295+05:30 pi-system-120 su: pam_unix(su-l:session): session  \
closed for user oracle
2018-02-26T03:30:14.923602+05:30 pi-system-120 su: pam_unix(su-l:session): session  \
opened for user oracle by (uid=0)
pi-system-120/admin#
```

ncs run tls-server-versions

To set the TLS (Transport Layer Security) version, use **ncs run tls-server-versions** command in EXEC mode.

ncs run tls-server-version <TLS version>

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

The following example illustrates the use of the ncs run set-tls-versionscommand:

```
pi-system-117/admin# ncs run tls-server-versions TLSv1 TLSv1.1 TLSv1.2
Error : Invalid TLS version - TLSv1 not supported in FIPS mode
pi-system-117/admin# ncs run tls-server-versions TLSv1.1 TLSv1.2
Enabled TLS version are - TLSv1.1,TLSv1.2
Restart is required for the changes to take effect
pi-system-117/admin#
```

Warning Running this command requires an immediate software restart. It is suggested you perform a failover and failback so that changes are reflected in both primary and secondary servers.

ncs start

To start the server, use the **ncs start** command.

ncs start [verbose]

Syntax Description

verbose	Displays the detailed messages during the start process.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

To see the messages in the console, use the **ncs start verbose** command.

Examples

This example shows how to start the server:

Examples

```
pi-common-133/admin# ncs start verbose

Starting Prime Infrastructure...

Reporting Server Heap size = 4096m
XMP Server Heap size = 6656m
Starting Health Monitor

Starting Health Monitor as a primary
Checking for Port 8082 availability... OK
CERT MATCHED :
Updating web server configuration file ...
Starting Health Montior Web Server...
Health Monitor Web Server Started.
Setting UID to 499:110
UID set to 499:110
Starting Health Monitor Server...
Health Monitor Server Started.
Database server started for instance : wcs

Processing Service Name: Database
Database is already running.

Processing Service Name: FTP Service

Processing Service Name: TFTP Service

Processing Service Name: Matlab
FTP Service is disabled.

Processing Service Name: Matlab1
Starting Remoting Service: Matlab Server

Processing Service Name: Matlab2

Processing Service Name: NMS Server
```

```
Starting Remoting Service: Matlab Server Instance 1
Starting Remoting Service: Matlab Server Instance 2
Checking /tmp/remoting_launchout_Matlab1.lock...
Checking /tmp/remoting_launchout_Matlab.lock...
Checking /tmp/remoting_launchout_Matlab2.lock...
Executing startRemoting for Matlab2 ...
Executing startRemoting for Matlab1 ...
Executing startRemoting for Matlab ...
DEPENDENCY CHECK: Database
DB scheme update process starting..
DB scheme update process finished.
Starting NMS Server
Started TFTP Service
/opt/CSCOlumos/classloader-conf:/opt/CSCOlumos/lib/xmp/XMPClassLoader-11.0.1.jar

Checking for running servers.
  Checking if DECAP is running.
  00:00 DECAP is not running.
00:00 Check complete. No servers running.
Unable to initialize com.mathworks.mwswing.MJStartup
Matlab pid = 9696
system property before init instance: null
Starting Remoting Instance: Matlab Server
Checking for Port 10555 availability... OK
Starting Remoting Service Web Server Matlab Server...
Warning: MATLAB does not support bit depths less than or equal to 8.
Figure windows may not be usable
Warning: latest version of matlab app-defaults file not found.
Contact your system administrator to have this file installed
Warning: Duplicate directory name: /opt/CSCOlumos/matlab/toolbox/compiler.
Remoting Service Web Server Matlab Server Started.
Starting Remoting Service Matlab Server...
Remoting 'Matlab Server' started successfully.
Unable to initialize com.mathworks.mwswing.MJStartup
Matlab1 pid = 9692
system property before init instance: null
Starting Remoting Instance: Matlab Server Instance 1
Checking for Port 10755 availability... OK
Starting Remoting Service Web Server Matlab Server Instance 1...
Warning: MATLAB does not support bit depths less than or equal to 8.
Figure windows may not be usable
Warning: latest version of matlab app-defaults file not found.
Contact your system administrator to have this file installed
Warning: Duplicate directory name: /opt/CSCOlumos/matlab/toolbox/compiler.
Remoting Service Web Server Matlab Server Instance 1 Started.
Starting Remoting Service Matlab Server Instance 1...
  00:09 DECAP setup complete.
Started executing compliance_db_set_up.sh Input = checkAndCreatePariTableOnSID
Remoting 'Matlab Server Instance 1' started successfully.
No Pari table creation needed on SID wcs
Setting/Clearing remote database parameters
Done waiting DB initialization
_outputHdlr check:log4j:WARN No appenders could be found for logger              \
(com.cisco.ciscossl.provider.ciscojce.CiscoJCENativeCrypto).
Starting SAM daemon...
Done.
Done. Setting/Clearing remote database parameters
Starting DA daemon...
Starting Server ...
DASH_HOME = /opt/CSCOlumos/compliance
NCCMHOME = /opt/CSCOlumos/compliance
Asia/Kolkata
Starting NCCM server with Java memory 1024
Unable to initialize com.mathworks.mwswing.MJStartup
Matlab2 pid = 9693
system property before init instance: null
Starting Remoting Instance: Matlab Server Instance 2
Checking for Port 10756 availability... OK
Starting Remoting Service Web Server Matlab Server Instance 2...
Warning: MATLAB does not support bit depths less than or equal to 8.
Figure windows may not be usable
Warning: latest version of matlab app-defaults file not found.
Contact your system administrator to have this file installed
```

```
Warning: Duplicate directory name: /opt/CSCOlumos/matlab/toolbox/compiler.
Remoting Service Web Server Matlab Server Instance 2 Started.
Starting Remoting Service Matlab Server Instance 2...
Remoting 'Matlab Server Instance 2' started successfully.
Creating Application Context
Attempt 1: checking /opt/CSCOlumos/logs/remotingMatlab1-0-0.log and                \
/opt/CSCOlumos/logs/remoting_launchout_Matlab1.log whether Remoting Service Web     \
Server Matlab.* Started.
Detected: /opt/CSCOlumos/logs/remotingMatlab1-0-0.log:02/28/18 01:21:27.147 INFO   \
[system] [main] Remoting Service Web Server Matlab Server Instance 1 Started.
/opt/CSCOlumos/logs/remoting_launchout_Matlab1.log:Remoting Service Web Server      \
Matlab Server Instance 1 Started.
Completed launchout Matlab1 as 9692
Attempt 1: checking /opt/CSCOlumos/logs/remotingMatlab-0-0.log and                 \
/opt/CSCOlumos/logs/remoting_launchout_Matlab.log whether Remoting Service Web      \
Server Matlab.* Started.
Detected: /opt/CSCOlumos/logs/remotingMatlab-0-0.log:02/28/18 01:21:21.247 INFO    \
[system] [main] Remoting Service Web Server Matlab Server Started.
/opt/CSCOlumos/logs/remoting_launchout_Matlab.log:Remoting Service Web Server       \
Matlab Server Started.
Completed launchout Matlab as 9696
Attempt 1: checking /opt/CSCOlumos/logs/remotingMatlab2-0-0.log and                \
/opt/CSCOlumos/logs/remoting_launchout_Matlab2.log whether Remoting Service Web     \
Server Matlab.* Started.
Detected: /opt/CSCOlumos/logs/remotingMatlab2-0-0.log:02/28/18 01:21:37.344 INFO   \
[system] [main] Remoting Service Web Server Matlab Server Instance 2 Started.
/opt/CSCOlumos/logs/remoting_launchout_Matlab2.log:Remoting Service Web Server      \
Matlab Server Instance 2 Started.
Completed launchout Matlab2 as 9693
Starting servlet container.
NMS Server started successfully

Processing Service Name: Compliance engine
Compliance Engine is enabled in this server
Compliance engine is already running.
Invoked post init hook - com.cisco.ifm.telemetry.config.UpdateProxyInitHook@5d67dec7

Prime Infrastructure started successfully.
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
Completed in 577 seconds
pi-common-133/admin#
```

Examples

```
pi-system-120/admin# ncs start
Starting Prime Infrastructure...
This may take a while (10 minutes or more) ...
_outputHdlr check:log4j:WARN No appenders could be found for logger                 \
(com.cisco.ciscossl.provider.ciscojce.CiscoJCENativeCrypto).
Prime Infrastructure started successfully.
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
Completed in 490 seconds
pi-system-120/admin#
```

Related Commands

Command	Description
ncs stop	Stops the server.
ncs status	Displays the current status of the server.

ncs stop

To stop the server, use the **ncs stop** command in EXEC mode. To see the detailed messages, use the **ncs stop verbose** command.

ncs stop [verbose]

Syntax Description

verbose	Displays the detailed messages during the stop process.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

To see the detailed messages, use the **ncs stop verbose** command.

Examples

This example shows how to stop the server:

```
pi-system-120/admin# ncs stop
Stopping Prime Infrastructure...
This may take a few minutes...
Database is not running.
FTP Service is not running.
TFTP Service is not running.
Matlab is not running.
Matlab1 is not running.
Matlab2 is not running.
Matlab3 is not running.
NMS Server is not running!.
Compliance engine is not running!.
Prime Infrastructure successfully shutdown.
log4j:WARN No appenders could be found for logger                                   \
(com.cisco.ciscossl.provider.ciscojce.CiscoJCENativeCrypto).
log4j:WARN Please initialize the log4j system properly.
Stopping SAM daemon...
Checking for SAM daemon again ...
SAM Daemon not found...
Stopping DA daemon ...
Checking for DA daemon again ...
DA Daemon not found...
Compliance engine stopped
Completed shutdown of all services
pi-system-120/admin#
```

Examples

```
pi-common-133/admin# ncs stop verbose
Stopping Prime Infrastructure...

Status:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
```

```
ServerStartupStatus:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
ServerStartupStatus:Creating
Starting servlet container.
ServerStartupStatus:Starting
ServerStartupStatus:Starting
ServerStartupStatus:Starting
ServerStartupStatus:Starting
ServerStartupStatus:Starting
ServerStartupStatus:Starting
ServerStartupStatus:Starting
ServerStartupStatus:Starting
ServerStartupStatus:Starting
ServerStartupStatus:Starting
ServerStartupStatus:Starting
ServerStartupStatus:Starting
ServerStartupStatus:Starting
ServerStartupStatus:Starting
ServerStartupStatus:Starting
ServerStartupStatus:Starting
ServerStartupStatus:Starting
ServerStartupStatus:Starting
ServerStartupStatus:Starting
ServerStartupStatus:Starting
ServerStartupStatus:Starting
ServerStartupStatus:Starting
ServerStartupStatus:Starting
ServerStartupStatus:Starting
NMS Server started successfully

Processing Service Name: Compliance engine
In startService - serviceType:
In startService - serviceName:Compliance engine

Processing Service Name: WSA Service
In startService - serviceType:processScript
In startService - serviceName:WSA Service
Starting the script....wsa_admin.sh
Completed the script....wsa_admin.sh start & Exit value : 0
Invoked post init hook - com.cisco.ifm.telemetry.config.UpdateProxyInitHook@5db6148e
ServerStartupStatus:Invoked
ServerStartupStatus:Invoked
ServerStartupStatus:Invoked
ServerStartupStatus:Invoked
ServerStartupStatus:Invoked
```

```
ServerStartupStatus:Invoked
ServerStartupStatus:Invoked
ServerStartupStatus:Invoked
ServerStartupStatus:Invoked
ServerStartupStatus:Invoked
ServerStartupStatus:Invoked
ServerStartupStatus:Invoked
ServerStartupStatus:Invoked
ServerStartupStatus:Invoked
ServerStartupStatus:Invoked
ServerStartupStatus:Invoked
ServerStartupStatus:Invoked
ServerStartupStatus:Invoked
ServerStartupStatus:Invoked
ServerStartupStatus:Invoked
ServerStartupStatus:Invoked
ServerStartupStatus:Invoked
ServerStartupStatus:Invoked
Processing post upgrade hook -                                                      \
com.cisco.xmp.data.contributions.SecurityContributionsPostUpgradeHook@2a85fe24
ServerStartupStatus:Processing
Processing post upgrade hook -                                                      \
com.cisco.ifm.grouping.service.portgrouping.PortGroupHierarchyChangeUpgradeHook@43f8\
0236
ServerStartupStatus:Processing
Started
ServerStartupStatus:Started
19:45 Server started.
Done
Stopping NMS Server
Stopping XMP .Stopping SAM daemon...
Checking for SAM daemon again ...
Found SAM daemon ...
Stopping SAM daemon ...
Stopping DA daemon ...
Checking for DA daemon again ...
Found DA daemon ...
Stopping DA daemon ...
NMS Server successfully shutdown.
Shutting down database server ...
Database Instance Name = wcs
Database 'wcs' Role = PRIMARY
Listener is not running.
Database server is not running.
Stopped FTP Service
Stopped TFTP Service
Stopping remoting: Matlab Server
Remoting 'Matlab Server' stopped successfully.
Stopping remoting: Matlab Server Instance 1
Remoting 'Matlab Server Instance 1' stopped successfully.
NMS Server is not running!.
Stopping Tomcat...
Tomcat Stopped.

Prime Infrastructure successfully shutdown.

Stopping SAM daemon...
Checking for SAM daemon again ...
SAM Daemon not found...
Stopping DA daemon ...
Checking for DA daemon again ...
DA Daemon not found...
Completed shutdown of all services
```

Related Commands

Command	Description
ncs start	Starts the server.

Command	Description
ncs status	Displays the current status of he server.

ncs status

To display the server status, use the **ncs status** command in EXEC mode.

ncs status

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

This example shows how to display the status of the server:

```
pi-system-117/admin# ncs status
Health Monitor Server is running. ( [Role] Primary [State] HA not Configured )
Database server is running
FTP Service is disabled
TFTP Service is disabled
Matlab Server is running
Matlab Server Instance 1 is running
Matlab Server Instance 2 is running
Matlab Server Instance 3 is running
NMS Server is running.
log4j:WARN No appenders could be found for logger                                  \
(com.cisco.ciscossl.provider.ciscojce.CiscoJCENativeCrypto).
log4j:WARN Please initialize the log4j system properly.
SAM Daemon is running ...
DA Daemon is running ...
Compliance engine is running
pi-system-117/admin#
```

Related Commands

Command	Description
ncs start	Starts the server.
ncs stop	Stops the server.

ncs run tls-server-ciphers

You can enable a TLS cipher group using **ncs run tls-server-ciphers** command in EXEC mode.

ncs run tls-server-ciphers { *tls-ecdhe* **|** *tls-dhe* **|** *tls-static*

Syntax Description

tls-ecdhe	Refers to tls cipher group ecdhe
tls-dhe	Refers to tls cipher group dhe
tls-static	Refers to tls cipher group static

Command Default

No default behavior or values.

EXEC

Examples

```
admin# ncs run tls-server-ciphers tls-ecdhe
Enabled TLS cipher groups are - tls-ecdhe
Restart is required for the changes to take effect
```

ncs password ftpuser

To change the FTP username and password, use the **ncs password ftpuser** command in EXEC mode.

Note The value for ftpuser in the above command should always be set to ftp-user.

After you enable the ftp-user, you can FTP files to and from the /localdisk/ftp folder on standalone or, if configured, High Availability primary servers only. You cannot use change directory (cd) or list directory (ls) functionality with ftp-user.

ncs passwod ftpuser *ftp-user* **password** *password*

Syntax Description

ftp-user	The FTP user name

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

This example shows how to change the FTP username and password:

```
pi-system-65/admin# ncs password ftpuser ftp-user password Password123
Updating FTP password
Saving FTP account password in credential store
Synching FTP account passwd to database store - location-ftp-user
Synching FTP account password to system store
Completed FTP password update
pi-system-65/admin#
```

ncs password root password

To change the root password, use the **ncs password root password** command in EXEC mode.

ncs password root password *userpassword*

Syntax Description

userpassword	Password for the root user.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

This example shows how to migrate archived files to server:

```
pi-systems/admin# ncs password root password Userpassword
Password updated for web root user
pi-systems/admin#
```

ncs ha authkey

To enter the authentication key for high availability (HA), use the **ncs ha authkey** command in EXEC mode.

ncs ha authkey *authorization key*

Syntax Description

authorization key	The authorization key for high availability. Up to 81 alphanumeric characters.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

The **ncs ha authkey** command changes the authorization for the health monitor.

Examples

This example shows how to set up the authorization key for high availability:

```
pi-system/admin#ncs ha authkey cisco123
Going to update primary authentication key
Successfully updated primary authentication key
Successfully intimated  Primary updated  authentication key to Secondary Server
pi-system/admin#
```

Related Commands

Command	Description
ncs ha remove	Removes the high availability configuration settings from .
ncs ha status	Provides the current status of high availability.

ncs ha remove

To remove the high availability configuration settings from , use the **ncs ha remove** command in EXEC mode.

ncs ha remove

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

The **ncs ha remove** command removes the high availability configuration settings from . If you enter this command, you will see the following confirmation message:

```
High availability configuration will be removed.
Do you wish to continue? (Y/N)
```

Examples

```
pi-system/admin# ncs ha remove
High availability configuration will be removed
Do you wish to continue? (y/N)  y

Removing primary configuration will remove all database information
Primary is attempting to remove high availability configuration from both primary    \
and secondary
Successfully removed high availability configuration
pi-system/admin#
```

Related Commands

Command	Description
ncs ha authkey	Allows you to enter the authentication key for high availability in . This command also changes the authorization for the health monitor.
ncs ha status	Provides the current status of high availability.

ncs ha status

To display the current status of high availability (HA), use the **ncs ha status** command in EXEC mode.

ncs ha status

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Displays the current status of HA.

If you enter the **ncs ha status** command when HA is not configured, you will see the following response:

```
[State] Stand Alone
```

Examples

```
pi-system/admin# ncs ha status
[Role] Primary [State] HA not Configured
pi-systems/admin#
```

In Primary server:

```
pi-system/admin# ncs ha status
[Role] Primary [Secondary Server] 10.197.71.162(10.197.71.162) [State] Primary
Active [Failover Type] Automatic
pi-system/admin#
```

In Secondary server:

```
pi-system/admin# ncs ha status
[Role] Secondary [Primary Server] pi-system-161(10.197.71.161) [State] Secondary
Syncing [Failover Type] Automatic
pi-system/admin#
```

Related Commands

Command	Description
ncs ha authkey	Allows you to enter the authentication key for high availability in . This command also changes the authorization for the health monitor.
ncs ha remove	Removes the high availability configuration.

ncs key genkey

To generate a new RSA key and self-signed certificate, use the **ncs key genkey** command. You can use this command in the following ways:

ncs key genkey -newdn -csr csrfilename repository repositoryname

Syntax Description

genkey	Generates a new RSA key and self-signed certificate. You can use the following options with this command: **-csr**: Generate Certificate Signing Request(CSR) file **-newdn**: Generate new RSA key and self-signed certificate with domain information **<cr>**: Carriage return.
-newdn	Generates a new RSA key and self-signed cert with domain information. You can use the following options with this command: **-csr**: Generate Certificate Signing Request(CSR) file **<cr>**: Carriage return.
-csr	Generates new CSR certificate file. You can use the following option with this command: **<WORD>**: Type in certificate file name (Max Size - 80)
csrfilename	CSR filename.
repository	Repository command. This option is available when you use the -csr option.
repositoryname	Location where the files should be backed up to. Up to 80 alphanumeric characters.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

This example shows how to generate new rsa key and certificate files in the Prime Infrastructure server:

```
pi-cluster-88/admin# ncs key genkey -newdn -csr test.csr repository defaultRepo

Changes will take affect on the next server restart
  Enter the fully qualified domain name of the server !!!!: pi-cluster-88.cisco.com
  Enter the name of your organization unit !!!!!!!!!!!!!!!: cisco
  Enter the name of your organization !!!!!!!!!!!!!!!!!!!!: hcl
  Enter the name of your city or locality !!!!!!!!!!!!!!!!: chennai
  Enter the name of your state or province !!!!!!!!!!!!!!!: tn
  Enter the two letter code for your country !!!!!!!!!!!!!: US
```

```
    Specify subject alternate names.
    If none specified, CN will be used.
  Use comma seperated list - DNS:<name>,IP:<address> !!!!!:                         \
DNS:pi-cluster-88.cisco.com,IP:10.126.168.88

  Specify the public key algorithm [rsa/ec] !!!!!!!!!!!!!!: rsa
  Specify the RSA key size [2048/4096/8192] !!!!!!!!!!!!!!: 4096
  Specify the signature algorithm [sha256/sha512] !!!!!!!!: sha256

Key and CSR/Certificate will be generated with following details
  Subject                :                                                          \
/C=US/ST=tn/L=chennai/O=hcl/OU=cisco/CN=pi-cluster-88.cisco.com
  Subject Alternate Name : DNS:pi-cluster-88.cisco.com,IP:10.126.168.88
  Public Key Alg         : rsa, 4096
  Signature Alg          : sha256

Continue [yes] : yes
Generating...
Completed generating new key...Changes will take affect on the next server restart
Note: You can provide comma separated list of FQDN and IP of PI servers where you want to
import the same certificate received from CA.
To import same CA in other server, you need to import the key from the server where you
generate CSR and them import the CA certiifcates.
```

Note You will get csr file generated in location where repository is pointing. Use that csr file get CA certificate or signed certificate from any CA agent.

Related Commands

Command	Description
ncs key importcacert	Applies a CA certificate to the trust store in Prime Infrastructure.
ncs key listcacerts	Lists all of the CA certificates that exist in the Prime Infrastructure trust store.
ncs key deletecacert	Deletes a CA certificates that exist in the Prime Infrastructure trust store.
ncs key importsignedcert	Applies an RSA key and signed certificate to Prime Infrastructure.
ncs key importkey	Applies an RSA key and certificate to Prime Infrastructure.

Note After entering this command, enter the **ncs stop** and **ncs start** command to restart the Prime Infrastructure server to make changes take effect.

ncs key importcacert

To apply a CA certificate to a trust store in , use the **ncs key importcacert** command in the EXEC mode.

To import the root certificate:

ncs key importcacert *aliasname ca-cert-filename* **repository** *repositoryname*

To import the subordinate certificate:

ncs key importcacert *aliasname* **sub***ca-cert-filename* **repository** *repositoryname*

Syntax Description

aliasname	A short name given for this CA certificate.
ca-cert-filename	CA certificate file name.
repository	Repository command.
sub	Subordinate certificate.
repositoryname	The repository name configured in where the ca-cert-filename is hosted.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

This example shows how to apply the CA certificate file to a trust store in the server:

```
ncs key importcacert truststore system alias root trca-4096-sha2.cer repository     \
defaultRepo

Certificate is added to trust store. Changes will take affect on the next server    \
restart


ncs key importcacert truststore system alias sub tsca-4096-sha2.cer repository      \
defaultRepo

Certificate is added to trust store. Changes will take affect on the next server    \
restart
```

Note After applying this command, enter the **ncs stop** and **ncs start** command to restart the server to make the changes take effect.

Related Commands

Command	Description
ncs key genkey	Generates a new RSA key and self-signed certificate.
ncs key listcacerts	Lists all of the CA certificates that exist in the trust store.
ncs key deletecacert	Deletes a CA certificates that exist in the trust store.
ncs key importsignedcert	Applies an RSA key and signed certificate to .
ncs key importkey	Applies an RSA key and certificate to .

ncs key importkey

To apply an RSA key and signed certificate to the Prime Infrastructure, use the **ncs key importkey** command in EXEC mode.

To export key:

ncs key exportkey *key-filename cert-filename* **repository** *repositoryname*

To import key:

ncs key importkey *key-filename cert-filename* **repository** *repositoryname*

Syntax Description

key-filename	RSA private key file name.
cert-filename	Certificate file name.
repository	Repository command
repositoryname	The repository name configured in the Prime Infrastructure where the key-file and cert-file is hosted.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

This example shows how to apply the new RSA key and certificate files to the server.

