Cisco Cloud Services Platform Command Reference

First Published: 2018-10-15
Last Updated: 2020-12-21

Contents

Overview

Information About Cisco Cloud Services Platform

Cisco Cloud Services Platform (CSP) is a software and hardware platform for data center network functions virtualization (NFV). This open kernel virtual machine (KVM) platform, with Red Hat Enterprise Linux (RHEL) as the base operating system, is designed to host networking virtual services. Cisco CSP provides REST APIs, a web interface, and a CLI for creating and managing the virtual machine (VM) lifecycle.

Command Modes

EXEC Command Mode

When you first log in, the Cisco CSP 2100 software places you in the EXEC mode. The commands available in the EXEC mode include the **show** commands that display the device status and configuration information, the **system** commands, and other commands that perform actions that you do not save in the device configuration.

Global Configuration Mode

You use the config terminal command to enter the global configuration mode, which provides access to the broadest range of commands. As indicated by the term, global configuration allows configuration of characteristics or features that affect the device as a whole. You can enter commands in the global configuration mode to configure your device globally or to enter more specific configuration modes to configure specific elements such as clusters or pNICS.

When you enter the global configuration mode, the CLI prompt changes to indicate that you are in the global configuration mode.

Example

```
csp# config terminal
csp(config)#
```

Other Command Modes

From within the global configuration mode, you can enter a number of other command modes to configure other elements. To enter these command modes, you enter the command mode and the name of the element you want to create, modify, or delete. The CLI prompt changes when you enter the new mode. It indicates the name of the new mode and the name of the element. The following table lists various command modes.

Mode	Access Method	Example
Cluster configuration	From the global configuration mode, use the following command: cluster *name*	`csp(config)# cluster cluster1` `csp(config-cluster-cluster1)#`
pNIC and Port Channel configuration	From the global configuration mode, use the following command: pnic *name*	`csp(config)# pnic Eth4-0` `csp(config-pnic-Eth4-0)#`
Service configuration	From the global configuration mode, use the following command:	`csp(config)# service vsm-sf` `csp(config-service-vsm-sf)#`

Mode	Access Method	Example
	service *name*	

Exiting a Command Mode

When you exit a command mode using the exit command, you are simply reverted to the previous command level. When you use the end command, Cisco CSP 2100 prompts you to commit any changes before exiting the current command mode.

Almost every configuration command has a no form that can be used to disable a feature, revert to a default value, or remove a configuration. However, if a service is using a feature, you might not able to remove the feature configuration. For example, you cannot disable the SR-IOV support if any existing service is already using this feature. This reference guide mentions about the no form of the command whenever a no form of the command is available.

Example

```
csp# config terminal
csp(config)# no cluster name
csp(config-cluster-name)# commit
```

Completing a Command

At the end of a command, you can enter a question mark (?) to list all possible keywords and arguments that you can use at that point in the command. Cisco CSP 2100 returns one or more of the following:

- Possible completions–Keywords and actual values of objects that have already been created (such as names of port channels or pNICs) that you can use in your configuration.
- Possible match completions–Keywords and arguments that programmatically can work with the command but might not be available because certain objects or features have not been set up yet.
- <cr> Carriage Return–No additional keywords or arguments are required for the command. In some cases, there might be a default value that is applied.

Conventions

This document uses the following conventions.

Convention	Indication
bold font	Commands and keywords and user-entered text appear in bold font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
courier font	Terminal sessions and information the system displays appear in `courier` font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Commands

Authentication, Authorization, and Accounting (AAA) Commands

aaa authentication

To specify the server and caching time to be used for AAA, use the aaa authentication command.

aaa authentication *authentication_server* rest_req_caching_tmout *rest_req_caching_tmout*

Syntax Description

Parameter	Description
authentication_server	Specifies the server for AAA. Valid values are: • tacacs: TACACS+ server. This is the default server. • radius: RADIUS server.
rest_req_caching_tmout	Specifies the time in seconds to cache the external authentication responses for the REST API requests. Valid values (in seconds) are:

	• 1-600: Caching is enabled. • 0: Caching is disabled.

Command Modes

Global configuration (config)

Examples

```
Example for specifying the authentication server
csp# config terminal
csp (config)# aaa authentication tacacs

Example for specifying the caching time
csp# config terminal
csp(config) # aaa rest_req_caching_tmout 100
```

show running-config aaa

To display the running configuration information for AAA, use the show running-config aaa command.

show running-config aaa

Command Modes

EXEC mode

Example

```
csp# show running-config aaa
aaa authentication tacacs
aaa rest_req_caching_tmout 0
```

Command History

Release	Modification
2.7.0	This *rest_req_caching_tmout* parameter is introduced.
2.2.0	This show running-config aaa command is introduced.

Command History

Banner Commands

banner login

To configure a pre-login banner that is displayed before a user logs in to the Cisco CSP 2100, use the banner login command. To revert to the default or remove the configured banner, use the no form of this command. This banner is displayed on the login page of the web interface and the Cisco CSP 2100 CLI window.

banner login *filename*

After configuring the pre-login banner, if you make any changes in the banner file, you must do the following:

1. Remove the banner file by using the no banner login command.
2. Add the banner file again in the configuration by using the banner login *filename* command.