```
ncs key exportkey private.key server.cer repository defaultRepo

ncs key importkey keyfile certfile repository ncs-sftp-repo
```

Note After applying this command, enter the **ncs stop** and **ncs start** command to restart the server to make the changes take effect.

Related Commands

Command	Description
ncs key genkey	Generates a new RSA key and self-signed certificate.
ncs key listcacerts	Lists all of the CA certificates that exist in the Prime Infratsructure trust store.
ncs key deletecacert	Deletes a CA certificates that exist in the Prime Infratsructure trust store.

Command	Description
ncs key importsignedcert	Applies an RSA key and signed certificate to Prime Infratsructure.
ncs key importcacert	Applies an CA certificate to trust store in the Prime Infratsructure.

ncs key listcacerts

To list all of the CA certificates that exist in the trust store, use the **ncs key listcacerts** command EXEC mode.

ncs key listcacerts

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

This example shows how to list all of the CA certificates that exist in the trust store:

```
>  ncs key listcacerts
--------------------------  DevMgmt Trust Store                                      \
------------------------------------
local_rootca_rsa, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
E0:41:6B:A3:E8:F5:EA:A8:FF:4B:88:FB:E8:C2:54:A7:CB:99:7F:85
cmca3, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
08:DA:AB:CE:42:B3:0D:64:03:33:7D:EB:87:C9:8E:4D:F5:9B:7C:6F
cmca2, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
90:B2:E0:6B:7A:D5:DA:FF:CF:D4:31:87:29:09:F3:81:37:47:1B:F8
ciscoassurancerootca2099, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
2C:A6:69:D0:B2:79:08:F7:29:C9:10:C6:23:17:8E:98:14:35:9B:C9
local_rootca_ec, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
C2:FC:D6:19:2A:00:E2:95:C6:D2:05:11:34:5B:94:49:43:32:B3:14
ciscorootca2048, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
DE:99:0C:ED:99:E0:43:1F:60:ED:C3:93:7E:7C:D5:BF:0E:D9:E5:FA
hasudi, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
F8:1D:55:50:D6:7D:CD:1D:D1:11:92:B5:7F:8F:DE:09:A4:A5:69:B7
ceca, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
F1:16:68:0E:E9:A4:8D:0B:D6:94:72:76:F8:C7:B4:A7:5C:E7:11:16
xsslr2, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
AC:23:0A:22:B9:FE:19:FC:5F:A0:FD:D0:8D:91:54:F9:8F:7F:B6:AE
eccroot, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
52:EC:7D:BB:5C:65:11:DD:C1:C5:46:DB:BC:29:49:B5:AB:E9:D0:EE
ciscoumbrellaroot, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
C5:09:11:32:E9:AD:F8:AD:3E:33:93:2A:E6:0A:5C:8F:A9:39:E8:24
airespace-root, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
94:EC:7D:BA:E4:E6:FB:F1:E0:44:03:81:CB:ED:EF:32:79:C9:90:B5
cmca, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
E3:E7:83:D3:CC:9C:30:AE:DE:FF:CD:EB:5E:CF:EE:08:FF:8F:16:84
rxcr2, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
2C:8A:FF:CE:96:64:30:BA:04:C0:4F:81:DD:4B:49:C7:1B:5B:81:A0
```

```
ciscorootca2099, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
AC:1E:DE:2E:1C:97:0F:ED:3E:E8:5F:8C:3A:CF:E2:BA:C0:4A:13:76
act2eccsudi, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
32:78:95:B8:C4:E0:3C:EC:14:AE:D9:70:EF:99:C8:D9:34:0B:80:E6
crcam2, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
93:3D:63:3A:4E:84:0D:A4:C2:8E:89:5D:90:0F:D3:11:88:86:F7:A3
crcam1, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
45:AD:6B:B4:99:01:1B:B4:E8:4E:84:31:6A:81:C2:7D:89:EE:5C:E7
act2sudica, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
F6:96:9B:BD:48:E5:F6:12:5B:93:4D:01:E7:1F:E9:C2:7C:6F:54:7E
attca, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
C1:C4:B5:6B:D1:88:47:B8:D5:94:92:1F:ED:94:D5:21:FC:65:04:FE
ciscoclientca001, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
50:0B:9B:BE:D7:DB:DE:00:3A:3E:F4:3E:AF:9E:D5:2B:01:34:C3:5F

--------------------------- System Trust Store                                      \
---------------------------------------
verisignclass1g3ca, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
20:42:85:DC:F7:EB:76:41:95:57:8E:13:6B:D4:B7:D1:E9:8E:46:A5
digicertglobalrootca, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
A8:98:5D:3A:65:E5:E5:C4:B2:D7:D6:6D:40:C6:DD:2F:B1:9C:54:36
quovadisrootca3cert, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
1F:49:14:F7:D8:74:95:1D:DD:AE:02:C0:BE:FD:3A:2D:82:75:51:85
verisignclass2g2ca, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
B3:EA:C4:47:76:C9:C8:1C:EA:F2:9D:95:B6:CC:A0:08:1B:67:EC:9D
verisigntsaca, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
20:CE:B1:F0:F5:1C:0E:19:A9:F3:8D:B1:AA:8E:03:8C:AA:7A:C7:01
verisignclass3g3ca, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
13:2D:0D:45:53:4B:69:97:CD:B2:D5:C3:39:E2:55:76:60:9B:5C:C6
quovadisrootca3g3cert, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
48:12:BD:92:3C:A8:C4:39:06:E7:30:6D:27:96:E6:A4:CF:22:2E:7D
tomcat, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
D4:72:AD:57:25:94:73:6F:E2:0D:F1:65:D7:36:D2:95:E8:A6:AA:C6
quovadisrootca2g3cert, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
09:3C:61:F3:8B:8B:DC:7D:55:DF:75:38:02:05:00:E1:25:F5:C8:36
verisignclass3g5ca, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
4E:B6:D5:78:49:9B:1C:CF:5F:58:1E:AD:56:BE:3D:9B:67:44:A5:E5
ciscolicensingrootca, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
5C:A9:5F:B6:E2:98:0E:C1:5A:FB:68:1B:BB:7E:62:B5:AD:3F:A8:B8
quovadisrootca1g3cert, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
1B:8E:EA:57:96:29:1A:C9:39:EA:B8:0A:81:1A:73:73:C0:93:79:67
verisignclass1ca, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
CE:6A:64:A3:09:E4:2F:BB:D9:85:1C:45:3E:64:09:EA:E8:7D:60:F1
quovadisroot, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
DE:3F:40:BD:50:93:D3:9B:6C:60:F6:DA:BC:07:62:01:00:89:76:C9
quovadisrootca2cert, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
AC:4A:72:8B:4D:FC:35:60:1F:A3:4B:92:24:22:A4:2C:25:3F:75:6C
verisignclass1g2ca, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                     \
27:3E:E1:24:57:FD:C4:F9:0C:55:E8:2B:56:16:7F:62:F5:32:E5:47
verisignclass3ca, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                       \
A1:DB:63:93:91:6F:17:E4:18:55:09:40:04:15:C7:02:40:B0:AE:6B
quovadisrootca2, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                       \
CA:3A:FB:CF:12:40:36:4B:44:B2:16:20:88:80:48:39:19:93:7C:F7
verisignuniversalrootca, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                       \
36:79:CA:35:66:87:72:30:4D:30:A5:FB:87:3B:0F:A7:7B:B7:0D:54
ciscoeccrootcacertp2, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                       \
52:EC:7D:BB:5C:65:11:DD:C1:C5:46:DB:BC:29:49:B5:AB:E9:D0:EE
verisignclass2g3ca, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                       \
61:EF:43:D7:7F:CA:D4:61:51:BC:98:E0:C3:59:12:AF:9F:EB:63:11
quovadisrootca4cert, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                       \
DE:3F:40:BD:50:93:D3:9B:6C:60:F6:DA:BC:07:62:01:00:89:76:C9
verisignclass3g2ca, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                       \
85:37:1C:A6:E5:50:14:3D:CE:28:03:47:1B:DE:3A:09:E8:F8:77:0F
verisignclass3g4ca, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                       \
22:D5:D8:DF:8F:02:31:D1:8D:F7:9D:B7:CF:8A:2D:64:C9:3F:6C:3A
ciscomanufacturingrootca2048, Mar 19, 2018, trustedCertEntry,
Certificate fingerprint (SHA1):                                                       \
E3:E7:83:D3:CC:9C:30:AE:DE:FF:CD:EB:5E:CF:EE:08:FF:8F:16:84
pi-cluster-88/admin#
```

Related Commands

Command	Description
ncs key genkey	Generates a new RSA key and self-signed certificate.
ncs key importkey	Applies an RSA key and signed certificate to the .
ncs key deletecacert	Deletes CA certificates that exist in the trust store.
ncs key importsignedcert	Applies an RSA key and signed certificate to the .
ncs key importcacert	Applies a CA certificate to the trust store in .

ncs key deletecacert

To delete CA certificates that exist in trust store, use the **ncs key deletecacert** command in the EXEC mode.

ncs key deletecacert trustore *system alias root*

Syntax Description

alias	The short or alias name of the CA certificate which needs to be deleted from the trust store.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

This example shows how to delete CA certificates that exist in the trust store:

```
ncs key deletecacert truststore system alias root
```

```
Deleting certificate from trust store
```

Related Commands

Command	Description
ncs key genkey	Generates a new RSA key and self-signed certificate.
ncs key importkey	Applies an RSA key and signed certificate to .
ncs key listcacerts	Lists all of the CA certificates that exist in the trust store.
ncs key importsignedcert	Applies an RSA key and signed certificate to .
ncs key importcacert	Applies a CA certificate to the trust store in .

ncs key importsignedcert

To apply an RSA key and signed certificate, use the **ncs key importsignedcert** command EXEC mode.

ncs key importsignedcert *signed-cert-filename* **repository** *repositoryname*

Syntax Description

signed-cert-filename	Signed certificate filename.
repository	Repository command
repositoryname	The repository name configured in where the key-file and cert-file is hosted.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

This example shows how to apply signed certificate files to the server:

```
> ncs key importsingedcert signed-certfile repository ncs-sftp-repo
```

Note After applying this command, enter the **ncs stop** and the **ncs start** command to restart the server to make changes take effect.

Related Commands

Command	Description
ncs key genkey	Generates a new RSA key and self-signed certificate.
ncs key importkey	Applies an RSA key and signed certificate to .
ncs key deletecacert	Deletes CA certificates that exist in the trust store.
ncs key listcacerts	Lists all of the CA certificates that exist in the trust store.
ncs key importcacert	Applies a CA certificate to the trust store in .

ncs cleanup

To clean up the following data,below datafree up and reclaim the disk space, use the **ncs cleanup** command in EXEC mode.

- Files under /opt/backup
- *.m-n.logs, *.n.logs, *.log.n log files under /opt/CSCOlumos/logs
- Regular files under /localdisk
- .hprof file under opt/CSCOlumos/crash
- Matlab*.log under /opt/tmp/
- .trm and .trc files under /opt/oracle/base/diag/rdbms/*/*/trace
- Older expired Archive logs and backup set under /opt/oracle/base/fast_recovery_area/WCS

ncs cleanup

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

When does not have enough disk space, an alarm is raised to free up and reclaim the disk space. If you enter the **ncs cleanup** command, you will see the following confirmation message:

```
Do you want to delete all the files in the local disk partition? (Y/N)
```

Examples

```
pi-system-117/admin# ncs cleanup
***************************************************************************
!!!!!!!                            WARNING                          !!!!!!!
***************************************************************************
The clean up can remove all files located in the backup staging directory.
Older log files will be removed and other types of older debug information
will be removed
***************************************************************************
Do you wish to continue? ([NO]/yes) yes


***************************************************************************
!!!!!!!                 DATABASE CLEANUP WARNING                    !!!!!!!
***************************************************************************
Cleaning up database will stop the server while the cleanup is performed.
The operation can take several minutes to complete
***************************************************************************
Do you wish to cleanup database? ([NO]/yes) yes


***************************************************************************
!!!!!!!                 USER LOCAL DISK WARNING                     !!!!!!!
***************************************************************************
```

```
Cleaning user local disk will remove all locally saved reports, locally
backed up device configurations. All files in the local FTP and TFTP
directories will be removed.
***************************************************************************
Do you wish to cleanup user local disk? ([NO]/yes) yes
===================================================
Starting Cleanup: Wed Feb 28 01:50:44 IST 2018
===================================================
{Wed Feb 28 01:50:47 IST 2018} Removing all files in backup staging directory
{Wed Feb 28 01:50:47 IST 2018} Removing all Matlab core related files
{Wed Feb 28 01:50:47 IST 2018} Removing all older log files
{Wed Feb 28 01:50:47 IST 2018} Cleaning older archive logs
{Wed Feb 28 01:51:03 IST 2018} Cleaning database backup and all archive logs
{Wed Feb 28 01:51:03 IST 2018} Cleaning older database trace files
{Wed Feb 28 01:51:03 IST 2018} Removing all user local disk files
{Wed Feb 28 01:51:03 IST 2018} Cleaning database
{Wed Feb 28 01:51:05 IST 2018} Stopping server
{Wed Feb 28 01:52:05 IST 2018} Not all server processes stop. Attempting to stop    \
remaining
{Wed Feb 28 01:52:05 IST 2018} Stopping database
{Wed Feb 28 01:52:07 IST 2018} Starting database
{Wed Feb 28 01:52:20 IST 2018} Starting database clean
{Wed Feb 28 01:58:50 IST 2018} Completed database clean
{Wed Feb 28 01:58:50 IST 2018} Stopping database
{Wed Feb 28 01:59:14 IST 2018} Starting server
===================================================
Completed Cleanup
Start Time: Wed Feb 28 01:50:44 IST 2018
Completed Time: Wed Feb 28 02:07:07 IST 2018
===================================================
pi-system-117/admin#
```

nslookup

To look up the hostname of a remote system on the server, use the **nslookup** command in EXEC mode.

nslookup *word*

Syntax Description

word	IPv4 address or hostname of a remote system. Up to 63 alphanumeric characters.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

```
ncs/admin# nslookup 209.165.200.225
Trying "209.165.200.225.in-addr.arpa"
Received 127 bytes from 172.16.168.183#53 in 1 ms
Trying "209.165.200.225.in-addr.arpa"
Host 209.165.200.225.in-addr.arpa. not found: 3(NXDOMAIN)
Received 127 bytes from 172.16.168.183#53 in 1 ms

ncs/admin#

ncs/admin# nslookup 209.165.200.225
Trying "225.200.165.209.in-addr.arpa"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 65283
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;225.200.165.209.in-addr.arpa.  IN      PTR

;; ANSWER SECTION:
225.200.165.209.in-addr.arpa. 86400 IN  PTR     209-165-200-225.got.net.

;; AUTHORITY SECTION:
192.168.209.in-addr.arpa. 86400 IN      NS      ns1.got.net.
192.168.209.in-addr.arpa. 86400 IN      NS      ns2.got.net.

Received 119 bytes from 172.16.168.183#53 in 28 ms

ncs/admin#
```

ocsp

Online Certificate Status Protocol (OCSP) enables certificate-based authentication for web clients using OCSP responders. Typically, the OCSP responder's URL is read from the certificate's Authority Information Access (AIA). As a failover mechanism, you can configure the same URL on the Prime Infrastructure server as well. You can enable or disable a custom OCSP responder, and set or remove OCSP responder URLs, using **ocsp responder** command in EXEC mode.

ocsp responder { *remove* | *set* | *show* }

Syntax Description

clear	Clear OCSP responder URL
custom	Enable or disable custom OCSP responder
set	Set OCSP responder URL.

Command Default

No default behaviour.

Command Modes

EXEC

Examples

```
ncs/admin# ocsp responder
ncs/admin# ocsp responder custom enable

ncs/admin# ocsp responder set url1 <WORD>
<WORD>  Enter ocsp url (Max Size - 1024)

ncs/admin# ocsp responder clear url1
```

ping

To diagnose the basic IPv4 network connectivity to a remote system, use the **ping** command in EXEC mode.

ping *{ip-address | hostname}* [**Df***df]*[**packetsize***packetsize]*[**pingcount***pingcount]*

Syntax Description

ip-address	IP address of the system to ping. Up to 32 alphanumeric characters.
hostname	Hostname of the system to ping. Up to 32 alphanumeric characters.
df	Specification for packet fragmentation.
df	Specifies the value as **1** to prohibit packet fragmentation, or **2** to fragment the packets locally, or **3** to not set df.
packetsize	Size of the ping packet.
packetsize	Specifies the size of the ping packet; the value can be between 0 and 65507.
pingcount	Number of ping echo requests.
pingcount	Specifies the number of ping echo requests; the value can be between 1 and 10.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

The **ping** command sends an echo request packet to an address, then awaits a reply. The ping output can help you evaluate path-to-host reliability, delays over the path, and whether you can reach a host.

Examples

```
ncs/admin# ping 172.16.0.1 df 2 packetsize 10 pingcount 2
PING 172.16.0.1 (172.16.0.1) 10(38) bytes of data.
18 bytes from 172.16.0.1: icmp_seq=0 ttl=40 time=306 ms
18 bytes from 172.16.0.1: icmp_seq=1 ttl=40 time=300 ms

--- 172.16.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 300.302/303.557/306.812/3.255 ms, pipe 2
ncs/admin#
```

Related Commands

Command	Description
ping6	Pings a remote IPv6 address.

ping6

To diagnose the basic IPv6 network connectivity to a remote system, use the **ping6** command in EXEC mode.

ping6 *{ip-address* | *hostname}* *[***GigabitEthernetpacketsize***packetsize][***pingcount***pingcount]*

Syntax Description

ip-address	IP address of the system to ping. Up to 64 alphanumeric characters.
hostname	Hostname of the system to ping. Up to 64 alphanumeric characters.
GigabitEthernet	Selects the ethernet interface.
packetsize	Size of the ping packet.
packetsize	Specifies the size of the ping packet; the value can be between 0 and 65507.
pingcount	Number of ping echo requests.
pingcount	Specifies the number of ping echo requests; the value can be between 1 and 10.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

The IPv6 **ping6** command sends an echo request packet to an address, then awaits a reply. The ping output can help you evaluate path-to-host reliability, delays over the path, and whether you can reach a host.

The IPv6 **ping6** command is similar to the existing IPv4 ping command that does not support the IPv4 ping fragmentation (df in IPv4) options, but allows an optional specification of an interface. The interface option is primarily useful for pinning with link-local addresses that are interface-specific. The packetsize and pingcount options work identically the same as they do with the IPv4 command.

Examples

```
ncs/admin# ping6 3ffe:302:11:2:20c:29ff:feaf:da05
PING 3ffe:302:11:2:20c:29ff:feaf:da05(3ffe:302:11:2:20c:29ff:feaf:da05) from
3ffe:302:11:2:20c:29ff:feaf:da05 eth0: 56 data bytes
64 bytes from 3ffe:302:11:2:20c:29ff:feaf:da05: icmp_seq=0 ttl=64 time=0.599 ms
64 bytes from 3ffe:302:11:2:20c:29ff:feaf:da05: icmp_seq=1 ttl=64 time=0.150 ms
64 bytes from 3ffe:302:11:2:20c:29ff:feaf:da05: icmp_seq=2 ttl=64 time=0.070 ms
64 bytes from 3ffe:302:11:2:20c:29ff:feaf:da05: icmp_seq=3 ttl=64 time=0.065 ms

--- 3ffe:302:11:2:20c:29ff:feaf:da05 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3118ms
rtt min/avg/max/mdev = 0.065/0.221/0.599/0.220 ms, pipe 2

ncs/admin#

ncs/admin# ping6 3ffe:302:11:2:20c:29ff:feaf:da05 GigabitEthernet 0 packetsize 10 pingcount
 2
```

```
PING 3ffe:302:11:2:20c:29ff:feaf:da05(3ffe:302:11:2:20c:29ff:feaf:da05) from
3ffe:302:11:2:20c:29ff:feaf:da05 eth0: 10 data bytes
18 bytes from 3ffe:302:11:2:20c:29ff:feaf:da05: icmp_seq=0 ttl=64 time=0.073 ms
18 bytes from 3ffe:302:11:2:20c:29ff:feaf:da05: icmp_seq=1 ttl=64 time=0.073 ms

--- 3ffe:302:11:2:20c:29ff:feaf:da05 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1040ms
rtt min/avg/max/mdev = 0.073/0.073/0.073/0.000 ms, pipe 2

ncs/admin#
```

Related Commands

	Description
ping	Pings a remote IP address.

reload

To reload the operating system, use the **reload** command in EXEC mode.

reload

Syntax Description

This command has no arguments or keywords.

Command Default

The command has no default behavior or values.

Command Modes

EXEC

Usage Guidelines

The **reload** command reboots the system. Use the **reload** command after you enter configuration information into a file and save the running-configuration to the persistent startup-configuration on the CLI and save any settings in the web Administration user interface session.

Before you enter the **reload** command, ensure that the is not performing any backup, restore, installation, upgrade, or remove operation. If the performs any of these operations and you enter the **reload** command, you will notice any of the following warning messages:

```
WARNING: A backup or restore is currently in progress! Continue with reload?
```

```
WARNING: An install/upgrade/remove is currently in progress! Continue with reload?
```

If you get any of these warnings, enter YES to halt the operation, or enter NO to cancel the halt.

If no processes are running when you use the **reload** command or you enter YES in response to the warning message displayed, the asks you to respond to the following option:

```
Do you want to save the current configuration ?
```

Enter YES to save the existing configuration. The displays the following message:

```
Saved the running configuration to startup successfully
```

Examples

```
ncs/admin# reload
Do you want to save the current configuration ? (yes/no) [yes] ? yes
Generating configuration...
Saved the running configuration to startup successfully
Continue with reboot? [y/n] y

Broadcast message from root (pts/0) (Fri Aug  7 13:26:46 2010):

The system is going down for reboot NOW!

ncs/admin#
```

Related Commands

Command	Description
halt	Disables the system.

restore

To perform a restore of a previous backup, use the **restore** command in EXEC mode.

Application Backup Restore:

Use the following command to restore data related only to application:

restore *filename* **repository** *repository-name* **application** *application-name*

Application Backup Restore

Use the following command to restore data related to the application and Cisco ADE OS:

restore *filename* **repository** *repository-name*

Syntax Description

filename	Name of the backed-up file that resides in the repository. Up to 120 alphanumeric characters. **Note** You must add the .tar.gpg extension after the filename (for example, myfile.tar.gpg).
repository	The repository keyword.
repository-name	Name of the repository you want to restore from backup.
application	The application keyword.
application-name	The name of the application data to be restored. Up to 255 alphanumeric characters. **Note** Enter the application name as ‘PI’ in upper case.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

A restore operation restores data related to the as well as the Cisco ADE OS. To perform a restore of a previous backup of the application data of the only, add the **application** command to the **restore** command in EXEC mode.

When you use these two commands in the , the server restarts automatically.

Examples

```
pi-system-153/admin# restore                                                    \
veeraiah-180306-1952__VER3.4.0.0.120_BKSZ10G_CPU4_MEM3G_RAM11G_SWAP15G_APP_CK1753058
834.tar.gpg repository defaultRepo application NCS

* NOTE *
If the system console is disconnected or got cleared on session timeout
```

```
run 'show restore log' to see the output of the last restore session.

Restore will restart the application services. Continue? (yes/no) [yes] ? yes

DO NOT press ^C while the restoration is in progress
Aborting restore with a ^C may leave the system in a unrecoverable state

Enter the backup password, if your backup is password protected. Otherwise, press
Enter to continue the data restoration.

Password :
Initiating restore.  Please wait...
  Restore Started at 03/06/18 20:17:16
  Stage 1 of 9: Transferring backup file ...
  -- completed at 03/06/18 20:17:17
  Stage 2 of 9: Decrypting backup file ...
  -- completed at  03/06/18 20:17:24
  Stage 3 of 9: Unpacking backup file ...
  -- completed at  03/06/18 20:17:24
  Stopping PI server ...
  Stage 4 of 9: Decompressing backup ...
  -- completed at  03/06/18 20:19:18
  Stage 5 of 9: Restoring Support Files ...
  -- completed at  03/06/18 20:19:29
  Stage 6 of 9: Restoring Database Files ...
   -- completed at  03/06/18 20:21:09
  Stage 7 of 9: Recovering Database ...                              72%)
  -- completed at  03/06/18 20:28:30
  Stage 8 of 9: Updating Database Schema ...
    This could take long time based on the existing data size.
                  Stage 1 of 5: Pre Migration Schema Upgrade ...

                                        -- completed at: 2018-03-06 20:56:51.473,
Time Taken : 0 hr, 28 min, 14 sec
                  Stage 2 of 5: Schema Upgrade ...
                                        -- completed at: 2018-03-06 21:01:43.078,
Time Taken : 0 hr, 4 min, 50 sec
                  Stage 3 of 5: Post Migration Schema Upgrade ...

                                        -- completed at: 2018-03-06 21:01:49.583,
Time Taken : 0 hr, 0 min, 5 sec
                  Stage 4 of 5: Enabling DB Constraints ...

                                        -- completed at: 2018-03-06 21:02:30.131,
Time Taken : 0 hr, 0 min, 38 sec
                  Stage 5 of 5: Finishing Up ...
                                        -- completed at: 2018-03-06 21:02:52.174,
Time Taken : 0 hr, 0 min, 21 sec
  -- completed at  03/06/18 21:03:26
  Stage 9 of 9: Re-enabling Database Settings ...
   -- completed at  03/06/18 21:28:17
   Total Restore duration is: 01h:11m:01s
INFO: Restore completed successfully.

Starting Prime Infrastructure...

This may take a while (10 minutes or more) ...

Prime Infrastructure started successfully.

Completed in 889 seconds
```

Related Commands

Command	Description
backup	Performs a backup (and Cisco ADE OS) and places the backup in a repository.
show restore, on page 146	Displays the restore history.

Command	Description
repository	Enters the repository submode for configuration of backups.
show repository	Displays the available backup files located on a specific repository.
show backup history	Displays the backup history of the system.

rmdir

To remove an existing directory, use the **rmdir** command in EXEC mode.

rmdir *word*

Syntax Description

word	Directory name. Up to 80 alphanumeric characters.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

```
ncs/admin# mkdir disk:/test
ncs/admin# dir

Directory of disk:/

       4096 May 06 2010 13:34:49  activemq-data/
       4096 May 06 2010 13:40:59  logs/
      16384 Mar 01 2010 16:07:27  lost+found/
       4096 May 06 2010 13:42:53  target/
       4096 May 07 2010 12:26:04  test/

           Usage for disk: filesystem
                  181067776 bytes total used
                19084521472 bytes free
                20314165248 bytes available
ncs/admin#

ncs/admin# rmdir disk:/test
ncs/admin# dir

Directory of disk:/

       4096 May 06 2010 13:34:49  activemq-data/
       4096 May 06 2010 13:40:59  logs/
      16384 Mar 01 2010 16:07:27  lost+found/
       4096 May 06 2010 13:42:53  target/

           Usage for disk: filesystem
                  181063680 bytes total used
                19084525568 bytes free
                20314165248 bytes available
ncs/admin#
```

Related Commands

Command	Description
dir	Displays a list of files on the server.
mkdir	Creates a new directory.

rsakey

To display a configured RSA key or to set a new RSA public key for user authentication, use **rsakey** command in EXEC mode. You can also use it to remove a configured RSA key.

rsakey { remove | set | show }

Syntax Description

remove	Remove RSA public key for user authentication.
set	Set RSA public key for user authentication.
show	Show RSA public key for user authentication.

Command Default

No default behaviour.

Command Modes

EXEC

Examples

```
ncs/admin# rsakey
ncs/admin# rsakey show
No RSA key configured for user 'admin'
```

```
ncs/admin# rsakey remove
No RSA key configured for user 'admin
```

```
ncs/admin# rsakey set <WORD>
<WORD>  Filename of RSA public key (Max Size - 256)
```

show

To show the running system information, use the **show** command in EXEC mode. The **show** commands are used to display the settings and are among the most useful commands.

The commands in Table A-6 require the **show** command to be followed by a keyword; for example, **show application status**. Some **show** commands require an argument or variable after the keyword to function; for example, **show application version**.

For detailed information on all of the **show** commands, see show Commands.

show keyword

Syntax Description

Table 2: Summary of show Commands

Command(1)	Description
application (requires keyword)(2)	Displays information about the installed application; for example, status or version.
backup (requires keyword)	Displays information about the backup.
cdp (requires keyword)	Displays information about the enabled Cisco Discovery Protocol interfaces.
clock	Displays the day, date, time, time zone, and year of the system clock.
cpu	Displays CPU information.
disks	Displays file-system information of the disks.
interface	Displays statistics for all of the interfaces configured on the Cisco ADE OS.
logging (requires keyword)	Displays system logging information.
logins (requires keyword)	Displays login history.
memory	Displays memory usage by all running processes.
ntp	Displays the status of the Network Time Protocol (NTP).
ports	Displays all of the processes listening on the active ports.
process	Displays information about the active processes of the server.

Command(1)	Description
repository (requires keyword)	Displays the file contents of a specific repository.
restore (requires keyword)	Displays restore history on the server.
running-config	Displays the contents of the currently running configuration file on the server.
startup-config	Displays the contents of the startup configuration on the server.
tech-support	Displays system and configuration information that you can provide to the TAC when you report a problem.
terminal	Displays information about the terminal configuration parameter settings for the current terminal line.
timezone	Displays the time zone of the server.
timezones	Displays all of the time zones available for use on the server.
udi	Displays information about the unique device identifier (UDI) of the .
uptime	Displays how long the system you are logged in to has been up and running.
users	Displays information for currently logged in users.
version	Displays information about the installed application version.

12

[1] (1) The commands in this table require that the show command precedes a keyword; for example, show application.

[2] (2) Some show commands require an argument or variable after the keyword to function; for example, show application version. This show command displays the version of the application installed on the system (see show application).

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

All **show** commands require at least one keyword to function.

Examples

```
pi-system-117/admin# show application
name          Description
NCS              Cisco Prime Infrastructure
pi-system-117/admin#
```

Examples

```
pi-cluster-88/admin# show version

Cisco Application Deployment Engine OS Release: 3.1
ADE-OS Build Version: 3.1.0.001
ADE-OS System Architecture: x86_64

Copyright (c) 2009-2018 by Cisco Systems, Inc.
All rights reserved.
Hostname: pi-cluster-88


Version information of installed applications
---------------------------------------------

Cisco Prime Infrastructure
********************************************************
Version : 3.4.0
Build : 3.4.0.0.330
pi-cluster-88/admin#
```

ssh

To start an encrypted session with a remote system, use the **ssh** command in EXEC mode.

Note An Admin or Operator (user) can use this command (see Table 1-1).

ssh *[ip-address | hostname] username***port***[number]***version[1|2] delete hostkey***word*

Syntax Description

ip-address	IP address of the remote system. Up to 64 alphanumeric characters.
hostname	Hostname of the remote system. Up to 64 alphanumeric characters.
username	Username of the user logging in through SSH.
port [*number*]	(Optional) Indicates the port number of the remote host. From 0 to 65,535. Default 22.
version [1 | 2]	(Optional) Indicates the version number. Default 2.
delete hostkey	Deletes the SSH fingerprint of a specific host.
word	IPv4 address or hostname of a remote system. Up to 64 alphanumeric characters.

Command Default

Disabled.

Command Modes

EXEC (Admin or Operator).

Usage Guidelines

The **ssh** command enables a system to make a secure, encrypted connection to another remote system or server. This connection provides functionality similar to that of an outbound Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client allows for secure communication over an insecure network.

Examples

```
ncs/admin# ssh ncs1 admin
admin@ncs1's password:
Last login: Wed Jul 11 05:53:20 2008 from ncs.cisco.com

ncs1/admin#

ncs/admin# ssh delete host ncs
ncs/admin#
```

tech dumptcp

To dump a Transmission Control Protocol (TCP) package to the console, use the **tech dumptcp** command in EXEC mode.

tech dumptcp *gigabit-ethernet*

Syntax Description

gigabit-ethernet	Gigabit Ethernet interface number 0 to 1.

Command Default

Disabled.

Command Modes

EXEC

Examples

```
ncs/admin# tech dumptcp 0
140816:141088(272) ack 1921 win 14144
08:26:12.034630 IP NCS.cisco.com.ssh > dhcp-64-102-82-153.cisco.com.2221: P 141088:141248(160)
 ack 1921 win 14144
08:26:12.034635 IP dhcp-64-102-82-153.cisco.com.2221 > NCS.cisco.com.ssh: . ack 139632 win
 64656
08:26:12.034677 IP NCS.cisco.com.ssh > dhcp-64-102-82-153.cisco.com.2221: P 141248:141520(272)
 ack 1921 win 14144
08:26:12.034713 IP NCS.cisco.com.ssh > dhcp-64-102-82-153.cisco.com.2221: P 141520:141680(160)
 ack 1921 win 14144
08:26:12.034754 IP NCS.cisco.com.ssh > dhcp-64-102-82-153.cisco.com.2221: P 141680:141952(272)
 ack 1921 win 14144
08:26:12.034756 IP dhcp-64-102-82-153.cisco.com.2221 > NCS.cisco.com.ssh: . ack 140064 win
 65520
08:26:12.034796 IP NCS.cisco.com.ssh > dhcp-64-102-82-153.cisco.com.2221: P 141952:142112(160)
 ack 1921 win 14144
1000 packets captured
1000 packets received by filter
0 packets dropped by kernel
ncs/admin#
```

telnet

To log in to a host that supports Telnet, use the **telnet** command in operator (user) or EXEC mode.

telnet *[ip-address | hostname] port number*

Syntax Description

ip-address	IP address of the remote system. Up to 64 alphanumeric characters.
hostname	Hostname of the remote system. Up to 64 alphanumeric characters.
port number	(Optional) Indicates the port number of the remote host. From 0 to 65,535.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

```
ncs/admin# telnet 172.16.0.11 port 23
ncs.cisco.com login: admin
password:
Last login: Mon Jul  2 08:45:24 on ttyS0
ncs/admin#
```

terminal length

To set the number of lines on the current terminal screen for the current session, use the **terminal length** command in EXEC mode.

terminal length *integer*

Syntax Description

integer	Number of lines on the screen. Contains between 0 to 511 lines, inclusive. A value of zero (0) disables pausing between screens of output.

Command Default

24 lines.

Command Modes

EXEC

Usage Guidelines

The system uses the length value to determine when to pause during multiple-screen output.

Examples

```
ncs/admin# terminal length 0
ncs/admin#
```

terminal session-timeout

To set the inactivity timeout for all sessions, use the **terminal session-timeout** command in EXEC mode.

terminal session-timeout *minutes*

Syntax Description

minutes	Sets the number of minutes for the inactivity timeout. From 0 to 525,600. Zero (0) disables the timeout.

Command Default

30 minutes.

Command Modes

EXEC

Usage Guidelines

Setting the **terminal session-timeout** command to zero (0) results in no timeout being set.

Examples

```
ncs/admin# terminal session-timeout 40
ncs/admin#
```

Related Commands

Command	Description
terminal session-welcome	Sets a welcome message on the system for all users who log in to the system.

terminal session-welcome

To set a welcome message on the system for all users who log in to the system, use the **terminal session-welcome** command in EXEC mode.

terminal session-welcome *string*

Syntax Description

string	Welcome message. Up to 2,023 alphanumeric characters.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Specify a message using up to 2048 characters.

Examples

```
ncs/admin# terminal session-welcome Welcome
ncs/admin#
```

Related Commands

Command	Description
terminal session-timeout	Sets the inactivity timeout for all sessions.

terminal terminal-type

To specify the type of terminal connected to the current line for the current session, use the **terminal terminal-type** command in EXEC mode.

terminal terminal-type *type*

Syntax Description

type	Defines the terminal name and type, and permits terminal negotiation by hosts that provide that type of service. Up to 80 alphanumeric characters.

Command Default

VT100.

Command Modes

EXEC

Usage Guidelines

Indicate the terminal type if it is different from the default of VT100.

Examples

```
ncs/admin# terminal terminal-type vt220
ncs/admin#
```

traceroute

To discover the routes that packets take when traveling to their destination address, use the **traceroute** command in EXEC mode.

traceroute *[ip-address* | *hostname]*

Syntax Description

ip-address	IP address of the remote system. Up to 32 alphanumeric characters.
hostname	Hostname of the remote system. Up to 32 alphanumeric characters.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

```
ncs/admin# traceroute 172.16.0.11
traceroute to 172.16.0.11 (172.16.0.11), 30 hops max, 38 byte packets
 1  172.16.0.11 0.067 ms  0.036 ms  0.032 ms

ncs/admin#
```

undebug

To disable debugging functions, use the **undebug** command in EXEC mode.

undebug *{all* | *application* | *backup-restore* | *cdp* | *config* | *copy* | *icmp* | *locks* | *logging* | *snmp* | *system* | *transfer* | *user* | *utils}*

Syntax Description

all	Disables all debugging.
application	Application files. • *all*—Disables all application debug output. • *install*—Disables application install debug output. • *operation*—Disables application operation debug output. • *uninstall*—Disables application uninstall debug output.
backup-restore	Backs up and restores files. • *all*—Disables all debug output for backup-restore. • *backup*—Disables backup debug output for backup-restore. • *backup-logs*—Disables backup-logs debug output for backup-restore. • *history*—Disables history debug output for backup-restore. • *restore*—Disables restore debug output for backup-restore.
cdp	Cisco Discovery Protocol configuration files. • *all*—Disables all Cisco Discovery Protocol configuration debug output. • *config*—Disables configuration debug output for Cisco Discovery Protocol. • *infra*—Disables infrastructure debug output for Cisco Discovery Protocol.

config	Configuration files. • *all*—Disables all configuration debug output. • *backup*—Disables backup configuration debug output. • *clock*—Disables clock configuration debug output. • *infra*—Disables configuration infrastructure debug output. • *kron*—Disables command scheduler configuration debug output. • *network*—Disables network configuration debug output. • *repository*—Disables repository configuration debug output. • *service*—Disables service configuration debug output.
copy	Copy commands.
icmp	ICMP echo response configuration. *all*—Disable all debug output for ICMP echo response configuration. Set level between 0 and 7, with 0 being severe and 7 being all.
locks	Resource locking. • *all*—Disables all resource locking debug output. • *file*—Disables file locking debug output.
logging	Logging configuration files. *all*—Disables all debug output for logging configuration.
snmp	SNMP configuration files. *all*—Disables all debug output for SNMP configuration.
system	System files. • *all*—Disables all system files debug output. • *id*—Disables system ID debug output. • *info*—Disables system info debug output. • *init*—Disables system init debug output.
transfer	File transfer.
user	User management. • *all*—Disables all user management debug output. • *password-policy*—Disables user management debug output for password-policy.

utils	Utilities configuration files. *all*—Disables all utilities configuration debug output.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

```
ncs/admin# undebug all
ncs/admin#
```

Related Commands

Command	Description
debug	Displays errors or events for command situations.

write

To copy, display, or erase server configurations, use the **write** command with the appropriate argument in EXEC mode.

write *{erase* | *memory* | *terminal}*

Syntax Description

erase	Erases the startup configuration. This command is disabled by default.
memory	Copies the running configuration to the startup configuration.
terminal	Copies the running configuration to console.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

The following is an example of the write command with the erase keyword:

Note write erase command functionality is disabled from Cisco Prime Infrastructure Release 2.0 and later. If you try to write erase, then the following warning message is displayed.

```
pi-system/admin# write erase
% Warning: 'write erase' functionality has been disabled by application: NCS
pi-system/admin#
```

Cisco Plug and Play Gateway Commands

This section lists the **pnp** commands along with a brief description of their use, command defaults, command modes, command syntax, usage guidelines, command examples, and related commands, where applicable.

Prime Infrastructure Integrated Server Commands

This section lists the **ncs pnp gateway commands** along with a brief description of its use, command defaults, command modes, command syntax, usage guidelines, command examples, and related commands, where applicable.

ncs pnp-gateway

To enable or disable the local Cisco Plug and Play Gateway on the Prime Infrastructure Integrated Server and modify or view the properties of the software image on the Cisco Plug and Play Gateway, use the **ncs pnp-gateway** command in privileged EXEC mode.

ncs pnp-gateway {**enable** | **disable** | **modify** | **property**}

Syntax Description

enable	Enables the Cisco Plug and Play Gateway.
disable	Disables the Cisco Plug and Play Gateway.
modify	Enables the modification of the Cisco Plug and Play Gateway image's properties. The properties that can be modified are: activation timeout value, distribution timeout value, and transfer timeout value.
property	Enables viewing of the properties pertaining to the software image on the Cisco Plug and Play Gateway.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco Prime Infrastructure 2.0	This command was introduced.

Examples

The following is sample output from the **ncs pnp-gateway** command:

```
admin# ncs  pnp-gateway?

  disable   PNP Gateway Disable Command
  enable    PNP Gateway Enable command
  modify    Modify PnP Gateway properties and variables
  property  Show PnP properties and configuration
```

Examples

The following is sample output from the **ncs pnp-gateway disable** command:

```
ncs pnp-gateway disable

Disabling Plug and Play Gateway.....
Plug and Play Gateway is successfully disabled. Please restart Prime Infrastructure on this
 server
```

Examples

The following is a sample output of the **ncs pnp-gateway enable** command:

```
ncs pnp-gateway enable

Enabling Plug and Play Gateway.....
```

```
Plug and Play Gateway is successfully enabled. Please restart Prime Infrastructure on this
 server.
```

Examples

The following is a sample output of the **ncs pnp-gateway modify** command:

```
ncs pnp-gateway modify

bgl-dt-ncs-vm6-70/ayyanna# ncs pnp-gateway modify image ?
  activation-timeout    Activation timeout for PnP image upgrade job
  distribution-timeout  Distribution timeout for PnP image upgrade job
  transfer-timeout      Transfer timeout for PnP image upgrade job
bgl-dt-ncs-vm6-70/ayyanna# ncs pnp-gateway modify image
  activation-timeout ? <60-1048576> Type the image activation timeout value (seconds)
```

Examples

The following is a sample output of the **ncs pnp-gateway property image** command:

```
admin# ncs pnp-gateway property image

PnP Gateway Image Transfer Timeout = 2400
PnP Gateway Image Distribution Timeout = 2200
PnP Gateway Image Activation Timeout = 1600
```

Prime Infrastructure PnP Gateway Standalone Server Command

This section lists the **pnp gateway standalone server commands** along with a brief description of their use, command defaults, command modes, command syntax, usage guidelines, command examples, and related commands, where applicable.

pnp backup

To create a backup of the Cisco Plug and Play Gateway configuration, use the **pnp backup** command in privileged EXEC mode.

pnp backup

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco Prime Infrastructure 1.2	This command was introduced.
Cisco Prime Infrastructure 2.0	This command was modified.

Usage Guidelines

The backup file is usually created in a compressed tar file format in the *disk:/ directory* that corresponds to the */localdisk/ directory* on the Linux file system.

Examples

The following is sample output from the **pnp backup** command:

```
admin# pnp backup
```

```
The backup file created : /localdisk/20130130220403.pnp_backup.tar.gz
```

The following table describes the significant field shown in the display.

Table 3: pnp backup Field Description

Field	Description
20130130220403.pnp_backup.tar.gz	The backup file created in the above example, where *2013* is the year, *01* is the month, *30* is the date, *22* is the hour, *04* is the minute, and *03* is the second at which the backup file was created.

pnp modify image

To modify the properties of the Cisco Plug and Play Gateway software image in the Prime Infrastructure Plug and Play Standalone Gateway, use the **pnp modify image** command in privileged EXEC mode.

pnp modify image {**activation-timeout | distribution-timeout | transfer-timeout | transfer-timeout**}**timeout-value**

Syntax Description

activation timeout value	Activation timeout value, in seconds, for the Cisco Plug and Play Gateway software image upgrade job. The range is from 60 to 1048576. The default is 600.
distribution timeout value	Distribution timeout value, in seconds, for the Cisco Plug and Play Gateway software image upgrade job. The valid range is from 60 to 1048576. The default is 1200.
transfer timeout value	Transfer timeout value, in seconds, for the Cisco Plug and Play Gateway software image upgrade job. The valid range is from 60 to 1048576. The default is 1200.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco Prime Infrastructure 1.2	This command was introduced.
Cisco Prime Infrastructure 2.0	This command was modified.

Usage Guidelines

The Cisco Plug and Play Gateway does not have to be restarted for the timeout value to take effect. The timeout value that you specify will take effect for the next software image.

Examples

The following is sample output from the **pnp modify image** command:

```
admin# pnp modify image ?

  activation-timeout    Activation timeout for PnP image upgrade job
  distribution-timeout  Distribution timeout for PnP image upgrade job
  transfer-timeout      Transfer timeout for PnP image upgrade job

admin# pnp modify image activation-timeout 1200
Done

admin# pnp modify image distribution-timeout 2400
Done
```

```
admin# pnp modify image transfer-timeout 2200
Done
```

pnp modify log-level

To modify the log-level settings of the Cisco Plug and Play Gateway, use the **pnp modify log-level** command in privileged EXEC mode.

The Cisco Plug and Play Gateway supports these log levels: **debug, error, fatal, info, trace, and warn**.

pnp modify log-level {**fatal** | **error** | **warn** | **info** | **debug** | **trace**}

Syntax Description

fatal	Enables the collection of fatal-level log messages.
error	Enables the collection of fatal-level and error-level log messages.
warn	Enables the collection of fatal-level, error-level, and warn-level log messages.
info	Enables the collection of fatal-level, error-level, warn-level, and information-level log messages.
debug	Enables the collection of fatal-level, error-level, warn-level, information-level, and debug-level log messages.
trace	Enables the collection of fatal-level, error-level, warn-level, information-level, debug-level, and trace-level log messages.

Command Default

By default, the Cisco Plug and Play Gateway logs the error-level log messages.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco Prime Infrastructure 1.2	This command was introduced.
Cisco Prime Infrastructure 2.0	This command was modified.

Usage Guidelines

The **pnp modify log-level** command can be used to dynamically change the log level at run time. However, when you restart the Cisco Plug and Play Gateway, it will reset to the error-log level, which is the default.

Examples

The following is sample output from the **pnp modify log-level** command:

```
admin# pnp modify log-level ?

  debug  Log level: Debug
  error  Log level: Error
  fatal  Log level: Fatal
  info   Log level: Info
  trace  Log level: Trace
  warn   Log level: Warn

admin# pnp modify log-level debug
admin# pnp modify log-level error
admin# pnp modify log-level fatal
admin# pnp modify log-level info
admin# pnp modify log-level trace
admin# pnp modify log-level warn
```

pnp restore

To restore the configuration settings from an existing backup of the Cisco Plug and Play Gateway, use the **pnp restore** command in privileged EXEC mode.

To force a restore of the Cisco Plug and Play Gateway settings either when the **pnp setup** command is in operation or another instance of the **pnp restore** command is already running, use the **pnp restore force** command in privileged EXEC mode.

pnp restore *backup filename*

pnp restore force

Syntax Description

backup filename	Name of the Cisco Plug and Play Gateway backup file whose server settings must be restored.
force	Forces a restore of the Cisco Plug and Play Gateway settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco Prime Infrastructure 1.2	This command was introduced.
Cisco Prime Infrastructure 2.0	This command was modified.

Usage Guidelines

When you run the **pnp restore** command, the server reads the backup files from the */localdisk/ directory*. If there is more than one backup file in the */localdisk/ directory*, a list of the available backup files is displayed. You must provide the name of the backup file that is to be used for restoring the configuration settings.

After the Cisco Plug and Play Gateway settings have been restored, you are prompted to commit the changes. Press **y** to commit the changes or **n** to cancel the restore operation.

Note You must restart the Cisco Plug and Play Gateway for changes to take effect.

Note For information on how to copy files to the local disk, see copy, on page 12 command.

Use the **pnp restore force** command when you have to force a restore operation. This condition is normally seen when different instances of the **restore** command is already running or when the **pnp setup** command is in operation. The **pnp restore force** command forces the restore operation using an existing backup file.

Examples

The following is a sample output of the **pnp restore** command:

```
admin# pnp restore

------------------------------------------------
Tue Oct 2 23:05:53 UTC 2012
Restore operation started
------------------------------------------------
Please copy the backup required for restoration.
20121002230546.pnp_backup.tar.gz
20121002224919.pnp_backup.tar.gz
Please provide the backup file name [20121002230546.pnp_backup.tar.gz]:
Backup Filename used is /localdisk/20121002230546.pnp_backup.tar.gz

Commit changes and restart (y/n): y
```

pnp setup

To set up the Cisco Plug and Play Gateway information, use the **pnp setup** command in privileged EXEC mode.

To forcefully execute a setup operation of the Cisco Plug and Play Gateway when other commands are running and the **pnp setup** command cannot be used for setting up the server, use the **pnp setup force** command in privileged EXEC mode.

Note The **pnp setup** command can be executed only if Prime Infrastructure and the Cisco Plug and Play Gateway are running on different servers.

pnp setup

pnp setup force

Syntax Description

force	Executes a setup operation of the Cisco Plug and Play Gateway forcefully.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco Prime Infrastructure 1.2	This command was introduced.
Cisco Prime Infrastructure 2.0	This command was modified.

Usage Guidelines

The setup.log file is available in the *var/KickStart/install/ directory*.

Examples

The following is sample output from the **pnp setup** command:

```
admin# pnp setup
              ######################################################################
        Enter Plug and Play Gateway Setup.
        Setup log at /var/KickStart/install/setup.log.
       For detail information about the parameters in this setup,
        refer to Plug and Play Gateway Admin Guide.