Changes made in the banner file are not automatically updated in the pre-login banner.

Syntax Description

Parameter	Description
filename	Name of the banner file available in the Cisco CSP 2100 repository. The banner file can be up to 1024 bytes in size. You can use the copy image command to copy the banner file.

Command Modes

Global configuration (config)

Examples

```
csp# show repository
Local storage:
File Name                                     Last Modified                Size
n1000v-dk9.5.2.1.SV3.1.4.iso                  Mon Feb 15 23:17:48 2016      231815168
vwaas150.tmpl                                 Tue Feb 16 00:30:49 2016      864
nexus-1000v.5.2.1.VSG2.1.4.iso                Wed Nov 30 02:36:19 2016      149960704
banner.txt                                    Tue Mar 11 00:30:49 2016      348
```

Configuring the Pre-Login Banner

```
csp# config terminal
csp (config)# banner login banner.txt
csp (config)# commit
csp (config)# exit
```

Removing the Configured Pre-Login Banner

```
csp# config terminal
csp# no banner login
csp (config)# commit
csp (config)# exit
```

Command History

Release	Modification
2.1.0	This command is introduced.

banner motd

To configure the message-of-the-day (MOTD) banner that is displayed after a user logs in to the Cisco CSP 2100, use the banner motd command. To revert to the default or remove the configured banner, use the no form of this command. This banner is displayed in the web interface and the Cisco CSP 2100 CLI window.

banner motd *filename*

After configuring the MOTD banner, if you make any changes in the banner file, you must do the following:

1. Remove the banner file by using the no banner motd command.
2. Add the banner file again in the configuration by using the banner motd *filename* command.

Changes made in the banner file are not automatically updated in the MOTD banner.

Syntax Description

Parameter	Description
filename	Name of the banner file available in the Cisco CSP 2100 repository. The banner file can be up to 1024 bytes in size. You can use the copy image command to copy the banner file.

Command Modes

Global configuration (config)

Examples

```
csp# show repository
Local storage:
File Name                                     Last Modified                Size
n1000v-dk9.5.2.1.SV3.1.4.iso                  Mon Feb 15 23:17:48 2016      231815168
vwaas150.tmpl                                 Tue Feb 16 00:30:49 2016      864
nexus-1000v.5.2.1.VSG2.1.4.iso                Wed Nov 30 02:36:19 2016      149960704
motd.txt                                      Tue Mar 11 00:30:49 2016      400
```

Configuring the MOTD Banner

```
csp# config terminal
csp (config)# banner motd motd.txt
csp (config)# commit
csp (config)# exit
```

Removing the Configured MOTD Banner

```
csp# config terminal
csp# no banner motd
csp (config)# commit
csp (config)# exit
```

Command History

Release	Modification
2.1.0	This command is introduced.

Certificate Commands

Installing an SSL certificate consists of the following main tasks:

1. Generate a certificate request using the certificate request command.
2. Send the certificate request to a Certificate Authority to obtain an SSL certificate.
3. Install the certificate using the certificate install-certificate command.

For detailed information about the steps for installing an SSL certificate, see the *Cisco Cloud Services Platform Quick Start Guide*.

certificate request

To create a Certificate Signing Request (CSR), use the certificate request command.

certificate request sha {sha1 | sha256} keysize {1024 | 2048}

Syntax Description

Parameter	Description
sha	Specifies the sha algorithm. Valid choices are sha1 and sha256.
keysize	Specifies the key size. Valid choices are 1024 and 2048.

Command Modes

EXEC command mode (csp#)

Usage Guidelines

When you run the certificate request command, you are prompted for the following information: state or province name, locality name, organization name, organizational unit name, common name, email address, a challenge password, and an optional company name.

The common name is the DNS name of the host including the domain name, for example, myserver.mycompany.com. After you specify the required information, the following two files are created in the certificates directory.

- myhost.csr: The server certificate request file.

  Send the myhost.csr file to a Certification Authority (CA) to obtain an SSL certificate and then use the certificate install-certificate command to install the certificate.

- myPrivate.key: The server key file.

Note: We recommend that you also keep a copy of these files on a different server.

Example

```
csp# certificate request sha sha256 keysize 2048
Entering configuration mode terminal
Generating a 2048 bit RSA private key
.....................................+++
......................+++
writing new private key to '/osp/certificates/myPrivate.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:US
State or Province Name (full name) []: Massachusetts
Locality Name (eg, city) [Default City]: Boxborough
Organization Name (eg, company) [Default Company Ltd]: Cisco
Organizational Unit Name (eg, section) []: CSP
Common Name (eg, your name or your server's hostname) []:myserver1.mycompany.com
Email Address []:xyz@cisco.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
csp#
```

Command History

Release	Modification
1.0	This command is introduced.

certificate install-certificate

To install an SSL certificate, use the certificate install-certificate command.

certificate install-certificate CertificateFile *certificatefile* ChainFile *chainfile* KeyFile *keyfile* localhost *localhost*

Note: Before running this command, copy the SSL certificate files that you received from the CA to the certificates directory using the scp: command.