        Plug and Play Gateway setup in standard mode
        Use the advanced setup by calling pnp setup advanced for
        1) Changing ports numbers and options for the different ports.
        2) Changing Prime Infrastructure message queue configuration like username.
        3) For Prime high availability configuration where prime
           primary and secondary have different IP Address.
        ######################################################################
        Enter the Prime Infrastructure Server IP Address, or
        Virtual IP Address in case Prime Infrastructure is
        configured in High Availability Mode with a Virtual IP.

Enter Prime Infrastructure IP Address: [10.104.105.170]

        The password for message queue between Plug and Play Gateway
        and Prime Infrastructure. Please set the password using
        'ncs pnp-secret <password>' command on Prime Infrastructure.
        Restart the Prime Infrastructure application
        and then provide in the below step.

Password is already set for message queue.
Do you want to reset the password (y/n)? [n]

Enable self certificate for Plug and Play Gateway server
bgl-dt-pnp-ha-216 (y/n)? [y]

Self Signed Certificate already available do you want to recreate (y/n)? [n]

        Automatic download of SSL Certificate is possible if
        Prime Infrastructure Server is up and running.

Automatically download the certificate for Prime Infrastructure server
10.104.105.170 (y/n)? [y]

        The event gateway ports 11011 and 11012 are reserved for port
        automatic allocation. If you want to zero touch deploy your devices
        or already have deployed devices currently using these 2 ports,
        then you should enable this feature and enter the correct 'cns event'
        command in the later part of this setup. For details please
        refer to the Plug and Play Gateway section of quick start guide.


Enable Event Gateways port automatic allocation (y/n)? [y]

        The maximum number of Event Gateways allowed is '10'
        for both plain text and ssl combined. The Event Gateway ports
        11011 and 11012 are reserved for port automatic allocation.
        These ports are not counted in the maximum number of ports.

        Each Event Gateway can serve maximum of 1000 devices.

Enter number of SSL event gateways to be started: [5]

        The maximum number of plain text event gateways ports possible is 5.

Enter number of plaintext event gateways to be started: [5]

        Plug and Play Gateway High Availability requires secondary server
        to be installed and reachable from primary server.The setup of Primary
        Plug and Play Gateway will automatically setup the secondary server.

Do you want to setup high availability with bgl-dt-pnp-ha-216 server
as primary (y/n)? [n] y

        Plug and Play Gateway High Availability can be configured with manual
        or automaticfailback from secondary to primary server.

         0) Manual mode would require the secondary to be shutdown for failback
             to occur to primary.(RECOMMENDED OPTION)
         1) Automatic mode would mean failback would happen as soon as primary
            is available and reachable again.

Provide whether the high availability should do failback manually or automatically
(0/1): [1]

Provide the virtual IP address to be used for high availability [] 10.104.50.179

Provide the virtual host name to be used for high availability [] myhost

Provide the Plug and Play Gateway secondary server IP address [10.104.50.217]
```

```
        The list of network interfaces on the Plug and Play Gateway
        server are listed below.
                lo
                eth0
                sit0
        Please select the appropriate interface on which to set the
        virtual IP address for high availability.

Provide the interface on which virtual IP is to be set [eth0]

        The CNS Event command configures how the managed devices should
        connect to this particular Plug and Play Gateway. The command entered
        in the following line should match what is configured on the devices
        WITHOUT the port number and keyword 'encrypt' if cryptographic is enabled.

        For example, if the following CLI is configured on devices
        'cns event myhost encrypt 11012 keepalive 120 2 reconnect 10'
        ,then 'encrypt 11012' should be removed and the below line should be
        entered:'cns event myhost keepalive 120 2 reconnect 10'

        Another example, if this is a backup Plug and Play Gateway and the
        following CLI is configured on devices
        'cns event myhost 11011 source Vlan1 backup', '11011'
        should be removed and the below line should be entered:
        'cns event myhost source Vlan1 backup'

        Plug and Play Gateway has a new feature to automatically get
        the CNS event on the device using CNS exec functionality ('cns exec').
        If this function is unable to get the CLI from the device then the
        CLI mentioned below is used as the default CLI to be pushed onto the
        device. Please provide a proper default CLI which is accessible from
        most devices.

Enter CNS Event command:
[cns event bgl-dt-pnp-ha-216 keepalive 120 2 reconnect 10]


Commit changes (y/n)?
```

Note For more information on how to copy files from the local disk, see copy, on page 12 command.

pnp setup advanced

To change port level settings, use the **pnp setup advanced** command in the privileged EXEC mode.

To forcefully execute a setup operation of the Cisco Plug and Play Gateway when other commands are running and the **pnp setup advanced** command cannot be used for setting up the server, use the **pnp setup advanced force** command in privileged EXEC mode.

pnp setup advanced

pnp setup advanced force

Syntax Description

force	Executes a setup operation of the Cisco Plug and Play Gateway forcefully.

Command Modes

Privileged EXEC (#)

Command History

Release	**Modification**
Cisco Prime Infrastructure 2.0	This command was introduced.

Usage Guidelines

The setup.log file is available in the *var/KickStart/install/ directory*.

Examples

The following is a sample output of the **pnp setup advanced** command:

```
pnp setup  advanced
######################################################################
        Enter Plug and Play Gateway Setup.
        Setup log at /var/KickStart/install/setup.log.
        For detail information about the parameters in this setup,
        refer to Plug and Play Gateway Admin Guide.
        ######################################################################

Enter IP address of Plug and Play Gateway server: [10.104.50.216]

Enter the fully qualified host name of Plug and Play Gateway server
: [bgl-dt-pnp-ha-216]

        Enter the Prime Infrastructure Server IP Address, or
        Prime Infrastructure Primary Server IP Address
        in case Primary and Secondory have different IP Address, or
        Virtual IP Address in case Prime Infrastructure is
        configured in High Availability Mode with a Virtual IP.

Enter Prime Infrastructure IP Address: [10.104.105.170]

Enter Prime Infrastructure message queue port parameter: [61617]

Enable password on the messaging queue between Plug and Play Gateway and
Prime Infrastructure (y/n)? [y]

        The username for message queue between Plug and Play Gateway and
        Prime Infrastructure.This is usually the default value 'xmpBroker'
        and kept as the default itself. Modify this only if the
        Prime Infrastructure username has changed.

Enter the messge queue username for the Prime Infrastructure: [xmpBroker]

        The password for message queue between Plug and Play Gateway
        and Prime Infrastructure. Please set the password using
        'ncs pnp-secret <password>' command on Prime Infrastructure.
        Restart the Prime Infrastructure application
       and then provide in the below step.

Password is already set for message queue.
Do you want to reset the password (y/n)? [n]

Enable self certificate for Plug and Play Gateway server
bgl-dt-pnp-ha-216 (y/n)? [y]

Self Signed Certificate already available do you want to recreate (y/n)? [n]

        Automatic download of SSL Certificate is possible if
        Prime Infrastructure Server is up and running.

Automatically download the certificate for Prime Infrastructure server
10.104.105.170 (y/n)? [y]

Enable secure HTTPS/SSL encryption to secure Plug and Play Gateway (y/n)? [y]

Enter port number for https web access: [443]

        Enabling clear text operation
        between Plug and Play Gateway and device(s) increases security risk.

Enable clear text operation between device CNS agent and Plug and Play Gateway
(y/n)? [y]

        Prime Infrastructure High Availability can be configured with Virtual IP
        Address or Primary and Secondary Server having different IP Address.
        Please select 'y' only if primary and secondary have different IP.

Do you want to configure Prime Infrastructure HA with IP address for
secondary server (y/n)? [n] y

Enter Prime Infrastructure secondary server IP address: [] 10.104.105.170

        Automatic download of SSL Certificate is possible if
        Prime Infrastructure High Availability Secondary Server.
        Health Monitoring should be up and running in port 8082

Automatically download the certificate for Prime Infrastructure server
10.104.105.170 (y/n)? [y]

Enter Tomcat internal AJP port number: [8009]

Enter Tomcat shutdown port number: [8005]

        IOS Devices can be authenticated before being allowed to
        connect to the Event Gateway/Config Server.
        Prime Infrastructure server doesn't support
        authentication for CNS devices.
        Please keep the default 'n' for this option.

Enable authentication (y/n)? [n]

        The event gateway ports 11011 and 11012 are reserved for port
        automatic allocation. If you want to zero touch deploy your devices
        or already have deployed devices currently using these 2 ports,
        then you should enable this feature and enter the correct 'cns event'
        command in the later part of this setup. For details please
        refer to the Plug and Play Gateway section of quick start guide.


Enable Event Gateways port automatic allocation (y/n)? [y]
```

```
        The maximum number of Event Gateways allowed is '10'
        for both plain text and ssl combined. The Event Gateway ports
        11011 and 11012 are reserved for port automatic allocation.
        These ports are not counted in the maximum number of ports.

        Each Event Gateway can serve maximum of 1000 devices.

Enter number of SSL event gateways to be started: [5]

Enter port number for http web access: [80]

        The maximum number of plain text event gateways ports possible is 5.

Enter number of plaintext event gateways to be started: [5]

        Plug and Play Gateway High Availability requires secondary server
        to be installed and reachable from primary server.The setup of Primary
        Plug and Play Gateway will automatically setup the secondary server.

Do you want to setup high availability with bgl-dt-pnp-ha-216 server
as primary (y/n)? [n] y

        Plug and Play Gateway High Availability can be configured with manual
        or automaticfailback from secondary to primary server.

         0) Manual mode would require the secondary to be shutdown for failback
             to occur to primary.(RECOMMENDED OPTION)
         1) Automatic mode would mean failback would happen as soon as primary
            is available and reachable again.

Provide whether the high availability should do failback manually or automatically
(0/1): [1]

Provide the virtual IP address to be used for high availability [] 10.104.50.178

Provide the virtual host name to be used for high availability [] secondary

Provide the Plug and Play Gateway secondary server IP address [10.104.50.217]

        The list of network interfaces on the Plug and Play Gateway
        server are listed below.
                lo
                eth0
                sit0
        Please select the appropriate interface on which to set the
        virtual IP address for high availability.

Provide the interface on which virtual IP is to be set [eth0]

        The CNS Event command configures how the managed devices should
       connect to this particular Plug and Play Gateway. The command entered
        in the following line should match what is configured on the devices
        WITHOUT the port number and keyword 'encrypt' if cryptographic is enabled.

        For example, if the following CLI is configured on devices
        'cns event secondary encrypt 11012 keepalive 120 2 reconnect 10'
        ,then 'encrypt 11012' should be removed and the below line should be
        entered:'cns event secondary keepalive 120 2 reconnect 10'

        Another example, if this is a backup Plug and Play Gateway and the
        following CLI is configured on devices
        'cns event secondary 11011 source Vlan1 backup', '11011'
        should be removed and the below line should be entered:
        'cns event secondary source Vlan1 backup'

        Plug and Play Gateway has a new feature to automatically get
        the CNS event on the device using CNS exec functionality ('cns exec').
        If this function is unable to get the CLI from the device then the
        CLI mentioned below is used as the default CLI to be pushed onto the
        device. Please provide a proper default CLI which is accessible from
        most devices.
```

```
Enter CNS Event command:
[cns event bgl-dt-pnp-ha-216 keepalive 120 2 reconnect 10]

        Enter IP address for CNS Gateway to listen to.
        Enter 1 to have CNSGateway listens to all IP addresses.

IP addresses:[1]

Enter Plug and Play Gateway event port parameter: [62616]

Do you want to use FTP for image distribution (y/n)? [n]

Enter base directory for Plug and Play Gateway log : [/var/log]

        Data directory contains Template and Image files

Enter data directory for Plug and Play Gateway : [/var/KickStart]

        The Automatic device connection feature can be enabled to tear down
        device connection after first successful configuration push.
        This will tear down all connection to the PnP Gateway from device.

        ############################## NOTE ##################################
        Generally recommended to be disable this when more than one configuration
        would be sent from Prime Infrastructure management server.
        For example :- When Prime Infrastructure has a reload template
        as part of Plug and Play Gateway composite templates
        ######################################################################

Turn down device connection after first successful configuration push (y/n)? [n]


Commit changes (y/n)?
```

pnp start

To start the Cisco Plug and Play Gateway and display the status messages in detail during the startup process, use the **pnp start** command in privileged EXEC mode.

pnp start

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco Prime Infrastructure 1.2	This command was introduced.
Cisco Prime Infrastructure 2.0	This command was modified.

Usage Guidelines

Before you execute the **pnp start** command, stop the Cisco Plug and Play gateway. For more information on stopping the Cisco Plug and Play gateway, refer to the section pnp stop, on page 109.

Examples

The following is sample output from the **pnp start** command:

```
admin# pnp start

httpd is stopped
Monitoring process started.
Plug and Play Gateway start..................
Started Event Manager process
Starting tomcat...
Starting httpd:
                                                         [  OK  ]
Starting CNS Gateway:
Start of Plug and Play Gateway Completed!!
admin#
```

pnp status

To determine the status of the individual tasks and services that are currently running on the Cisco Plug and Play Gateway, use the **pnpstatus** command in privileged EXEC mode.

pnp status

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco Prime Infrastructure 1.2	This command was introduced.
Cisco Prime Infrastructure 2.0	This command was modified.

Usage Guidelines

This command can also be used to determine whether the tasks that are running on the Cisco Plug and Play Gateway are secure or nonsecure, and whether the services are up and running or down, along with their port and PID number, where applicable.

Examples

The following is sample output from the **pnp status** command:

```
admin# pnp status
SERVICE                       |  MODE           |  STATUS   |  ADDITIONAL INFO
------------------------------------------------------------------------------------------
System                        |                 |  UP       |
------------------------------------------------------------------------------------------
Event Messaging Bus           |  PLAIN TEXT     |  UP       | pid: 3839
CNS Gateway Dispatcher        |  PLAIN TEXT     |  UP       | pid: 4216, port: 11011
CNS Gateway                   |  PLAIN TEXT     |  UP       | pid: 4245, port: 11013
CNS Gateway                   |  PLAIN TEXT     |  UP       | pid: 4279, port: 11015
CNS Gateway                   |  PLAIN TEXT     |  UP       | pid: 4313, port: 11017
CNS Gateway                   |  PLAIN TEXT     |  UP       | pid: 4404, port: 11019
CNS Gateway                   |  PLAIN TEXT     |  UP       | pid: 4442, port: 11021
CNS Gateway Dispatcher        |  SSL            |  UP       | pid: 4645, port: 11014
CNS Gateway                   |  SSL            |  UP       | pid: 4645, port: 11014
CNS Gateway                   |  SSL            |  UP       | pid: 4706, port: 11016
CNS Gateway                   |  SSL            |  UP       | pid: 4881, port: 11018
CNS Gateway                   |  SSL            |  UP       | pid: 4921, port: 11020
CNS Gateway                   |  SSL            |  UP       | pid: 4955, port: 11022
HTTPD                         |                 |  UP       |
Image Web Service             |  SSL            |  UP       |
Config Web Service            |  SSL            |  UP       |
Resource Web Service          |  SSL            |  UP       |
Image Web Service             |  PLAIN TEXT     |  UP       |
Config Web Service            |  PLAIN TEXT     |  UP       |
Resource Web Service          |  PLAIN TEXT     |  UP       |
Prime Infrastructure Broker   |  SSL            |  UP       | port: 61617,connection:1
```

pnp stop

To stop the Cisco Plug and Play Gateway and display detailed messages during the stop process, use the **pnp stop** command in privileged EXEC mode.

pnp stop

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco Prime Infrastructure 1.2	This command was introduced.
Cisco Prime Infrastructure 2.0	This command was modified.

Examples

The following is sample output from the **pnp stop** command:

```
admin# pnp stop

start   status  stop
bgl-dt-ncs-vm64-228/admin# pnp stop
Plug and Play Gateway is being shut down..... Please wait!!!
Stopping monitoring process ...
Stopping CNS Gateway Processes:
Stopping tomcat...
Stopping httpd:
OK                                                         [  OK  ]
Stopping Event Manager Processes :
Stop of Plug and Play Gateway Completed!!
admin#
```

pnp tech

To view the environment variables of the Cisco Plug and Play Gateway process, use the **pnp tech** command in privileged EXEC mode.

pnp tech

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco Prime Infrastructure 1.2	This command was introduced.
Cisco Prime Infrastructure 2.0	This command was modified.

Examples

The following is sample output from the **pnp tech** command:

```
admin# pnp tech

------------------------------------------
Cisco Prime Network Control System
Plug and Play
------------------------------------------
Environment variables
------------------------------------------
LOGMANAGER_OPTS=-DPNP_LOG_DIR=/var/log/KickStart -Dlog4j.configuration=log4j.properties
-DPNP_PROCESS_LOG=logmanager
MONITOR_PROCESS=com.cisco.pnp.ks.monitor.Monitor
NCS_PNP_WEB_DIR=/opt/CSCOlumos/tomcat/webapps/
PNP_VAR_INSTALL=/var/KickStart/install
GREP=grep
SETUP_FLAG_FILE=/var/KickStart/install/.setupRunning
PNP_ENABLE_AUTH=n
GREP_CMD=/bin/grep
SED_CMD=/bin/sed
KILL_CMD=/bin/kill
CNS_ENABLE_AUTO_PASS=y
TOMCAT_HOME=/opt/CSCOlumos/KickStart/tomcat
NCS_SERVER_CERTIFICATE=/root/server.crt
HTTPD_MODULES=/etc/httpd/modules
PNP_NCS_MOM_HOST_NAME=127.0.0.1
INIT_DIR=/etc/init.d
RPM_CMD=/bin/rpm
CNS_ENCRYPT_SERVER_TRUST_STORE=/var/KickStart/install/kickstart.truststore
PNP_DATA_BASE=/var
LN_CMD=/bin/ln -sf
CNS_MAX_NO_DEVICE_PER_PORT=500
PNP_ENABLE_DMZ=y
PNP_VAR_TOMCAT_LOG=/var/KickStart/tomcat/logs
MKDIR_CMD=/bin/mkdir -p
PNP_DEFAULT_NO_OF_PORT=5
PNP_CNS_EVENT_CMD=cns event bgl-pnp-dev1-ovf keepalive 120 2 reconnect 10
TOMCAT_SHUTDOWN_PORT=8005
NCS_PNP_WEBAPP_DIR=/opt/CSCOlumos/tomcat/conf/Catalina/localhost
PNP_HTTP_PORT=80
NCS_PROJECT_DISPLAY_NAME=Prime Infrastructure
DATE_CMD=/bin/date
PNP_LOG_FILE=/var/KickStart/install/pnp_start_stop.log
```

```
RM_CMD=/bin/rm -f
ECHO_CMD=/bin/echo -e
TERM=xterm
SHELL=NONE
PNP_NCS_LIB_DIR=/opt/CSCOlumos/lib/lib_pnp_ks
CNS_ENCRYPT_SERVER_KEY_STORE=/var/KickStart/install/kickstart.keystore
GREP_ENHANCED_CMD=/bin/grep -E
TAR_CMD=/bin/tar
ENV_CMD=/bin/env
SSH_CLIENT=10.21.84.117 54389 22
PNP_DATE_FORMAT=%Y%m%d%H%M%S
PNP_ENABLE_HTTPS=Y
CNS_GATEWAY_IP=
PNP_LOG_BASE=/var/log
PNP_MODJK_PACKAGE=mod_jk-ap20
CATALINA_BASE=/var/KickStart/tomcat
TOMCAT_VAR_DIR=/var/KickStart/tomcat
SE_ENABLED=0
HOST_NAME_SHORT_CMD=/bin/hostname -s
SSH_TTY=/dev/pts/1
PNP_WEBAPP_FILE=/var/KickStart/tomcat/conf/Catalina/localhost/cns.xml
PNP_VAR_TOMCAT=/var/KickStart/tomcat
PNP_CARSCLI_PACKAGE=PNPCARSCli
PNP_BIN=/opt/CSCOlumos/KickStart/bin
PNP_JAVA_VERSION=1.6
TOUCH_CMD=/bin/touch
CD_CMD=cd
USER=admin
PNP_IMAGE_TRANSFER_TIMEOUT=1200
CNS_NO_OF_PLAINTEXT_EVENTGW=5
CNS_NO_OF_CRYPTO_EVENTGW=5
PNP_DATA_IMAGE=/var/KickStart/image
PNP_ENABLE_SELF_SIGNED=y
PNP_ENABLE=Y
CPUFILE=/proc/cpuinfo
EVT_NCS_EVENT_PROTOCOL=ssl
PNP_VAR_HTTPD_CONF=/var/KickStart/httpd/conf
MORE_CMD=/bin/more
WGET_CMD_SSL=/usr/bin/wget --no-check-certificate
HEAD_CMD=/usr/bin/head
PNP_PROJECT_RPM_NAME=Lumos_PNP_Server
PNP_LOG_DIR=/var/log/KickStart
PNP_INSTALL_PREFIX=/opt/CSCOlumos
USERNAME_CMD=/usr/bin/id -un
IPTABLE=iptables
CNS_GATEWAY_OPTS=-DPNP_LOG_DIR=/var/log/KickStart -Dlog4j.configuration=cnslog4j.properties
PNP_ENABLE_EMBEDDED_FT=y
PNP_HTTPS_PORT=443
PNP_HTTPD_PACKAGE=httpd
PNP_IMAGE_ACTIVATION_TIMEOUT=600
PNP_ENABLE_AUTO_NCS=n
PNP_ENABLE_SSL=y
PNP_BACKUP_NAME=pnp_backup
SE_ENABLE_HTTPD_DIR=/usr/bin/chcon -Rv --type=httpd_sys_content_t
LOCAL_DISK_DIR=/localdisk
COREFILE=unlimited
PWD_CMD=pwd
MV_CMD=/bin/mv -f
PNP_STARTUP_FILE=/var/KickStart/install/cnsGatewayStartup.txt
MEMFILE=/proc/meminfo
PNP_CE_NG=n
MAIL=/var/mail/admin
PATH=/bin:/usr/bin:/sbin:/usr/sbin:/usr/local/bin:/usr/local/sbin:/opt/system/bin:/opt/system/lib:/opt/system/etc/carscli
IPTABLE_SAVE_CMD=service iptables save
IPTABLE_FILE=/etc/sysconfig/iptables
EVT_NCS_EVENT_PORT=61617
PNP_NCS=n
PNP_SETUP_LOG=/var/KickStart/install/setup.log
PNP_HTTPD_INIT_DIR=/opt/CSCOlumos/KickStart/httpd//etc/init.d
PNP_HOME=/opt/CSCOlumos/KickStart
IPTABLE_RESTART_CMD=service iptables restart
PNP_PRIMARY=y
EVT_MANAGER_PROCESS=com.cisco.pnp.ks.eventmanager.server.StartPNPKSMOMServer
```

```
EVT_MGR_EVENT_PORT=62616
PNP_VAR_HTTPD=/var/KickStart/httpd
PNP_SYSTEM_MONITOR_NAME=pnp_systemmonitor
PWD=/localdisk
JAVA_HOME=/usr/lib/jvm/java-1.6.0-sun-1.6.0.21.x86_64/jre
HTTP_SERVER_KEY=/var/KickStart/install/pnp_selfsigned_server.key
RPM_INSTALL_CMD=/bin/rpm -ivh
DF_CMD=/bin/df
CP_CMD=/bin/cp -f
NCS_TRUST_STORE=/opt/CSCOlumos/conf/truststore
DISKSIZE_CMD=/bin/df -lk
IPTABLE_ENABLE_TCP_PORT=/sbin/iptables -I INPUT -p tcp -j ACCEPT --dport
CAT_CMD=/bin/cat
NCS_KEY_STORE=/opt/CSCOlumos/conf/keystore
NETSTAT_CMD=/bin/netstat
PNP_SERVER_SSL_KEY=/var/KickStart/conf/server.key
PNP_HOST_NAME=bgl-pnp-dev1-ovf
RPM_REMOVE_CMD=/bin/rpm -e
TAIL_CMD=/bin/tail
PNP_SERVER_SSL_CERT=/var/KickStart/conf/server.crt
CATALINA_OPTS=-DPNP_LOG_DIR=/var/log/KickStart -DPNP_PROCESS_LOG=tomcat
CNS_ENABLE_PLAINTEXT=Y
HOST_NAME_FULL_CMD=/bin/hostname -f
NCS_PNP_WEBAPP_FILE=/opt/CSCOlumos/tomcat/conf/Catalina/localhost/cns.xml
PNP_FT_USERNAME=ciscopnp
PNP_PROJECT_NAME=KickStart
NETCONF_CMD=/sbin/ifconfig
AWK_CMD=/bin/awk
PNP_ENABLE_PORT_ALLOCATION=y
PNP_VAR_HTTPD_HTML=/var/KickStart/httpd/html
IPTABLE_STATUS_CMD=service iptables status
PNP_SHUTDOWN_FILE=/var/KickStart/install/cnsGatewayShutdown.txt
PNP_SERVER_IP=10.104.105.167
PNP_VAR_SERVICE=/var/KickStart/services
PNP_DEPLOYMENT_WEBAPP_FILE=/var/KickStart/tomcat/webapps/pnp-deployment-service.war
NCS_LOG_BASE=/opt/CSCOlumos/logs
PNP_VAR_CONF=/var/KickStart/conf
SHLVL=3
HOME=/home/admin
PNP_JAVA_OPTS=-DPNP_LOG_DIR=/var/log/KickStart -DPNP_PROCESS_LOG=tomcat
PNP_LIB=/opt/CSCOlumos/KickStart/lib
PS_CMD=/bin/ps
WGET_CMD=/usr/bin/wget
DIFF_CMD=/usr/bin/diff
EVT_MGR_OPTS=-DPNP_LOG_DIR=/var/log/KickStart -DPNP_PROCESS_LOG=evtmgr
HTTPD_CONF=/var/KickStart/httpd/conf
PNP_DATA_DIR=/var/KickStart
CUT_CMD=/bin/cut
PNP_DATA_TEMPLATE=/var/KickStart/template
PNP_PROJECT_RELEASE=1
MONITOR_OPTS=-DPNP_LOG_DIR=/var/log/KickStart -Dlog4j.configuration=monitorlog4j.properties
 -DPNP_PROCESS_LOG=monitor
TOMCAT_LOG_DIR=/var/log/KickStart/tomcat
SESTATUS_CMD=/usr/sbin/sestatus
OPENSSL_CMD=/usr/bin/openssl
LOGNAME=admin
PNP_NCS_CONTEXT_FILE=/opt/CSCOlumos/conf/pnp-ks-bean-context.xml
EVT_MGR_EVENT_PROTOCOL=tcp
PNP_END_PORT_STANDALONE=12010
DU_CMD=/usr/bin/du
CLASSPATH=:/var/KickStart/conf
NCS_PNP_DEPLOYMENT_WEBAPP_DIR=/opt/CSCOlumos/tomcat/webapps/pnp-deployment-service
IPTABLE_STOP_CMD=service iptables stop
PNP_PROJECT_VERSION=2.0.0.0
SSH_CONNECTION=10.21.84.117 54389 10.104.105.167 22
PNP_FT_PORT=21
PNP_PLAINTEXT_HTTPD=y
PNP_PROJECT_DISPLAY_NAME=PnP Gateway
PNP_START_PORT=11011
PNP_SETUP_COUNT=1
TOMCAT_AJP13_PORT=8009
MAXOPENFILE=4096
RPM_QUERY_PKG_CMD=/bin/rpm -qi
```

```
NCS_PROJECT_NAME=NCS
PNP_DATA=/var/KickStart
PNP_HOME_HTTPD=/opt/CSCOlumos/KickStart/httpd
CNS_TOTAL_EVENTGW=10
HTTP_SERVER_CERTIFICATE=/var/KickStart/install/pnp_self_signedserver.crt
EVT_MGR_EVENT_FAILOVER=y
LS_CMD=/bin/ls
NCS_INSTALL_PREFIX=/opt/CSCOlumos
NCS_PKG_NAME=LumosApp
PNP_LOG4J_OPTS=-DPNP_LOG_DIR=/var/log/KickStart
PNP_VAR_TOMCAT_CONF=/var/KickStart/tomcat/conf
PNP_VAR_DIR=/var/KickStart
SLEEP_CMD=/bin/sleep
PNP_IMAGE_DISTRIBUTION_TIMEOUT=1200
EVT_MGR_NETWORK_IP=10.104.105.167
RPM_FORCED_REMOVE_CMD=/bin/rpm -e --force --noscripts
PNP_LOG_LEVEL=warn
HTTPD_HOME=/usr
PNP_FT_PROTOCOL=ftp
CNS_GATEWAY_PROCESS=com.cisco.pnp.ks.cnsgateway.connection.ConnectionManagerBean
SE_DEL_HTTPD_MUTEX=/bin/rm -f -r /etc/httpd/logs/ssl_mutex*
PNP_END_PORT_NCS=11014
_=/bin/env
------------------------------------------
admin#
```

pnp tech log

To create a system-monitoring log file for the Cisco Plug and Play Gateway, use the **pnp tech log** command in privileged EXEC mode.

pnp tech log

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco Prime Infrastructure 1.2	This command was introduced.
Cisco Prime Infrastructure 2.0	This command was modified.

Usage Guidelines

The **pnp tech log** command creates a system-monitoring log file in a compressed tar format with the extension .pnp_systemmonitor.tar.gz.

Examples

The following is sample output from the **pnp tech log** command:

```
admin# pnp tech log

The System Status file created : /localdisk/20121003032209.pnp_systemmonitor.tar.gz
admin#
```

Note For more information on how to copy files from the local disk, see copy, on page 12 command.

show Commands

This section lists **show** commands. Each command includes a brief description of its use, any command defaults, command modes, usage guidelines, an example of the command syntax and any related commands.

show application

To show application information of the installed application packages on the system, use the **show application** command in EXEC mode.

show application [**status** | **version** [app_name]]

Syntax Description

status	Displays the status of the installed application.
version	Displays the application version for an installed application—the .
app_name	Name of the installed application.

Table 4: Output Modifier Variables for Count or Last

|	Output modifier variables: • *begin*—Matched pattern. Up to 80 alphanumeric characters. • *count*—Counts the number of lines in the output. Add number after the word *count*. |—Output modifier variables. • *end*—Ends with line that matches. Up to 80 alphanumeric characters. • *exclude*—Excludes lines that match. Up to 80 alphanumeric characters. • *include*—Includes lines that match. Up to 80 alphanumeric characters. • *last*—Displays last few lines of output. Add number after the word *last*. Up to 80 lines to display. Default 10. |—Output modifier variables (see Table A-8).

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

Example 1

```
pi-system/admin# show application
<name>          <Description>
NCS             Cisco Prime Infrastructure
pi-system/admin#
```

Related Commands

	Description
application start	Starts or enables an application.
application stop	Stops or disables an application.
application upgrade	Upgrades an application bundle.

show backup history

To display the backup history of the system, use the **show backup history** command in EXEC mode.

show backup history

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

Example 2

```
pi-common-133/admin# show restore log
Started at : Wed Feb 21 15:07:27 2018
Initiating restore.  Please wait...
  Restore Started at 02/21/18 15:07:27
  Stage 1 of 9: Transferring backup file ...
  -- completed at 02/21/18 15:07:57
  Stage 2 of 9: Decrypting backup file ...
  -- completed at  02/21/18 15:19:18
  Stage 3 of 9: Unpacking backup file ...
  -- completed at  02/21/18 15:19:20
  Stopping PI server ...
  Stage 4 of 9: Decompressing backup ...
  -- completed at  02/21/18 15:20:12
  Stage 5 of 9: Restoring Support Files ...
  -- completed at  02/21/18 15:20:33
  Stage 6 of 9: Restoring Database Files ...
   -- completed at  02/21/18 15:21:38
  Stage 7 of 9: Recovering Database ...
  -- completed at  02/21/18 15:39:52
  Stage 8 of 9: Updating Database Schema ...
    This could take long time based on the existing data size.
  -- completed at  02/21/18 16:20:51
  Stage 9 of 9: Re-enabling Database Settings ...
   -- completed at  02/21/18 16:38:33
   Total Restore duration is: 01h:31m:06s
INFO: Restore completed successfully.
System will reboot to enable FIPS and proceed with PI server startup
Finished at : Wed Feb 21 16:39:59 2018
pi-common-133/admin#
```

Examples

Example 3

```
pi-system/admin# sh backup history
backup history is empty
pi-system/admin#
```

Related Commands

Command	Description
backup	Performs a backup (and Cisco ADE OS) and places the backup in a repository.
restore	Restores from backup the file contents of a specific repository.
repository	Enters the repository submode for configuration of backups.
show repository	Displays the available backup files located on a specific repository.

show banner pre-login

To display the banner that you installed, use the **show banner pre-login** command in EXEC mode.

show banner pre-login

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

Example 1

```
pi-system/admin# show banner pre-login
No pre-login banner installed
pi-system/admin#
```

Example 2

```
pi-system/admin# show banner pre-login
Banner-Test
pi-system/admin#
```

Related Commands

Command	Description
banner, on page 9	Enables you to install a pre-login banner.

show cdp

To display information about the enabled Cisco Discovery Protocol interfaces, use the **show cdp** command in EXEC mode.

show cdp {**all** | **neighbors**}

Syntax Description

all	Shows all of the enabled Cisco Discovery Protocol interfaces.
neighbors	Shows the Cisco Discovery Protocol neighbors.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

Example 1

```
ncs/admin# show cdp all
CDP protocol is enabled ...
        broadcasting interval is every 60 seconds.
        time-to-live of cdp packets is 180 seconds.

        CDP is enabled on port GigabitEthernet0.
ncs/admin#
```

Example 2

```
ncs/admin# show cdp neighbors
CDP Neighbor : 000c297840e5
        Local Interface    : GigabitEthernet0
        Device Type        : L-NCS-1.0-50
        Port               : eth0
        Address            : 172.23.90.114

CDP Neighbor : isexp-esw5
        Local Interface    : GigabitEthernet0
        Device Type        : cisco WS-C3560E-24TD
        Port               : GigabitEthernet0/5
        Address            : 172.23.90.45

CDP Neighbor : 000c29e29926
        Local Interface    : GigabitEthernet0
        Device Type        : L-NCS-1.0-50
        Port               : eth0
        Address            : 172.23.90.115

CDP Neighbor : 000c290fba98
        Local Interface    : GigabitEthernet0
        Device Type        : L-NCS-1.0-50
        Port               : eth0
        Address            : 172.23.90.111

ncs/admin#
```

Related Commands

Command	Description
cdp holdtime	Specifies the length of time that the receiving device should hold a Cisco Discovery Protocol packet from your router before discarding it.
cdp run	Enables the Cisco Discovery Protocol.
cdp timer	Specifies how often the server sends Cisco Discovery Protocol updates.

show clock

To display the day, month, date, time, time zone, and year of the system software clock, use the **show clock** command in EXEC mode.

show clock

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

```
ncs/admin# show clock
Fri Aug  6 10:46:39 UTC 2010
ncs/admin#
```

Note The **show clock** output in the previous example includes Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT), Great Britain, or Zulu time (see Tables A-16, Table 8: Australia Time Zones, and Table 9: Asia Time Zones on pages A-84 and A-85 for sample time zones).

Related Commands

Command	Description
clock	Sets the system clock for display purposes.

show cpu

To display CPU information, use the **show cpu** command in EXEC mode.

show cpu [statistics] [|] [|]

Syntax Description

<table>
<tr><td>statistics</td><td>Displays CPU statistics.</td></tr>
<tr><td>|</td><td>Output modifier variables:
• <i>begin</i>—Matched pattern. Up to 80 alphanumeric characters.
• <i>count</i>—Counts the number of lines in the output. Add number after the word <i>count</i>.
|—Output modifier variables (see Table A-9).
• <i>end</i>—Ends with line that matches. Up to 80 alphanumeric characters.
• <i>exclude</i>—Excludes lines that match. Up to 80 alphanumeric characters.
• <i>include</i>—Includes lines that match. Up to 80 alphanumeric characters.
• <i>last</i>—Displays last few lines of output. Add number after the word <i>last</i>. Up to 80 lines to display. Default 10.
|—Output modifier variables (see Table A-9).</td></tr>
</table>

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

Example 1

```
ncs/admin# show cpu

processor : 0
model     : Intel(R) Xeon(R) CPU           E5320  @ 1.86GHz
speed(MHz): 1861.914
cache size: 4096 KB

ncs/admin#
```

Example 2

```
ncs/admin# show cpu statistics
user time:              265175
kernel time:            166835
idle time:             5356204
i/o wait time:          162676
irq time:                 4055

ncs/admin#
```

Related Commands

Command	Description
show disks	Displays the system information of all disks.
show memory	Displays the amount of system memory that each system process uses.

show disks

To display the disks file-system information, use the **show disks** command in EXEC mode.

show disks [|] [|]

Syntax Description

|	Output modifier variables: • *begin*—Matched pattern. Up to 80 alphanumeric characters. • *count*—Counts the number of lines in the output. Add number after the word *count*. |—Output modifier variables (see Table A-10). • *end*—Ends with line that matches. Up to 80 alphanumeric characters. • *exclude*—Excludes lines that match. Up to 80 alphanumeric characters. • *include*—Includes lines that match. Up to 80 alphanumeric characters. • *last*—Displays last few lines of output. Add number after the word *last*. Up to 80 lines to display. Default 10. |—Output modifier variables (see Table A-10).

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Only platforms that have a disk file system support the **show disks** command.

Examples

```
ncs/admin# show disks

temp. space 2% used (17828 of 988116)
disk: 3% used (143280 of 5944440)

Internal filesystems:
  all internal filesystems have sufficient free space

ncs/admin#
```

Related Commands

Command	Description
show cpu	Displays CPU information.
show memory	Displays the amount of system memory that each system process uses.

show icmp_status

To display the Internet Control Message Protocol echo response configuration information, use the **show icmp_status** command in EXEC mode.

show icmp_status {> file | |}

Syntax Description

>	Output direction.
file	Name of file to redirect standard output (stdout).
|	Output modifier commands: • *begin*—Matched pattern. Up to 80 alphanumeric characters. • *count*—Counts the number of lines in the output. Add number after the word count. ◦ |—Output modifier commands (see Table A-11). • *end*—Ends with line that matches. Up to 80 alphanumeric characters. • *exclude*—Excludes lines that match. Up to 80 alphanumeric characters. • *include*—Includes lines that match. Up to 80 alphanumeric characters. • last—Displays last few lines of output. Add number after the word last. Up to 80 lines to display. Default 10. ◦ |—Output modifier commands (see Table A-11).

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

Example 1

```
ncs/admin# show icmp_status
icmp echo response is turned on
ncs/admin#
```

Example 2

```
ncs/admin# show icmp_status
icmp echo response is turned off
ncs/admin#
```

Related Commands

Command	Description
icmp echo	Configures the Internet Control Message Protocol (ICMP) echo requests.

show ip route

To display details the ip route details of the application, use **show ip route** command in EXEC mode.

show ip route {| |}

Syntax Description

>	Output redirection
|	Output modifiers

Command Default

No default behaviour.

Command Modes

EXEC

Examples

```
ncs/admin# show ip route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.126.168.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
0.0.0.0         10.126.168.1    0.0.0.0         UG    0      0        0 eth0
Kernel IPv6 routing table
Destination                                 Next Hop                                Flags
Metric Ref    Use Iface
2001::/64                                   ::                                      UA
256    0        0 eth0
fe80::/64                                   ::                                      U
256    0        0 eth0
::/0                                        fe80::217:dfff:fe29:9800                UGDA
1024   18       0 eth0
::1/128                                     ::                                      U
0      10127       1 lo
2001::20c:29ff:fe6c:8f28/128                ::                                      U
0      0        1 lo
2001::813d:2d75:7d6:564f/128                ::                                      U
0      37       1 lo
2001::d992:4889:c9e1:f238/128               ::                                      U
0      0        1 lo
fe80::20c:29ff:fe6c:8f28/128                ::                                      U
0      3        1 lo
ff00::/8
```

show interface

To display the usability status of interfaces configured for IP, use the **show interface** command in EXEC mode.

show interface [GigabitEthernet] |

Syntax Description

<table>
<tr><td>GigabitEthernet</td><td>Shows the Gigabit Ethernet interface. Either 0 or 1.</td></tr>
<tr><td>|</td><td>Output modifier variables:
• <i>begin</i>—Matched pattern. Up to 80 alphanumeric characters.
• <i>count</i>—Counts the number of lines in the interface. Add number after the word <i>count</i>.
• <i>end</i>—Ends with line that matches. Up to 80 alphanumeric characters.
• <i>exclude</i>—Excludse lines that match. Up to 80 alphanumeric characters.
• <i>include</i>—Includes lines that match. Up to 80 alphanumeric characters.
• <i>last</i>—Displays last few lines of output. Add number after the word <i>last</i>. Up to 80 lines to display. Default 10.</td></tr>
</table>

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

In the **show interface GigabitEthernet 0** output, you can find that the interface has three IPv6 addresses. The first internet address (starting with 3ffe) is the result of using stateless autoconfiguration. For this to work, you need to have IPv6 route advertisement enabled on that subnet. The next address (starting with fe80) is a link local address that does not have any scope outside the host. You always see a link local address regardless of the IPv6 autoconfiguration or DHCPv6 configuration. The last address (starting with 2001) is the result obtained from an IPv6 DHCP server.

Examples

Example 1

```
ncs/admin# show interface
eth0      Link encap:Ethernet  HWaddr 00:0C:29:6A:88:C4
          inet addr:172.23.90.113  Bcast:172.23.90.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe6a:88c4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:48536 errors:0 dropped:0 overruns:0 frame:0
          TX packets:14152 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6507290 (6.2 MiB)  TX bytes:12443568 (11.8 MiB)
          Interrupt:59 Base address:0x2000
```

```
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1195025 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1195025 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:649425800 (619.3 MiB)  TX bytes:649425800 (619.3 MiB)

sit0      Link encap:IPv6-in-IPv4
          NOARP  MTU:1480  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

ncs/admin#
```

Example 2

```
ncs/admin# show interface GigabitEthernet 0
eth0      Link encap:Ethernet  HWaddr 00:0C:29:AF:DA:05
          inet addr:172.23.90.116  Bcast:172.23.90.255  Mask:255.255.255.0
          inet6 addr: 3ffe:302:11:2:20c:29ff:feaf:da05/64 Scope:Global
          inet6 addr: fe80::20c:29ff:feaf:da05/64 Scope:Link
          inet6 addr: 2001:558:ff10:870:8000:29ff:fe36:200/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:77848 errors:0 dropped:0 overruns:0 frame:0
          TX packets:23131 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10699801 (10.2 MiB)  TX bytes:3448374 (3.2 MiB)
          Interrupt:59 Base address:0x2000
```

Related Commands

Command	Description
interface	Configures an interface type and enters the interface configuration submode.
ipv6 address autoconfig	Enables IPv6 stateless autoconfiguration on an interface.
ipv6 address dhcp	Enables IPv6 address DHCP on an interface.

show inventory

To display information about the hardware inventory, including the appliance model and serial number, use the **show inventory** command in EXEC mode.

show inventory |

Syntax Description

|	Output modifier variables: • *begin*—Matched pattern. Up to 80 alphanumeric characters. • *count*—Counts the number of lines in the interface. Add number after the word *count*. • *end*—Ends with line that matches. Up to 80 alphanumeric characters. • *exclude*—Excludse lines that match. Up to 80 alphanumeric characters. • *include*—Includes lines that match. Up to 80 alphanumeric characters. • *last*—Displays last few lines of output. Add number after the word *last*. Up to 80 lines to display. Default 10.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

```
pi-system/admin# show inventory

NAME: "Cisco-VM chassis", DESCR: "Cisco-VM chassis"
PID: Cisco-VM-SPID     , VID: V01 , SN: GITQA6QC26B
Total RAM Memory: 12167972 kB
CPU Core Count: 4
CPU 0: Model Info: Intel(R) Xeon(R) CPU E5-4640 0 @ 2.40GHz
CPU 1: Model Info: Intel(R) Xeon(R) CPU E5-4640 0 @ 2.40GHz
CPU 2: Model Info: Intel(R) Xeon(R) CPU E5-4640 0 @ 2.40GHz
CPU 3: Model Info: Intel(R) Xeon(R) CPU E5-4640 0 @ 2.40GHz
Hard Disk Count(*): 1
Disk 0: Device Name: /dev/sda
Disk 0: Capacity: 322.10 GB
Disk 0: Geometry: 255 heads 63 sectors/track 39162 cylinders
NIC Count: 1
NIC 0: Device Name: eth0
NIC 0: HW Address: 00:0C:29:11:51:83
NIC 0: Driver Descr: e1000: eth0: e1000_probe: Intel(R) PRO/1000 Network Connection

(*) Hard Disk Count may be Logical.
pi-system-61/admin#
```

show logging

To display the state of system logging (syslog) and the contents of the standard system logging buffer, use the **show logging** command in EXEC mode.

show logging {**application** [*application-name*]} {**internal**} {**system**} |

Syntax Description

application	Displays application logs.
application-name	Application name. Up to 255 alphanumeric characters. • *tail*—Tail system syslog messages. • *count*—Tail last count messages. From 0 to 4,294,967,295. |—Output modifier variables (see below).
internal	Displays the syslogs configuration.
system	Displays the system syslogs.
|	Output modifier variables: • *begin*—Matched pattern. Up to 80 alphanumeric characters. • *count*—Counts the number of lines in the interface. Add number after the word *count*. • *end*—Ends with line that matches. Up to 80 alphanumeric characters. • *exclude*—Excludes lines that match. Up to 80 alphanumeric characters. • *include*—Includes lines that match. Up to 80 alphanumeric characters. • *last*—Displays last few lines of output. Add number after the word *last*. Up to 80 lines to display. Default 10.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

This command displays the state of syslog error and event logging, including host addresses, and for which, logging destinations (console, monitor, buffer, or host) logging is enabled.

Examples

Example 1

```
ncs/admin# show logging system
```

```
ADEOS Platform log:
-----------------

Aug  5 10:44:32 localhost debugd[1943]: [16618]: config:network: main.c[252] [setup]: Setup
 is complete
Aug  5 10:45:02 localhost debugd[1943]: [17291]: application:install cars_install.c[242]
[setup]: Install initiated with bundle - ncs.tar.gz,
repo - SystemDefaultPkgRepos
Aug  5 10:45:02 localhost debugd[1943]: [17291]: application:install cars_install.c[256]
[setup]: Stage area - /storeddata/Installing/.1281030
302
Aug  5 10:45:02 localhost debugd[1943]: [17291]: application:install cars_install.c[260]
[setup]: Getting bundle to local machine
Aug  5 10:45:03 localhost debugd[1943]: [17291]: transfer: cars_xfer.c[58] [setup]: local
copy in of ncs.tar.gz requested
Aug  5 10:45:46 localhost debugd[1943]: [17291]: application:install cars_install.c[269]
[setup]: Got bundle at - /storeddata/Installing/.1281
030302/ncs.tar.gz
Aug  5 10:45:46 localhost debugd[1943]: [17291]: application:install cars_install.c[279]
[setup]: Unbundling package ncs.tar.gz
Aug  5 10:47:06 localhost debugd[1943]: [17291]: application:install cars_install.c[291]
[setup]: Unbundling done. Verifying input parameters.
..
Aug  5 10:47:06 localhost debugd[1943]: [17291]: application:install cars_install.c[313]
[setup]: Manifest file is at - /storeddata/Installing
/.1281030302/manifest.xml
Aug  5 10:47:07 localhost debugd[1943]: [17291]: application:install cars_install.c[323]
[setup]: Manifest file appname - ncs
Aug  5 10:47:09 localhost debugd[1943]: [17291]: application:install cars_install.c[386]
[setup]: Manifest file pkgtype - CARS
Aug  5 10:47:09 localhost debugd[1943]: [17291]: application:install cars_install.c[398]
[setup]: Verify dependency list -
Aug  5 10:47:09 localhost debugd[1943]: [17291]: application:install cars_install.c[410]
[setup]: Verify app license -
Aug  5 10:47:09 localhost debugd[1943]: [17291]: application:install cars_install.c[420]
[setup]: Verify app RPM's
Aug  5 10:47:09 localhost debugd[1943]: [17291]: application:install cars_install.c[428]
[setup]: No of RPM's - 9
Aug  5 10:47:09 localhost debugd[1943]: [17291]: application:install cars_install.c[439]
[setup]: Disk - 50
Aug  5 10:47:09 localhost debugd[1943]: [17291]: application:install ci_util.c[325] [setup]:
 Disk requested = 51200 KB
Aug  5 10:47:09 localhost debugd[1943]: [17291]: application:install ci_util.c[345] [setup]:
 More disk found Free = 40550400, req_disk = 51200
Aug  5 10:47:09 localhost debugd[1943]: [17291]: application:install cars_install.c[450]
[setup]: Mem requested by app - 100
Aug  5 10:47:09 localhost debugd[1943]: [17291]: application:install ci_util.c[369] [setup]:
 Mem requested = 102400
Aug  5 10:47:09 localhost debugd[1943]: [17291]: application:install ci_util.c[384] [setup]:
 Found MemFree = MemFree:         13028 kB
Aug  5 10:47:09 localhost debugd[1943]: [17291]: application:install ci_util.c[390] [setup]:
 Found MemFree value = 13028
Aug  5 10:47:09 localhost debugd[1943]: [17291]: application:install ci_util.c[393] [setup]:
 Found Inactive = Inactive:       948148 kB
Aug  5 10:47:09 localhost debugd[1943]: [17291]: application:install ci_util.c[399] [setup]:
 Found Inactive MemFree value = 948148
Aug  5 10:47:09 localhost debugd[1943]: [17291]: application:install ci_util.c[409] [setup]:
 Sufficient mem found
Aug  5 10:47:09 localhost debugd[1943]: [17291]: application:install ci_util.c[415] [setup]:
 Done checking memory...
Aug  5 10:47:09 localhost debugd[1943]: [17291]: application:install cars_install.c[461]
[setup]: Verifying RPM's...
--More--
(press Spacebar to continue)
```

Example 2

```
ncs/admin# show logging internal

log server:          localhost
Global loglevel:     6
Status:              Enabled
ncs/admin#
```

Example 3

```
ncs/admin# show logging internal

log server:          localhost
Global loglevel:     6
Status:              Disabled
ncs/admin#
```

show logins

To display the state of system logins, use the **show logins** command in EXEC mode.

show logins cli

Syntax Description

cli	Lists the **cli** login history.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Requires the **cli** keyword; otherwise, an error occurs.

Examples

```
ncs/admin# show logins cli
admin    pts/0        10.77.137.60     Fri Aug  6 09:45   still logged in
admin    pts/0        10.77.137.60     Fri Aug  6 08:56 - 09:30  (00:33)
admin    pts/0        10.77.137.60     Fri Aug  6 07:17 - 08:43  (01:26)
reboot   system boot  2.6.18-164.el5PA Thu Aug  5 18:17          (17:49)
admin    tty1                          Thu Aug  5 18:15 - down   (00:00)
reboot   system boot  2.6.18-164.el5PA Thu Aug  5 18:09          (00:06)
setup    tty1                          Thu Aug  5 17:43 - 18:07  (00:24)
reboot   system boot  2.6.18-164.el5PA Thu Aug  5 16:05          (02:02)

wtmp begins Thu Aug  5 16:05:36 2010

ncs/admin#
```

show memory

To display the memory usage of all of the running processes, use the **show memory** command in EXEC mode.

show memory

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

```
ncs/admin# show memory
total memory:    1035164 kB
free memory:       27128 kB
cached:           358888 kB
swap-cached:      142164 kB

ncs/admin#
```

show netstat

To display statistics about your network connection, use **show netstat** command in EXEC mode.

show netstat{ > | | }

Syntax Description

>	Output redirection.
|	Output modifiers.

Command Default

No default behavior.

Command Modes

EXEC

Examples

```
ncs/admin# show netstat
TCP Listeners ------------------------------------------------------------
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 0.0.0.0:65000               0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:39949               0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:111                 0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:2000              0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:6100                0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:21                  0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:22                  0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:2012                0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:2013                0.0.0.0:*                   LISTEN
tcp        0      0 :::61603                    :::*                        LISTEN
tcp        0      0 :::10755                    :::*                        LISTEN
tcp        0      0 :::61604                    :::*                        LISTEN
tcp        0      0 :::31204                    :::*                        LISTEN
tcp        0      0 :::9992                     :::*                        LISTEN
tcp        0      0 :::65000                    :::*                        LISTEN
tcp        0      0 :::8009                     :::*                        LISTEN
tcp        0      0 :::5001                     :::*                        LISTEN
tcp        0      0 :::1199                     :::*                        LISTEN
tcp        0      0 :::111                      :::*                        LISTEN
tcp        0      0 :::80                       :::*                        LISTEN
tcp        0      0 :::35088                    :::*                        LISTEN
tcp        0      0 :::21648                    :::*                        LISTEN
tcp        0      0 :::16113                    :::*                        LISTEN
tcp        0      0 :::2001                     :::*                        LISTEN
tcp        0      0 :::61617                    :::*                        LISTEN
tcp        0      0 :::1522                     :::*                        LISTEN
tcp        0      0 :::8082                     :::*                        LISTEN
tcp        0      0 :::6100                     :::*                        LISTEN
tcp        0      0 :::21                       :::*                        LISTEN
tcp        0      0 :::22                       :::*                        LISTEN
tcp        0      0 :::48504                    :::*                        LISTEN
tcp        0      0 :::443                      :::*                        LISTEN
tcp        0      0 :::10555                    :::*                        LISTEN

TCP Connections ----------------------------------------------------------
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 10.126.168.61:22            10.65.57.243:55027          ESTABLISHED
```

show ntp

To show the status of the NTP associations, use the **show ntp** command in EXEC mode.

show ntp

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC ncs/admin# show ntp pi-system-241/admin# show ntp NTP Server 1 : 10.81.254.202 NTP Server 2 : 10.64.58.50 synchronised to NTP server (10.81.254.202) at stratum 2 time correct to within 173 ms polling server every 1024 s remote refid st t when poll reach delay offset jitter === === ==== *10.81.254.202 .GPS. 1 u 255 1024 377 272.081 1.756 1.850 +10.64.58.50 10.67.68.33 2 u 27 1024 377 0.388 -0.936 1.904 Warning: Output results may conflict during periods of changing synchronization.

Related Commands

Command	Description
ntp server	Allows synchronization of the software clock by the NTP server for the system.

show ports

To display information about all of the processes listening on active ports, use the **show ports** command in EXEC mode.

show ports [|] [|]

Syntax Description

|	Output modifier variables: • *begin*—Matched pattern. Up to 80 alphanumeric characters. • *count*—Counts the number of lines in the interface. Add number after the word *count*. |—Output modifier variables (see Table A-12). • *end*—Ends with line that matches. Up to 80 alphanumeric characters. • *exclude*—Excludes lines that match. Up to 80 alphanumeric characters. • *include*—Includes lines that match. Up to 80 alphanumeric characters. • *last*—Displays last few lines of output. Add number after the word *last*. Up to 80 lines to display. Default 10. |—Output modifier variables (see Table A-12).

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

When you run the **show ports** command, the port must have an associated active session.

Examples

```
ncs/admin# show ports
Process : timestensubd (21372)
     tcp: 127.0.0.1:11298
Process : timestenorad (21609)
     tcp: 127.0.0.1:51715
     udp: ::1:28314, ::1:59055, ::1:45113, ::1:49082, ::1:64737, ::1:62570, ::1:19577,
::1:29821
Process : ttcserver (21382)
     tcp: 127.0.0.1:16612, 0.0.0.0:53385
Process : timestenrepd (21579)
     tcp: 127.0.0.1:62504, 0.0.0.0:18047
     udp: ::1:51436
Process : timestend (21365)
     tcp: 0.0.0.0:53384
Process : rpc.statd (2387)
     tcp: 0.0.0.0:873
     udp: 0.0.0.0:867, 0.0.0.0:870
Process : timestensubd (21373)
     tcp: 127.0.0.1:43407
```

```
Process : portmap (2350)
     tcp: 0.0.0.0:111
     udp: 0.0.0.0:111
Process : Decap_main (21468)
     tcp: 0.0.0.0:2000
     udp: 0.0.0.0:9993
Process : timestensubd (21369)
     tcp: 127.0.0.1:37648
Process : timestensubd (21374)
     tcp: 127.0.0.1:64211
Process : sshd (2734)
     tcp: 172.23.90.113:22
Process : java (21432)
    tcp: 127.0.0.1:8888, :::2080, :::2020, ::ffff:127.0.0.1:8005, :::8009, :::8905, :::8010,
 :::2090, :::1099, :::9999, :::61616, :::8080, ::
:80, :::60628, :::8443, :::443
    udp: 0.0.0.0:1812, 0.0.0.0:1813, 0.0.0.0:1700, 0.0.0.0:10414, 0.0.0.0:3799, 0.0.0.0:1645,
 0.0.0.0:1646, :::8905, :::8906
Process : monit (21531)
     tcp: 127.0.0.1:2812
Process : java (21524)
     tcp: :::62627
Process : java (21494)
     tcp: ::ffff:127.0.0.1:20515
     udp: 0.0.0.0:20514
Process : tnslsnr (21096)
     tcp: :::1521
Process : ora_d000_ncs1 (21222)
     tcp: :::26456
     udp: ::1:63198
Process : ntpd (2715)
     udp: 172.23.90.113:123, 127.0.0.1:123, 0.0.0.0:123, ::1:123, fe80::20c:29ff:fe6a:123,
 :::123
Process : ora_pmon_ncs1 (21190)
     udp: ::1:51994
Process : ora_mmon_ncs1 (21218)
     udp: :::38941
Process : ora_s000_ncs1 (21224)
     udp: ::1:49864

ncs/admin#
```

show process

To display information about active processes, use the **show process** command in the EXEC mode.

show process |

Syntax Description

<table>
<tr><td>|</td><td>(Optional) Output modifier variables:
• <i>begin</i>—Matched pattern. Up to 80 alphanumeric characters.
• <i>count</i>—Counst the number of lines in the interface. Add number after the word <i>count</i>.
• <i>end</i>—Ends with line that matches. Up to 80 alphanumeric characters.
• <i>exclude</i>—Excludes lines that match. Up to 80 alphanumeric characters.
• <i>include</i>—Includes lines that match. Up to 80 alphanumeric characters.
• <i>last</i>—Displays last few lines of output. Add number after the word <i>last</i>. Up to 80 lines to display. Default 10.</td></tr>
</table>

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

```
/admin# show process
USER       PID     TIME TT       COMMAND
root         1 00:00:02 ?        init
root         2 00:00:00 ?        migration/0
root         3 00:00:00 ?        ksoftirqd/0
root         4 00:00:00 ?        watchdog/0
root         5 00:00:00 ?        events/0
root         6 00:00:00 ?        khelper
root         7 00:00:00 ?        kthread
root        10 00:00:01 ?        kblockd/0
root        11 00:00:00 ?        kacpid
root       170 00:00:00 ?        cqueue/0
root       173 00:00:00 ?        khubd
root       175 00:00:00 ?        kseriod
root       239 00:00:32 ?        kswapd0
root       240 00:00:00 ?        aio/0
root       458 00:00:00 ?        kpsmoused
root       488 00:00:00 ?        mpt_poll_0
root       489 00:00:00 ?        scsi_eh_0
root       492 00:00:00 ?        ata/0
root       493 00:00:00 ?        ata_aux
root       500 00:00:00 ?        kstriped
root       509 00:00:07 ?        kjournald
root       536 00:00:00 ?        kauditd
root       569 00:00:00 ?        udevd
root      1663 00:00:00 ?        kmpathd/0
root      1664 00:00:00 ?        kmpath_handlerd
root      1691 00:00:00 ?        kjournald
root      1693 00:00:00 ?        kjournald
root      1695 00:00:00 ?        kjournald
root      1697 00:00:00 ?        kjournald
root      2284 00:00:00 ?        auditd
root      2286 00:00:00 ?        audispd
root      2318 00:00:10 ?        debugd
rpc       2350 00:00:00 ?        portmap
root      2381 00:00:00 ?        rpciod/0

pi-admin/admin#
```

Table 5: Show Process Field Descriptions

Field	Description
USER	Logged-in user.
PID	Process ID.
TIME	The time that the command was last used.
TT	Terminal that controls the process.
COMMAND	Type of process or command used.

show repository

To display the file contents of the repository, use the **show repository** command in EXEC mode.

show repository repository-name

Syntax Description

repository-name	Name of the repository whose contents you want to view. Up to 30 alphanumeric characters.

Command Default

No default behavior or values.

Command Modes

EXEC

Related Commands

Command	Description
backup	Performs a backup (and Cisco ADE OS) and places the backup in a repository.
restore	Restores from backup the file contents of a specific repository.
repository	Enters the repository submode for configuration of backups.
show backup history	Displays the backup history of the system.

show restore

To display the restore history, use the **show restore** command in EXEC mode.

show restore {**history**}

Syntax Description

history	Displays the restore history.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

```
pi-common-133/admin# show restore history
Wed Feb 21 16:39:50 IST 2018: restore                                               \
pi-common-241-171216-0330__VER2.2.0.0.158_BKSZ91G_FIPS_ON_CPU16_MEM4G_RAM15G_SWAP15G\
_APP_CK201773545.tar.gpg from repository defaultRepo: success
pi-common-133/admin#
Page No: 167
Show restore log examples can be changed:
pi-common-133/admin# show restore log
Started at : Wed Feb 21 15:07:27 2018
Initiating restore.  Please wait...
  Restore Started at 02/21/18 15:07:27
  Stage 1 of 9: Transferring backup file ...
  -- completed at 02/21/18 15:07:57
  Stage 2 of 9: Decrypting backup file ...
  -- completed at  02/21/18 15:19:18
  Stage 3 of 9: Unpacking backup file ...
  -- completed at  02/21/18 15:19:20
  Stopping PI server ...
  Stage 4 of 9: Decompressing backup ...
  -- completed at  02/21/18 15:20:12
  Stage 5 of 9: Restoring Support Files ...
  -- completed at  02/21/18 15:20:33
  Stage 6 of 9: Restoring Database Files ...
   -- completed at  02/21/18 15:21:38
  Stage 7 of 9: Recovering Database ...
  -- completed at  02/21/18 15:39:52
  Stage 8 of 9: Updating Database Schema ...
    This could take long time based on the existing data size.
  -- completed at  02/21/18 16:20:51
  Stage 9 of 9: Re-enabling Database Settings ...
   -- completed at  02/21/18 16:38:33
   Total Restore duration is: 01h:31m:06s
INFO: Restore completed successfully.
System will reboot to enable FIPS and proceed with PI server startup
Finished at : Wed Feb 21 16:39:59 2018
pi-common-133/admin#
```

Related Commands

Command	Description
backup	Performs a backup (and Cisco ADE OS) and places the backup in a repository.

Command	Description
restore	Restores from backup the file contents of a specific repository.
repository	Enters the repository submode for configuration of backups.
show backup history	Displays the backup history of the system.

show restore log

To display the last restore operation in the case of Auto logout console, use the **show restore log** command in EXEC mode. You can run this command even while performing a restore operation and a successful restore operation.

show restore log

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

Example 1

```
pi-system/admin# show restore log
No restore log available
pi-system/admin#
```

Examples

Example 2

```
pi-system/admin# show restore log
Started at : Tue Nov 14 13:10:09 2017
Initiating restore.  Please wait...
  Restore Started at 11/14/17 13:10:09
  Stage 1 of 9: Transferring backup file ...
  -- completed at 11/14/17 13:10:41
  Stage 2 of 9: Decrypting backup file ...
  -- completed at  11/14/17 13:21:30
  Stage 3 of 9: Unpacking backup file ...
  -- completed at  11/14/17 13:21:33
  Stopping PI server ...
  Stage 4 of 9: Decompressing backup ...
  -- completed at  11/14/17 13:23:29
  Stage 5 of 9: Restoring Support Files ...
  -- completed at  11/14/17 13:24:06
  Stage 6 of 9: Restoring Database Files ...
   -- completed at  11/14/17 13:24:40
  Stage 7 of 9: Recovering Database ...
  -- completed at  11/14/17 13:38:12
  Stage 8 of 9: Updating Database Schema ...
    This could take long time based on the existing data size.
  -- completed at  11/14/17 14:35:04
  Stage 9 of 9: Re-enabling Database Settings ...
   -- completed at  11/14/17 14:49:28
   Total Restore duration is: 01h:39m:19s
INFO: Restore completed successfully.
Starting Prime Infrastructure...
This may take a while (10 minutes or more) ...
Prime Infrastructure started successfully.
Completed in 988 seconds
Finished at : Tue Nov 14 15:07:01 2017
pi-system-123/admin#
```

Related Commands

Command	Description
restore	Restores from backup the file contents of a specific repository.

show running-config

To display the contents of the currently running configuration file or the configuration, use the **show running-config** command in EXEC mode.

showrunning-config

Syntax Description

This command has no arguments or keywords.

Command Default

The **show running-config** command displays all of the configuration information.

Command Modes

EXEC

Examples

```
ncs/admin# show running-config
Generating configuration...
!
hostname ncs
!
ip domain-name cisco.com
!
interface GigabitEthernet 0
  ip address 172.23.90.113 255.255.255.0
  ipv6 address autoconfig
!
ip name-server 172.16.168.183
!
ip default-gateway 172.23.90.1
!
clock timezone UTC
!
ntp server time.nist.gov
!
username admin password hash $1$JbbHvKVG$xMZ/XL4tH15Knf.FfcZZr. role admin
!
service sshd
!
password-policy
  lower-case-required
  upper-case-required
  digit-required
  no-username
  disable-cisco-passwords
  min-password-length 6
!
logging localhost
logging loglevel 6
!
cdp timer 60
cdp holdtime 180
cdp run GigabitEthernet 0
!
icmp echo on
!

ncs/admin#
```

Related Commands

Command	Description
configure	Enters configuration mode.
show startup-config	Displays the contents of the startup configuration file or the configuration.

show startup-config

To display the contents of the startup configuration file or the configuration, use the **show startup-config** command in EXEC mode.

showstartup-config

Syntax Description

This command has no arguments or keywords.

Command Default

The **show startup-config** command displays all of the startup configuration information.

Command Modes

EXEC

Examples

```
ncs/admin# show startup-config
!
hostname ncs
!
ip domain-name cisco.com
!
interface GigabitEthernet 0
  ip address 172.23.90.113 255.255.255.0
  ipv6 address autoconfig
!
ip name-server 172.16.168.183
!
ip default-gateway 172.23.90.1
!
clock timezone UTC
!
ntp server time.nist.gov
!
username admin password hash $1$JbbHvKVG$xMZ/XL4tH15Knf.FfcZZr. role admin
!
service sshd
!
password-policy
  lower-case-required
  upper-case-required
  digit-required
  no-username
  disable-cisco-passwords
  min-password-length 6
!
logging localhost
logging loglevel 6
!
cdp timer 60
cdp holdtime 180
cdp run GigabitEthernet 0
!
icmp echo on
!
ncs/admin#
```

Related Commands

Command	Description
configure	Enters configuration mode.
show running-config	Displays the contents of the currently running configuration file or the configuration.

show security-status

To display the security-related configuration information, use the **show security-status** command in EXEC mode.

show security-status

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

Example

```
pi-system-120/admin# show security-status
Open TCP Ports  : 22 443 1522 8082 9992
Open UDP Ports  : 162 500 514 9991

FIPS Mode       : enabled
Non-FIPS ssh client ciphers: disabled

TFTP Service    : disabled
FTP Service     : disabled

JMS port(61617) : disabled
Root Access     : enabled

TLS versions    : TLSv1.2
TLS ciphers     : tls-ecdhe,tls-dhe,tls-static

Note : Shows currently configured values
Changes made after last system start if any,
will be effective after next restart

pi-system-120/admin#
```

show tech-support

To display technical support information, including email, use the **show tech-support** command in EXEC mode.

show tech-support file [word]

Syntax Description

file	Saves any technical support data as a file in the local disk.
word	Filename to save. Up to 80 alphanumeric characters.

Command Default

Passwords and other security information do not appear in the output.

Command Modes

EXEC

Usage Guidelines

The **show tech-support** command is useful for collecting a large amount of information about your server for troubleshooting purposes. You can then provide output to technical support representatives when reporting a problem.

Examples

```
ncs/admin# show tech-support
###################################################
Application Deployment Engine(ADE) - 2.0.0.568
Technical Support Debug Info follows...
###################################################


*****************************************
Checking dmidecode Serial Number(s)
*****************************************
  None
 VMware-56 4d 14 cb 54 3d 44 5d-49 ee c4 ad a5 6a 88 c4

*****************************************
Displaying System Uptime...
*****************************************
 12:54:34 up 18:37,  1 user,  load average: 0.14, 0.13, 0.12

*****************************************
Display Memory Usage(KB)
*****************************************
             total       used       free     shared    buffers     cached
Mem:       1035164    1006180      28984          0      10784     345464
-/+ buffers/cache:     649932     385232
Swap:      2040244     572700    1467544

*****************************************
Displaying Processes(ax --forest)...
*****************************************
  PID TTY      STAT   TIME COMMAND
    1 ?        Ss     0:02 init [3]
    2 ?        S<     0:00 [migration/0]
    3 ?        SN     0:00 [ksoftirqd/0]
    4 ?        S<     0:00 [watchdog/0]
    5 ?        S<     0:00 [events/0]
--More--
(press Spacebar to continue)

ncs/admin#
```

Related Commands

Command	Description
show interface	Displays the usability status of the interfaces.
show process	Displays information about active processes.
show running-config	Displays the contents of the current running configuration.

show terminal

To obtain information about the terminal configuration parameter settings, use the **show terminal** command in EXEC mode.

show terminal

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

```
ncs/admin# show terminal
TTY: /dev/pts/0 Type: "vt100"
Length: 27 lines, Width: 80 columns
Session Timeout: 30 minutes
ncs/admin#
```

show terminal describes the fields of the **show terminal** output.

Table 6: Show Terminal Field Descriptions

Field	Description
TTY: /dev/pts/0	Displays standard output to type of terminal.
Type: “vt100“	Type of current terminal used.
Length: 24 lines	Length of the terminal display.
Width: 80 columns	Width of the terminal display, in character columns.
Session Timeout: 30 minutes	Length of time, in minutes, for a session, after which the connection closes.

show timezone

To display the time zone set on the system, use the **show timezone** command in EXEC mode.

show timezone

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

```
pi-system/admin# show timezone
Asia/Kolkata
pi-system/admin#
```

Related Commands

Command	Description
clock timezone	Sets the time zone on the system.
show timezones	Displays the time zones available on the system.

show timezones

To obtain a list of time zones from which you can select, use the **show timezones** command in EXEC mode.

show timezones

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

See the clock timezone command, for examples of the time zones available for the server.

Examples

```
ncs/admin# show timezones
Africa/Blantyre
Africa/Dar_es_Salaam
Africa/Dakar
Africa/Asmara
Africa/Timbuktu
Africa/Maputo
Africa/Accra
Africa/Kigali
Africa/Tunis
Africa/Nouakchott
Africa/Ouagadougou
Africa/Windhoek
Africa/Douala
Africa/Johannesburg
Africa/Luanda
Africa/Lagos
Africa/Djibouti
Africa/Khartoum
Africa/Monrovia
Africa/Bujumbura
Africa/Porto-Novo
Africa/Malabo
Africa/Ceuta
Africa/Banjul
Africa/Cairo
Africa/Mogadishu
Africa/Brazzaville
Africa/Kampala
Africa/Sao_Tome
Africa/Algiers
Africa/Addis_Ababa
Africa/Ndjamena
Africa/Gaborone
Africa/Bamako
Africa/Freetown
--More--
(press Spacebar to continue)

ncs/admin#
```

Related Commands

Command	Description
show timezone	Displays the time zone set on the system.
clock timezone	Sets the time zone on the system.

show udi

To display information about the UDI of the Cisco ISE 3315 appliance, use the **show udi** command in EXEC mode.

show udi

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

The following output appears when you run the **show udi** on **Hyper V**appliance server.

Example 1

```
pi-system/admin# sh udi
SPID: Cisco-HY-SPID
VPID: V02
Serial: KDGGLLPDJDC

pi-system-241/admin#
```

The following output appears when you run the **show udi** on **Gen 2** appliance server.

Example 2

```
pi-system/admin# sh udi
PID: PI-UCS-APL-K9
VPID: A0
Serial: FCH1842V1EH

pi-system-117/admin#
```

show uptime

To display the length of time that you have been logged in to the server, use the **show uptime** command in EXEC mode.

show uptime |

Syntax Description

|	(Optional) Output modifier variables: • *begin*—Matched pattern. Up to 80 alphanumeric characters. • *count*—Counts the number of lines in the output. Add number after the word *count*. • *end*—Ends with line that matches. Up to 80 alphanumeric characters. • *exclude*—Excludes lines that match. Up to 80 alphanumeric characters. • *include*—Includse lines that match. Up to 80 alphanumeric characters. • *last*—Displays last few lines of output. Add number after the word *last*. Up to 80 lines to display. Default 10.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

```
ncs/admin# show uptime
3 day(s), 18:55:02
ncs/admin#
```

show users

To display the list of users logged in to the server, use the **show users** command in EXEC mode.

show users

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

```
ncs/admin# show users
USERNAME         ROLE   HOST                     TTY      LOGIN DATETIME

admin            Admin  10.77.137.60             pts/0    Fri Aug  6 09:45:47 2010

ncs/admin#
```

show version

To display information about the software version of the system, use the **show version** command in EXEC mode.

show version

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

This command displays version information about the Cisco ADE-OS software running on the server, and displays the version.

Configuration Commands

This section lists the **configuration commands** along with a brief description of their use, command defaults, command syntax, command modes, usage guidelines, command examples, and related commands, where applicable.

Configuration commands include **interface** and **repository**.

Note Some of the configuration commands require you to enter the configuration submode to complete the command configuration.

To access configuration mode, you must use the **configure** command in EXEC mode.

aaa authentication

To configure external authentication, use the **aaa authentication** command in configuration mode.

aaa authentication tacacs+ server *TACACS server address* **key plain** *shared-key*

Syntax Description

TACACS server address	IP address or hostname of the TACACS+ server.
shared-key	Indicates the shared secret text string.

Command Default

No default behavior or values.

Command Modes

Configuration

Examples

```
admin# aaa authentication tacacs+ server 1.1.1.5 key plain Secret
admin# username tacacsuser password remote role admin
```

Ensure that the TACACS+ server has the same user name of the Prime Infrastructure server, and Prime Infrastructure and TACACS+ servers are integrated properly.

backup-staging-url

You can use this option to configure a Network File System (NFS) share on Cisco Prime Infrastructure when partition is low on disk space and a backup cannot be taken. You can do so by using the **backup-staging-url** command in configuration mode.

backup-staging-url *word*

Syntax Description

word	NFS URL for staging area. Up to 2048 alphanumeric characters. Use **nfs:**//*server*:*path*(1) .

Command Default

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

The URL is NFS only. The format of the command is **backup-staging-url nfs:**//server:path.

Caution

Ensure that you secure your NFS server in such a way that the directory can be accessed only by the IP address of the server.

Examples

```
ncs/admin(config)# backup-staging-url nfs://loc-filer02a:/vol/local1/private1/jdoe
ncs/admin(config)#
```

cdp holdtime

To specify the amount of time for which the receiving device should hold a Cisco Discovery Protocol packet from the server before discarding it, use the **cdp holdtime** command in configuration mode. To revert to the default setting, use the **no** form of this command.

[no] cdp holdtime *seconds*

Syntax Description

seconds	Specifies the hold time, in seconds. Value from 10 to 255 seconds.

Command Default

180 seconds

Command Modes

Configuration

Usage Guidelines

Cisco Discovery Protocol packets transmit with a time to live, or hold time, value. The receiving device will discard the Cisco Discovery Protocol information in the Cisco Discovery Protocol packet after the hold time has elapsed.

The **cdp holdtime** command takes only one argument; otherwise, an error occurs.

Examples

```
ncs/admin(config)# cdp holdtime 60
ncs/admin(config)#
```

Related Commands

	Description
cdp timer	Specifies how often the server sends Cisco Discovery Protocol updates.
cdp run	Enables the Cisco Discovery Protocol.

cdp run

To enable the Cisco Discovery Protocol, use the **cdp run** command in configuration mode. To disable the Cisco Discovery Protocol, use the **no** form of this command.

[no] cdp run *[GigabitEthernet]*

Syntax Description

GigabitEthernet	Specifies the Gigabit Ethernet interface on which to enable the Cisco Discovery Protocol.

Command Default

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

The command has one optional argument, which is an interface name. Without an optional interface name, the command enables the Cisco Discovery Protocol on all interfaces.

Note The default for this command is on interfaces that are already up and running. When you are bringing up an interface, stop the Cisco Discovery Protocol first; then, start the Cisco Discovery Protocol again.

Examples

```
ncs/admin(config)# cdp run GigabitEthernet 0
ncs/admin(config)#
```

Related Commands

	Description
cdp holdtime	Specifies the length of time that the receiving device should hold a Cisco Discovery Protocol packet from the server before discarding it.
cdp timer	Specifies how often the server sends Cisco Discovery Protocol updates.

cdp timer

To specify how often the server sends Cisco Discovery Protocol updates, use the **cdp timer** command in configuration mode. To revert to the default setting, use the **no** form of this command.

[no] cdp timer *seconds*

Syntax Description

seconds	Specifies how often, in seconds, the server sends Cisco Discovery Protocol updates. Value from 5 to 254 seconds.

Command Default

60 seconds

Command Modes

Configuration

Usage Guidelines

Cisco Discovery Protocol packets transmit with a time to live, or hold time, value. The receiving device will discard the Cisco Discovery Protocol information in the Cisco Discovery Protocol packet after the hold time has elapsed.

The **cdp timer** command takes only one argument; otherwise, an error occurs.

Examples

```
ncs/admin(config)# cdp timer 60
ncs/admin(config)#
```

Related Commands

	Description
cdp holdtime	Specifies the amount of time that the receiving device should hold a Cisco Discovery Protocol packet from the server before discarding it.
cdp run	Enables the Cisco Discovery Protocol.

clock timezone

To set the time zone, use the **clock timezone** command in configuration mode. To disable this function, use the **no** form of this command.

clock timezone *timezone*

Syntax Description

timezone	Name of the time zone visible when in standard time. Up to 64 alphanumeric characters.

Command Default

UTC

Command Modes

Configuration

Usage Guidelines

The system internally keeps time in Coordinated Universal Time (UTC). If you do not know your specific time zone, you can enter the region, country, and city (see Tables Table 7: Common Time Zones, Table 8: Australia Time Zones, and Table 9: Asia Time Zones for sample time zones to enter on your system).

Table 7: Common Time Zones

Acronym or name	Time Zone Name
Europe	
GMT, GMT0, GMT-0, GMT+0, UTC, Greenwich, Universal, Zulu	Greenwich Mean Time, as UTC
GB	British
GB-Eire, Eire	Irish
WET	Western Europe Time, as UTC
CET	Central Europe Time, as UTC + 1 hour
EET	Eastern Europe Time, as UTC + 2 hours
United States and Canada	
EST, EST5EDT	Eastern Standard Time, as UTC -5 hours
CST, CST6CDT	Central Standard Time, as UTC -6 hours

Acronym or name	Time Zone Name
MST, MST7MDT	Mountain Standard Time, as UTC -7 hours
PST, PST8PDT	Pacific Standard Time, as UTC -8 hours
HST	Hawaiian Standard Time, as UTC -10 hours

Table 8: Australia Time Zones

AustraliaFootnote.			
ACTFootnote.	Adelaide	Brisbane	Broken_Hill
Canberra	Currie	Darwin	Hobart
Lord_Howe	Lindeman	LHIFootnote.	Melbourne
North	NSWFootnote.	Perth	Queensland
South	Sydney	Tasmania	Victoria
West	Yancowinna		

3456

[3] (1) Enter the country and city together with a forward slash (/) between them; for example, Australia/Currie.
[4] (2) ACT = Australian Capital Territory
[5] (3) LHI = Lord Howe Island
[6] (4) NSW = New South Wales

Table 9: Asia Time Zones

AsiaFootnote.			
AdenFootnote.	Almaty	Amman	Anadyr
Aqtau	Aqtobe	Ashgabat	Ashkhabad
Baghdad	Bahrain	Baku	Bangkok
Beirut	Bishkek	Brunei	Calcutta
Choibalsan	Chongqing	Columbo	Damascus
Dhakar	Dili	Dubai	Dushanbe

AsiaFootnote.			
Gaza	Harbin	Hong_Kong	Hovd
Irkutsk	Istanbul	Jakarta	Jayapura
Jerusalem	Kabul	Kamchatka	Karachi
Kashgar	Katmandu	Kuala_Lumpur	Kuching
Kuwait	Krasnoyarsk		

78

[7] (1) The Asia time zone includes cities from East Asia, Southern Southeast Asia, West Asia, and Central Asia.

[8] (2) Enter the region and city or country together separated by a forward slash (/); for example, Asia/Aden.

Note Several more time zones are available to you. On your server, enter the **show timezones** command. A list of all of the time zones available in the server appears. Choose the most appropriate one for your time zone.

Examples

```
pi-admin/admin(config)# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
pi-admin/admin(config)# clock timezone Asia/Kolkata
pi-admin/admin(config)#
```

Related Commands

	Description
show timezones, on page 159	Displays a list of available time zones on the system.
show timezone, on page 158	Displays the current time zone set on the system.

do

To execute an EXEC-level command from configuration mode or any configuration submode, use the **do** command in any configuration mode.

do

Syntax Description

This command has no arguments or keywords.

Table 10: Command Options for the Do Command

	Description
application install	Installs a specific application.
application remove	Removes a specific application.
application start	Starts or enables a specific application
application stop	Stops or disables a specific application.
application upgrade	Upgrades a specific application.
backup	Performs a backup (and Cisco ADE OS) and places the backup in a repository.
backup-logs	Performs a backup of all of the logs on the server to a remote location.
clock	Sets the system clock on the server.
configure	Enters configuration mode.
copy	Copies any file from a source to a destination.
debug	Displays any errors or events for various command situations; for example, backup and restore, configuration, copy, resource locking, file transfer, and user management.
delete	Deletes a file on the server.
dir	Lists files on the server.
forceout	Forces the logout of all of the sessions of a specific node user.
halt	Disables or shuts down the server.
mkdir	Creates a new directory.
nslookup	Queries the IPv4 address or hostname of a remote system.

	Description
patch	Install System or Application patch.
pep	Configures the Inline PEP node.
ping	Determines the IPv4 network activity on a remote system.
ping6	Determines the IPv6 network activity on a IPv6 remote system.
reload	Reboots the server.
restore	Performs a restore and retrieves the backup out of a repository.
rmdir	Removes an existing directory.
show	Provides information about the server.
ssh	Starts an encrypted session with a remote system.
tech	Provides Technical Assistance Center (TAC) commands.
telnet	Establishes a Telnet connection to a remote system.
terminal length	Sets terminal line parameters.
terminal session-timeout	Sets the inactivity timeout for all terminal sessions.
terminal session-welcome	Sets the welcome message on the system for all terminal sessions.
terminal terminal-type	Specifies the type of terminal connected to the current line of the current session.
traceroute	Traces the route of a remote IP address.
undebug	Disables the output (display of errors or events) of the **debug** command for various command situations; for example, backup and restore, configuration, copy, resource locking, file transfer, and user management.
write	Erases the startup configuration that forces the setup utility to run and prompts the network configuration, copies the running configuration to the startup configuration, and displays the running configuration on the console.

Command Default

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

Use this command to execute EXEC commands (such as **show**, **clear**, and **debug** commands) while configuring your server. After the EXEC command executes, the system will return to the configuration mode that you were using.

Examples

```
ncs/admin(config)# do show run
Generating configuration...
!
hostname ncs
!
ip domain-name cisco.com
!
interface GigabitEthernet 0
  ip address 172.23.90.113 255.255.255.0
  ipv6 address autoconfig
!
ip name-server 172.16.168.183
!
ip default-gateway 172.23.90.1
!
clock timezone EST
!
ntp server time.nist.gov
!
username admin password hash $1$JbbHvKVG$xMZ/XL4tH15Knf.FfcZZr. role admin
!
service sshd
!
backup-staging-url nfs://loc-filer02a:/vol/local1/private1/jdoe
!
password-policy
  lower-case-required
  upper-case-required
  digit-required
  no-username
  disable-cisco-passwords
  min-password-length 6
!
logging localhost
logging loglevel 6
!
--More--

ncs/admin(config)#
```

end

To end the current configuration session and return to EXEC mode, use the **end** command in configuration mode.

end

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

This command brings you back to EXEC mode regardless of what configuration mode or submode you are in.

Use this command when you finish configuring the system and you want to return to EXEC mode to perform verification steps.

Examples

```
ncs/admin(config)# end
ncs/admin#
```

Related Commands

Command	Description
exit	Exits configuration mode.
exit (EXEC)	Closes the active terminal session by logging out of the server.

exit

To exit any configuration mode to the next-highest mode in the CLI mode hierarchy, use the **exit** command in configuration mode.

exit

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

The **exit** command is used in the server to exit the current command mode to the next highest command mode in the CLI mode hierarchy.

For example, use the **exit** command in configuration mode to return to EXEC mode. Use the **exit** command in the configuration submodes to return to configuration mode. At the highest level, EXEC mode, the **exit** command exits the EXEC mode and disconnects from the server (see exit, for a description of the **exit** (EXEC) command).

Examples

```
ncs/admin(config)# exit
ncs/admin#
```

Related Commands

Command	Description
end	Exits configuration mode.
exit (EXEC)	Closes the active terminal session by logging out of the server.

hostname

To set the hostname of the system, use the **hostname** command in configuration mode. To delete the hostname from the system, use the **no** form of this command, which resets the system to localhost.

[no] hostname word

Syntax Description

word	Name of the host. Contains at least 2 to 64 alphanumeric characters and an underscore (_). The hostname must begin with a character that is not a space.

Command Default

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

A single instance type of command, **hostname** only occurs once in the configuration of the system. The hostname must contain one argument; otherwise, an error occurs.

Examples

```
ncs/admin(config)# hostname ncs-1
Changing the hostname or IP may result in undesired side effects,
such as installed application(s) being restarted.
Are you sure you want to proceed? [y/n] y
Stopping NCS Monitoring & Troubleshooting Log Processor...
Stopping NCS Monitoring & Troubleshooting Log Collector...
Stopping NCS Monitoring & Troubleshooting Alert Process...
Stopping NCS Application Server...
Stopping NCS Monitoring & Troubleshooting Session Database...
Stopping NCS Database processes...
Starting NCS Database processes...
Starting NCS Monitoring & Troubleshooting Session Database...
Starting NCS Application Server...
Starting NCS Monitoring & Troubleshooting Log Collector...
Starting NCS Monitoring & Troubleshooting Log Processor...
Starting NCS Monitoring & Troubleshooting Alert Process...
Note: NCS Processes are initializing. Use 'show application status ncs'
      CLI to verify all processes are in running state.

ncs-1/admin(config)#

ncs-1/admin# show application status ncs

NCS Database listener is running, PID: 11142
NCS Database is running, number of processes: 29
NCS Application Server is still initializing.
NCS M&T Session Database is running, PID: 11410
NCS M&T Log Collector is running, PID: 11532
NCS M&T Log Processor is running, PID: 11555
NCS M&T Alert Process is running, PID: 11623

ncs-1/admin#
```

icmp echo

To configure the Internet Control Message Protocol (ICMP) echo responses, use the **icmp echo** command in configuration mode.

icmp echo {off | on}

Syntax Description

off	Disables ICMP echo response.
on	Enables ICMP echo response.

Command Default

The system behaves as if the ICMP echo response is on (enabled).

Command Modes

Configuration

Examples

```
ncs/admin(config)# icmp echo off
ncs/admin(config)#
```

Related Commands

Command	Description
show icmp_status	Display ICMP echo response configuration information.

interface

To configure an interface type and enter interface configuration mode, use the **interface** command in configuration mode.

Note VMware virtual machine may have a number of interfaces available. This depends on how many network interfaces (NIC) are added to the virtual machine.

interface GigabitEthernet ip-address

Syntax Description

GigabitEthernet	Configures the Gigabit Ethernet interface.
0 - 3	Number of the Gigabit Ethernet port to configure.

Note After you enter the Gigabit Ethernet port number in the **interface** command, you enter config-GigabitEthernet configuration submode (see the following Syntax Description).

do	EXEC command. Allows you to perform any EXEC commands in this mode (see do).
end	Exits config-GigabitEthernet submode and returns you to EXEC mode.
exit	Exits the config-GigabitEthernet configuration submode.
ip	Sets IP address and netmask for the Ethernet interface (see ip address).
ipv6	Configures the IPv6 autoconfiguration address and IPv6 address from DHCPv6 server. (see ipv6 address autoconfig and ipv6 address dhcp).
no	Negates the command in this mode. Two keywords are available: • ip—Sets the IP address and netmask for the interface. • shutdown—Shuts down the interface.
shutdown	Shuts down the interface (see shutdown).

Command Default

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

You can use the **interface** command to configure subinterfaces to support various requirements.

Examples

```
ncs/admin(config)# interface GigabitEthernet 0
ncs/admin(config-GigabitEthernet)#
```

Related Commands

Command	Description
show interface	Displays information about the system interfaces.
ip address (interface configuration mode)	Sets the IP address and netmask for the interface.
shutdown (interface configuration mode)	Shuts down the interface (see shutdown).

ipv6 address autoconfig

To enable IPv6 stateless autoconfiguration, use the **ipv6 address autoconfig** command in configuration mode. To remove the address from the interface, use the **no** form of this command.

[no] ipv6 address autoconfig [default]0

Syntax Description

default	(Optional) If a default router is selected on this interface, the default keyword causes a default route to be installed using that default router. The **default** keyword can be specified only on one interface.

Command Default

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

IPv6 stateless autoconfiguration has the security downfall of having predictable IP addresses. This downfall is resolved with privacy extensions. You can verify that the privacy extensions feature is enabled using the **show** command.

IPv6 address autoconfiguration is enabled by default in Linux. Cisco ADE 2.0 shows the IPv6 address autoconfiguration in the running configuration for any interface that is enabled.

Examples

Example 1

```
ncs/admin# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ncs/admin(config)# interface GigabitEthernet 0
ncs/admin(config)# (config-GigabitEthernet)# ipv6 address autoconfig
ncs/admin(config)# (config-GigabitEthernet)# end
ncs/admin#
```

When IPv6 autoconfiguration is enabled, the running configuration shows the interface settings similar to the following:

```
!
interface GigabitEthernet 0
  ip address 172.23.90.116 255.255.255.0
  ipv6 address autoconfig
!
```

You can use the **show interface GigabitEthernet 0** command to display the interface settings. In example 2, you can see that the interface has three IPv6 addresses. The first address (starting with 3ffe) is obtained using the stateless autoconfiguration. For the stateless autoconfiguration to work, you must have IPv6 route advertisement enabled on that subnet. The next address (starting with fe80) is a link-local address that does not have any scope outside the host. You will always see a link local address regardless of the IPv6 autoconfiguration or DHCPv6 configuration. The last address (starting with 2001) is obtained from a IPv6 DHCP server.

Example 2

```
ncs/admin# show interface GigabitEthernet 0
eth0      Link encap:Ethernet  HWaddr 00:0C:29:AF:DA:05
          inet addr:172.23.90.116  Bcast:172.23.90.255  Mask:255.255.255.0
          inet6 addr: 3ffe:302:11:2:20c:29ff:feaf:da05/64 Scope:Global
          inet6 addr: fe80::20c:29ff:feaf:da05/64 Scope:Link
          inet6 addr: 2001:558:ff10:870:8000:29ff:fe36:200/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:77848 errors:0 dropped:0 overruns:0 frame:0
          TX packets:23131 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10699801 (10.2 MiB)  TX bytes:3448374 (3.2 MiB)
          Interrupt:59 Base address:0x2000

ncs/admin#
```

To verify that the privacy extensions feature is enabled, you can use the **show interface GigabitEthernet 0** command. You can see two autoconfiguration addresses: one address is without the privacy extensions, and the other is with the privacy extensions.

In the example 3 below, the MAC is 3ffe:302:11:2:20c:29ff:feaf:da05/64 and the non-RFC3041 address contains the MAC, and the privacy-extension address is 302:11:2:9d65:e608:59a9:d4b9/64.

The output appears similar to the following:

Example 3

```
ncs/admin# show interface GigabitEthernet 0
eth0      Link encap:Ethernet  HWaddr 00:0C:29:AF:DA:05
          inet addr:172.23.90.116  Bcast:172.23.90.255  Mask:255.255.255.0
          inet6 addr: 3ffe:302:11:2:9d65:e608:59a9:d4b9/64 Scope:Global
          inet6 addr: 3ffe:302:11:2:20c:29ff:feaf:da05/64 Scope:Global
          inet6 addr: fe80::20c:29ff:feaf:da05/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:60606 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2771 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9430102 (8.9 MiB)  TX bytes:466204 (455.2 KiB)
          Interrupt:59 Base address:0x2000

ncs/admin#
```

Related Commands

Command	Description
show interface	Displays information about the system interfaces.
ip address (interface configuration mode)	Sets the IP address and netmask for the interface.
shutdown (interface configuration mode)	Shuts down the interface (see shutdown).
ipv6 address dhcp	Enables IPv6 address DHCP on an interface.
show running-config	Displays the contents of the currently running configuration file or the configuration.

ipv6 address dhcp

To enable IPv6 address DHCP, use the **ipv6 address dhcp** command in configuration mode. To remove the address from the interface, use the **no** form of this command.

[no] ipv6 address dhcp [rapid-commit] 0

Syntax Description

[rapid-commit]	(Optional) Allows the two-message exchange method for address assignment.
0	Gigabit Ethernet port number to be configured.

Command Default

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

None.

Examples

```
ncs/admin# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ncs/admin(config)# interface GigabitEthernet 0
ncs/admin(config-GigabitEthernet)# ipv6 address dhcp
ncs/admin(config-GigabitEthernet)# end
ncs/admin#
```

When IPv6 DHCPv6 is enabled, the running configuration shows the interface settings similar to the following:

```
!
interface GigabitEthernet 0
  ip address 172.23.90.116 255.255.255.0
  ipv6 address dhcp
!
```

Note The IPv6 stateless autoconfiguration and IPv6 address DHCP are not mutually exclusive. It is possible to have both IPv6 stateless autoconfiguration and IPv6 address DHCP on the same interface. You can use the **show interface** to display what IPv6 addresses are in use for a particular interface.

When both the IPv6 stateless autoconfiguration and IPv6 address DHCP are enabled, the running configuration shows the interface settings similar to the following:

```
!
interface GigabitEthernet 0
  ip address 172.23.90.116 255.255.255.0
  ipv6 address dhcp
!
```

Related Commands

Command	Description
show interface	Displays information about the system interfaces.
ip address (interface configuration mode)	Sets the IP address and netmask for the interface.
shutdown (interface configuration mode)	Shuts down the interface (see shutdown).
ipv6 address autoconfig	Enables IPv6 stateless autoconfiguration on an interface.
show running-config	Displays the contents of the currently running configuration file or the configuration.

ipv6 address static

To assign static IPv6 address, use the **ipv6 address static** command in configuration mode. To remove the address from the interface, use the **no** form of this command.

ipv6 address static [ipv6 address] 0

Command Default

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

None.

Examples

```
admin(config-GigabitEthernet)# ipv6 address static 0:0:0:0:0:ffff:a7e:a9d2
admin(config-GigabitEthernet)# ipv6 default-gateway 0:0:0:0:0:ffff:ffff:ffe0
```

Related Commands

Command	Description
ipv6 address autoconfig	Enables IPv6 stateless autoconfiguration on an interface.
ipv6 address dhcp, on page 185	Enables IPv6 address DHCP on an interface.

ip address

To set the IP address and netmask for the Ethernet interface, use the **ip address** command in interface configuration mode. To remove an IP address or disable IP processing, use the **no** form of this command.

[no] ip address ip-address netmask

Note You can configure the same IP address on multiple interfaces. You might want to do this to limit the configuration steps that are needed to switch from using one interface to another.

Syntax Description

ip-address	IPv4 version IP address.
netmask	Mask of the associated IP subnet.

Command Default

Enabled.

Command Modes

Interface configuration

Usage Guidelines

Requires exactly one address and one netmask; otherwise, an error occurs.

Examples

```
ncs/admin(config)# interface GigabitEthernet 1
ncs/admin(config-GigabitEthernet)# ip address 209.165.200.227 255.255.255.224
Changing the hostname or IP may result in undesired side effects,
such as installed application(s) being restarted.
........
To verify that NCS processes are running, use the
'show application status ncs' command.
ncs/admin(config-GigabitEthernet)#
```

Related Commands

Command	Description
shutdown (interface configuration mode)	Disables an interface (see shutdown).
ip default-gateway	Sets the IP address of the default gateway of an interface.
show interface	Displays information about the system IP interfaces.
interface	Configures an interface type and enters the interface mode.

ip default-gateway

To define or set a default gateway with an IP address, use the **ip default-gateway** command in configuration mode. To disable this function, use the **no** form of this command.

[no] ip default-gateway ip-address

Syntax Description

ip-address	IP address of the default gateway.

Command Default

Disabled.

Command Modes

Configuration

Usage Guidelines

If you enter more than one argument or no arguments at all, an error occurs.

Examples

```
ncs/admin(config)# ip default-gateway 209.165.202.129
ncs/admin(config)#
```

Related Commands

Command	Description
ip address (interface configuration mode)	Sets the IP address and netmask for the Ethernet interface.

ip domain-name

To define a default domain name that the server uses to complete hostnames, use the **ip domain-name** command in configuration mode. To disable this function, use the **no** form of this command.

[no] ip domain-name word

Syntax Description

word	Default domain name used to complete the hostnames. Contains at least 2 to 64 alphanumeric characters.

Command Default

Enabled.

Command Modes

Configuration

Usage Guidelines

If you enter more or fewer arguments, an error occurs.

Examples

```
ncs/admin(config)# ip domain-name cisco.com
ncs/admin(config)#
```

Related Commands

	Description
ip name-server	Sets the DNS servers for use during a DNS query.

ip name-server

To set the Domain Name Server (DNS) servers for use during a DNS query, use the **ip name-server** command in configuration mode. You can configure one to three DNS servers. To disable this function, use the **no** form of this command.

Note Using the **no** form of this command removes all of the name servers from the configuration. Using the **no** form of this command and one of the IP names removes only that IP name server.

[no] ip name-server *ip-address [ip-address*]*}

Syntax Description

ip-address	Address of a name server.
*ip-address**	(Optional) IP addresses of additional name servers. **Note** You can configure a maximum of three name servers.

Command Default

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

The first name server that is added with the **ip name-server** command occupies the first position and the system uses that server first to resolve the IP addresses.

You can add name servers to the system one at a time or all at once, until you reach the maximum (3). If you already configured the system with three name servers, you must remove at least one server to add additional name servers.

To place a name server in the first position so that the subsystem uses it first, you must remove all name servers with the **no** form of this command before you proceed.

Examples

```
ncs/admin(config)# ip name-server 209.165.201.1


To verify that NCS processes are running, use the
'show application status ncs' command.
ncs/admin(config)#
```

You can choose not to restart the server; nevertheless, the changes will take effect.

Related Commands

Command	Description
ip domain-name	Defines a default domain name that the server uses to complete hostnames.

ip route

To configure the static routes, use the **ip route** command in configuration mode. To remove static routes, use the **no** form of this command.

ip route prefix mask **gateway** ip-address

no ip route prefix mask

Syntax Description

prefix	IP route prefix for the destination.
mask	Prefix mask for the destination.
gateway	Route-specific gateway
ip-address	IP address of the next hop that can be used to reach that network.

Command Default

No default behavior or values.

Configuration.

Usage Guidelines

Static routes are manually configured, which makes them inflexible (they cannot dynamically adapt to network topology changes), but extremely stable. Static routes optimize bandwidth utilization, because no routing updates need to be sent to maintain them. They also make it easy to enforce routing policy.

Examples

```
ncs/admin(config)# ip route 192.168.0.0 255.255.0.0 gateway 172.23.90.2
ncs/admin(config)#
```

kron occurrence

To schedule one or more Command Scheduler commands to run at a specific date and time or a recurring level, use the **kron occurrence** command in configuration mode. To delete this schedule, use the **no** form of this command.

[no] kron {**occurrence**} *occurrence-name*

Syntax Description

occurrence-name	Name of the occurrence. Up to 80 alphanumeric characters. (See the following note and Syntax Description.)

Note After you enter the *occurrence-name* in the **kron occurrence** command, you enter the config-occurrence configuration submode (see the following syntax description).

at	Identifies that the occurrence is to run at a specified calendar date and time. Usage: at [*hh:mm*] [*day-of-week* | *day-of-month* | *month day-of-month*].
do	EXEC command. Allows you to perform any EXEC commands in this mode (see do).
end	Exits the kron-occurrence configuration submode and returns you to EXEC mode.
exit	Exits the kron-occurrence configuration mode.
no	Negates the command in this mode. Three keywords are available: • at—Usage: at [*hh:mm*] [*day-of-week* | *day-of-month* | *month day-of-month*]. • policy-list—Specifies a policy list to be run by the occurrence. Up to 80 alphanumeric characters. • recurring—Execution of the policy lists should be repeated.
policy-list	Specifies a Command Scheduler policy list to be run by the occurrence.
recurring	Identifies that the occurrences run on a recurring basis.

Command Default

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

Use the **kron occurrence** and **policy-list** commands to schedule one or more policy lists to run at the same time or interval.

Use the **kron policy-list** command in conjunction with the **cli** command to create a Command Scheduler policy that contains the EXEC CLI commands to be scheduled to run on the server at a specified time. See the kron policy-list command.

Examples

Note

When you run the **kron** command, backup bundles are created with a unique name (by adding a time stamp) to ensure that the files do not overwrite each other.

Example 1:Weekly Backup

```
ncs/admin(config)# kron occurrence WeeklyBackup
ncs/admin(config-Occurrence)# at 14:35 Monday
ncs/admin(config-Occurrence)# policy-list SchedBackupPolicy
ncs/admin(config-Occurrence)# recurring
ncs/admin(config-Occurrence)# exit
ncs/admin(config)#
```

Example 2: Daily Backup

```
ncs/admin(config)# kron occurrence DailyBackup
ncs/admin(config-Occurrence)# at 02:00
ncs/admin(config-Occurrence)# exit
ncs/admin(config)#
```

Command	Description
kron policy-list	Specifies a name for a Command Scheduler policy.

kron policy-list

To specify a name for a Command Scheduler policy and enter the kron-Policy List configuration submode, use the **kron policy-list** command in configuration mode. To delete a Command Scheduler policy, use the **no** form of this command.

[no] kron {**policy-list**} *list-name*

Syntax Description

policy-list	Specifies a name for Command Scheduler policies.
list-name	Name of the policy list. Up to 80 alphanumeric characters.

Note After you enter the *list-name* in the **kron policy-list** command, you enter the config-Policy List configuration submode (see the following Syntax Description).

cli	Command to be executed by the scheduler. Up to 80 alphanumeric characters.
do	EXEC command. Allows you to perform any EXEC commands in this mode (see the do) command.
end	Exits from the config-policy list configuration submode and returns you to EXEC mode.
exit	Exits this submode.
no	Negates the command in this mode. One keyword is available: • cli—Command to be executed by the scheduler.

Command Default

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

Use the **kron policy-list** command in conjunction with the **cli** command to create a Command Scheduler policy that contains the EXEC CLI commands to be scheduled to run on the server at a specified time. Use the **kron occurrence** and **policy list** commands to schedule one or more policy lists to run at the same time or interval. See the ip route command.

Examples

```
ncs/admin(config)# kron policy-list SchedBackupMonday
```

```
ncs/admin(config-Policy List)# cli backup SchedBackupMonday repository SchedBackupRepo
ncs/admin(config-Policy List)# exit
ncs/admin(config)#
```

Related Commands

Command	Description
ip route	Specifies schedule parameters for a Command Scheduler occurrence and enters config-Occurrence configuration mode.

logging

To enable the system to forward logs to a remote system or to configure the log level, use the **logging** command in configuration mode. To disable this function, use the **no** form of this command.

[no] logging *{ip-address* | *hostname}* {**loglevel** *level*}

Syntax Description

ip-address	IP address of remote system to which you forward logs. Up to 32 alphanumeric characters.
hostname	Hostname of remote system to which you forward logs. Up to 32 alphanumeric characters.
loglevel	The command to configure the log level for the **logging** command.
level	Number of the desired priority level at which you set the log messages. Priority levels are (enter the number for the keyword): • 0-emerg—Emergencies: System unusable. • 1-alert—Alerts: Immediate action needed. • 2-crit—Critical: Critical conditions. • 3-err—Error: Error conditions. • 4-warn—Warning: Warning conditions. • 5-notif—Notifications: Normal but significant conditions. • 6-inform—(Default) Informational messages. • 7-debug—Debugging messages.

Command Default

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

This command requires an IP address or hostname or the **loglevel** keyword; an error occurs if you enter two or more of these arguments.

Examples

Example 1

```
ncs/admin(config)# logging 209.165.200.225
ncs/admin(config)#
```

Example 2

```
ncs/admin(config)# logging loglevel 0
ncs/admin(config)#
```

Related Commands

Command	Description
show logging	Displays the list of logs for the system.

ntp server

To allow for software clock synchronization by the NTP server for the system, use the **ntp server** command in configuration mode. Allows up to three servers.

ntp server *{ ntp-server}*

For the unauthenticated NTP servers, use the following command:

ntp server *{ ntp-server}*

Syntax Description

intp-server |	IP address or hostname of the server providing the clock synchronization. Arguments are limited to 255 alphanumeric characters.

Command Default

No servers are configured by default.

Command Modes

Configuration

Usage Guidelines

Use this command if you want to allow the system to synchronize with a specified server.

Note The synchronization process can take up to 20 minutes to complete.

Related Commands

Command	Description
show ntp	Displays the status information about the NTP associations.

Examples

```
ncs/admin(config)# ntp server 192.0.2.1 10 plain password
ncs/admin(config)# ntp server 192.0.2.2 20 plain pass123
```

Examples

```
ncs/admin# sh ntp
pi-ha-test-237-75/admin# sh ntp
NTP Server 1 : 192.0.2.1 : keyid=10
NTP Server 2 : 192.0.2.2
NTP Server 3 : 192.0.2.3 : keyid=10

unsynchronised
  time server re-starting
   polling server every 64 s

     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
192.0.2.1    .INIT.          16 u    -   64    0    0.000    0.000   0.000
192.0.2.2   .GPS.            1 u   43   64    7  250.340    0.523   1.620
192.0.2.3  192.0.2.2    2 u   41   64    7  231.451    7.517   3.434
```

Examples

```
ncs/admin# sh ntp
NTP Server 1 : 192.0.2.1 : keyid=10
NTP Server 2 : 192.0.2.2
NTP Server 3 : 192.0.2.3 : keyid=10

synchronised to NTP server (10.81.254.131) at stratum 2
   time correct to within 569 ms
   polling server every 64 s

     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
192.0.2.1    .INIT.          16 u    -   64    0    0.000    0.000   0.000
*192.0.2.2   .GPS.            1 u   12   64   37  243.863    3.605   4.240
192.0.2.3  192.0.2.2    2 u    8   64   37  231.451    7.517   3.784

Warning: Output results may conflict during periods of changing synchronization.
```

password-policy

To enable or configure the passwords on the system, use the **password-policy** command in configuration mode. To disable this function, use the **no** form of this command.

[no] password-policy option

Note The **password-policy** command requires a policy option (see Syntax Description). You must enter the **password-expiration-enabled** command before the other password-expiration commands.

Syntax Description

option	Different command options.

Note After you enter the **password-policy** command, you can enter config-password-policy configuration submode.

digit-required	Requires a digit in the password.
disable-repeat-characters	Disables the ability of the password to contain more than four identical characters.
disable-cisco-password	Disables the ability to use the word Cisco or any combination as the password.
do	EXEC command.
end	Exits from configure mode.
exit	Exits from this submode.
lower-case-required	Requires a lowercase letter in the password.
min-password-length	Specifies a minimum number of characters for a valid password. Integer length from 1 to 40.
no	Negates a command or set its defaults.
no-previous-password	Prevents users from reusing a part of their previous password.
no-username	Prohibits users from reusing their username as a part of a password.
password-expiration-days	Number of days until a password expires. Integer length from 1 to 3600.

password-expiration-enabled	Enables password expiration. **Note** You must enter the **password-expiration-enabled** command before the other password-expiration commands.
password-expiration-warning	Number of days before expiration that warnings of impending expiration begin. Integer length from 0 to 3600.
password-lock-enabled	Locks a password after several failures.
password-lock-retry-count	Number of failed attempts before password locks. Integer length from 1 to 20.
upper-case-required	Requires an uppercase letter in the password.
special-required	Requires a special character in the password.

Command Default

No default behavior or values.

Command Modes

Configuration

Examples

```
ncs/admin(config)# password-policy
ncs/admin(config-password-policy)# password-expiration-days 30
ncs/admin(config-password-policy)# exit
ncs/admin(config)#
```

repository

To enter the repository submode for configuration of backups, use the **repository** command in configuration mode.

repository *repository-name*

Syntax Description

repository-name	Name of repository. Up to 80 alphanumeric characters.

Note After you enter the name of the repository in the **repository** command, you enter repository configuration submode.

do	EXEC command.
end	Exits repository config submode and returns you to EXEC mode.
exit	Exits this mode.
no	Negates the command in this mode. Two keywords are available: • url—Repository URL. • user—Repository username and password for access.
url	URL of the repository. Up to 80 alphanumeric characters (see Table A-20).
user	Configure the username and password for access. Up to 30 alphanumeric characters.

Table 11: URL Keywords

Keyword	Source of Destination
word	Enter the repository URL, including server and path info. Up to 80 alphanumeric characters.
cdrom:	Local CD-ROM drive (read only).

Keyword	Source of Destination
disk:	Local storage. You can enter the **show repository** *repository_name* command to view all of the files in the local repository. **Note** All local repositories are created on the /localdisk partition. When you specify disk:/ in the repository URL, the system creates directories in a path that is relative to /localdisk. For example, if you entered **disk:/backup,** the directory is created at /localdisk/backup.
ftp:	Source or destination URL for an FTP network server. Use url ftp://*server*/*path*(1) .
nfs:	Source or destination URL for an NFS network server. Use url nfs://*server:path*1.
sftp:	Source or destination URL for an SFTP network server. Use url sftp://*server*/*path*1. **Note** SFTP Repositories may require the // between the ip address/FQDN and the physical path on the SFTP store. If you find that you cannot access the SFTP repository with single slashes, add the additional slash and try the operation again. Example: Repository SFTP-Store url sftp://server//path
tftp:	Source or destination URL for a TFTP network server. Use url tftp://*server*/*path*1. **Note** You cannot use a TFTP repository for performing a upgrade.

Command Default

No default behavior or values.

Command Modes

Configuration

Examples

Example 1

```
ncs/admin#
ncs/admin(config)# repository myrepository
ncs/admin(config-Repository)# url sftp://example.com/repository/system1
ncs/admin(config-Repository)# user abcd password plain example
ncs/admin(config-Repository)# exit
ncs/admin(config)# exit
ncs/admin#
```

Example 2

```
ncs/admin# configure termainal
ncs/admin(config)# repository myrepository
ncs/admin(config-Repository)# url disk:/
ncs/admin(config-Repository)# exit
ncs/admin(config)# exit
```

Related Commands

Command	Description
backup	Performs a backup (and Cisco ADE OS) and places the backup in a repository.
restore	Performs a restore and takes the backup out of a repository.
show backup history	Displays the backup history of the system.
show repository	Displays the available backup files located on a specific repository.

service

To specify a service to manage, use the **service** command in configuration mode. To disable this function, use the **no** form of this command.

[no] service sshd

Syntax Description

sshd	Secure Shell Daemon. The daemon program for SSH.

Command Default

No default behavior or values.

Command Modes

Configuration

Examples

```
ncs/admin(config)# service sshd
ncs/admin(config)#
```

shutdown

To shut down an interface, use the **shutdown** command in interface configuration mode. To disable this function, use the **no** form of this command.

[no] shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Interface

Usage Guidelines

When you shut down an interface using this command, you lose connectivity to the Cisco ISE-3315 appliance through that interface (even though the appliance is still powered on). However, if you have configured the second interface on the appliance with a different IP and have not shut down that interface, you can access the appliance through that second interface.

To shut down an interface, you can also modify the ifcfg-eth[0,1] file, which is located at */etc/sysconfig/network-scripts,* using the ONBOOT parameter:

- Disable an interface: set ONBOOT="no"
- Enable an interface: set ONBOOT="yes"

You can also use the **no shutdown** command to enable an interface.

Examples

```
ncs/admin(config)# interface GigabitEthernet 0
ncs/admin(config-GigabitEthernet)# shutdown
```

Related Commands

Command	Description
interface	Configures an interface type and enters interface mode.
ip address (interface configuration mode)	Sets the IP address and netmask for the Ethernet interface.
show interface	Displays information about the system IP interfaces.
ip default-gateway	Sets the IP address of the default gateway of an interface.

snmp-server community

To set up the community access string to permit access to the Simple Network Management Protocol (SNMP), use the **snmp-server community** command in configuration mode. To disable this function, use the **no** form of this command.

[no] snmp-server community *word* **ro**

Syntax Description

word	Accessing string that functions much like a password and allows access to SNMP. No blank spaces allowed. Up to 255 alphanumeric characters.
ro	Specifies read-only access.

Command Default

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

The **snmp-server community** command requires a community string and the **ro** argument; otherwise, an error occurs.

Examples

```
ncs/admin(config)# snmp-server community new ro
ncs/admin(config)#
```

Related Commands

Command	Description
snmp-server host	Sends traps to a remote system.
snmp-server location	Configures the SNMP location MIB value on the system.
snmp-server contact	Configures the SNMP contact MIB value on the system.

snmp-server contact

To configure the SNMP contact Management Information Base (MIB) value on the system, use the **snmp-server contact** command in configuration mode. To remove the system contact information, use the **no** form of this command.

[no] snmp-server contact *word*

Syntax Description

word	String that describes the system contact information of the node. Up to 255 alphanumeric characters.

Command Default

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

None.

Examples

```
ncs/admin(config)# snmp-server contact Abcd
ncs/admin(config)#
```

Related Commands

Command	Description
snmp-server host	Sends traps to a remote system.
snmp-server community	Sets up the community access string to permit access to the SNMP.
snmp-server location	Configures the SNMP location MIB value on the system.

snmp-server host

To send SNMP traps to a remote user, use the **snmp-server host** command in configuration mode. To remove trap forwarding, use the **no** form of this command.

[no] snmp-server host {*ip-address* | *hostname*} **version** {1 | 2c} *community*

Syntax Description

ip-address	IP address of the SNMP notification host. Up to 32 alphanumeric characters.
hostname	Name of the SNMP notification host. Up to 32 alphanumeric characters.
version {1 | 2c}	(Optional) Version of the SNMP used to send the traps. Default = 1. If you use the version keyword, specify one of the following keywords: • 1—SNMPv1. • 2c—SNMPv2C.
community	Password-like community string that is sent with the notification operation.

Command Default

Disabled.

Command Modes

Configuration

Usage Guidelines

The command takes arguments as listed; otherwise, an error occurs.

Examples

```
ncs/admin(config)# snmp-server community new ro
ncs/admin(config)# snmp-server host 209.165.202.129 version 1 password
ncs/admin(config)#
```

Related Commands

Command	Description
snmp-server community	Sets up the community access string to permit access to SNMP.
snmp-server location	Configures the SNMP location MIB value on the system.
snmp-server contact	Configures the SNMP contact MIB value on the system.

snmp-server location

To configure the SNMP location MIB value on the system, use the **snmp-server location** command in configuration mode. To remove the system location information, use the **no** form of this command.

[no] snmp-server location *word*

Syntax Description

word	String that describes the physical location information of the system. Up to 255 alphanumeric characters.

Command Default

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

We recommend that you use underscores (_) or hyphens (-) between the terms within the *word* string. If you use spaces between terms within the *word* string, you must enclose the string in quotation marks (“).

Examples

Example 1

```
ncs/admin(config)# snmp-server location Building_3/Room_214
ncs/admin(config)#
```

Example 2

```
ncs/admin(config)# snmp-server location “Building 3/Room 214”
ncs/admin(config)#
```

Related Commands

Command	Description
snmp-server host	Sends traps to a remote system.
snmp-server community	Sets up the community access string to permit access to SNMP.
snmp-server contact	Configures the SNMP location MIB value on the system.

username

To add a user who can access the Cisco ISE-3315 using SSH, use the **username** command in configuration mode. If the user already exists, the password, the privilege level, or both change with this command. To delete the user from the system, use the **no** form of this command.

[no] username *username* **password** {**hash** | **plain**} *password* **role** {**admin** | **user**] [**disabled** [**email** email-address]] [**email** email-address]

For an existing user, use the following command option:

username username **password role** {admin | **user**} password

Syntax Description

username	You should enter only one word which can include hyphen (-), underscore (_) and period (.). **Note** Only alphanumeric characters are allowed at an initial setup.
password	The command to use specify password and user role.
password	Password character length up to 40 alphanumeric characters. You must specify the password for all new users.
hash | plain	Type of password. Up to 34 alphanumeric characters.
role admin | user	Sets the privilege level for the user.
disabled	Disables the user according to the user's email address.
email *email-address*	The user's email address. For example, user1@example.com.

Command Default

The initial user during setup.

Command Modes

Configuration

Usage Guidelines

The **username** command requires that the username and password keywords precede the hash | plain and the admin | user options.

Examples

Example 1

```
ncs/admin(config)# username admin password hash ###### role admin
ncs/admin(config)#
```

Example 2

```
ncs/admin(config)# username admin password plain Secr3tp@swd role admin
ncs/admin(config)#
```

Example 3

```
ncs/admin(config)# username admin password plain Secr3tp@swd role admin email
admin123@example.com
ncs/admin(config)#
```

Related Commands

	Description
password-policy	Enables and configures the password policy.
show users	Displays a list of users and their privilege level. It also displays a list of logged-in users.