To verify that the certificate is installed, log in to the Cisco CSP web interface using a web browser and click on the lock im displayed in the address bar. The information about the installed certificate is displayed. For information about accessing the Cisco CSP web interface, see the *Cisco Cloud Services Platform Quick Start Guide*.

Syntax Description

Parameter	Description
CertificateFile *certificatefile*	Specifies the name of the certificate file received from the CA. The certificate file must be available in the certificates directory.
ChainFile *chainfile*	Specifies the name of the chain file received from the CA. The chain file must be available in the certificates directory.
KeyFile *keyfile*	Specifies the name of the key file (myPrivate.key) created using the certificate request command. The key file must be available in the certificates directory.
localhost *localhost*	Specifies the name of the local host.

Command Modes

EXEC command mode (csp#)

Example

```
csp# certificate install-certificate
Value for 'localhost' (<string>): myserver.mycompany.com
Value for 'CertificateFile' (<string>): Mycert.crt
Value for 'KeyFile' (<string>): myPrivate.key
Value for 'ChainFile' (<string>): myChainFile.crt
csp#
```

Command History

Release	Modification
1.0	This command is introduced.

certificate default-certificate

To install the default certificate provided with Cisco CSP 2100, use the certificate default-certificate command.

certificate default-certificate

Note: The default self-signed certificate provided with Cisco CSP 2100 is only for temporary use. You must generate and install an SSL certificate on Cisco CSP 2100 using the certificate request and certificate install-certificate commands.

Command Modes

EXEC command mode (csp#)

Example

```
csp# certificate default-certificate
results success
csp#
```

Command History

Release	Modification
1.0	This command is introduced.

certificate delete-certificate

To delete a certificate, use the certificate delete-certificate command.

certificate delete-certificate certname *certificatefile*

Syntax Description

Parameter	Description
certname *certificatefile*	Specifies the name of the certificate file to be deleted.

Command Modes

EXEC command mode (csp#)

Example

```
csp# certificate delete-certificate certname server.pem
results success deleted server.pem
csp#
```

Command History

Release	Modification
1.0	This command is introduced.

copy certificate

To copy a certificate from a remote location to Cisco CSP 2100, use the copy certificate command.

Note: From release 2.3.0, you cannot copy a certificate from CSP 2100. Hence, if you are using versions earlier than 2.3.0, you can copy a certificate to and from CSP 2100.

copy certificate *source_file destination_file*

Syntax Description

Parameter	Description
source_file	Source URL and the name of the file to be copied in the following format: `user@host:file`. The source can be remote.
destination_file	Destination URL and the name with which the file is copied. The destination can be either local or remote. Note: If you are copying a certificate file to Cisco CSP 2100, you cannot change the name of the copied file. Specify a period (.) instead of the filename to copy a certificate file to Cisco CSP 2100.

Command Modes

EXEC mode

Examples

```
Example for copying to the Cisco CSP 2100
csp# copy certificate user1@myhost:/temp_cert.pem .
```

Command History

Release	Modification
2.2.2	This command is introduced.

show certificates

To display the certificates available in the certificates directory, use the show certificates command.

show certificates

Command Modes

EXEC command mode (csp#)

Example

```
csp# show certificates
server-chain.crt          Tue Aug 11 12:08:39 2015           1375
hostname_stackedChain.pem Thu Aug 13 08:21:08 2015           6749
server.pem                Tue Aug 11 12:08:39 2015           3050
yourPrivateKey.key        Thu Aug 13 08:20:22 2015           1704
csp#
```

Command History

Release	Modification
1.0	This command is introduced.

show certificates certificate *filename*

To display the certificates available in the server certificate request file, use the show certificates certificate *filename* command.

show certificates certificate *filename*

Syntax Description

Parameter	Description
filename	Specifies the name of the server certificate request file.

Command Modes

EXEC command mode (csp#)

Example

```
csp# show certificates certificate myhost.csr
-----BEGIN CERTIFICATE REQUEST-----
MIICvDCCAaQCAQAwdzELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAkNBMRUwEwYDVQQH
DAxEZWZhdWx0IENpdHkxDjAMBgNVBAoMBUNJU0NPMRIwEAYDVQQDDAljaXNjb2MI
LAgxIDAeBgkqhkiG9w0BCQEWEXNoaXYxNTJAZ21haWwuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxWeVHk9fkmhwl/e1TV2E5K58XrHQbSsWSEaX
d0zNdJrof5+odggdioCs4TaIUrVm7iaIs36+OaigVNnKSWboiI1b6b2QGA9kLxM2
Pv48px9qy6toic+mPZy3++FYFMb7dNyYP2GjOl9M3vTkwMFO5UNOJ9EUVWXHRngR
8Lj1fx7SGeNVBZFAIjVuy05hNVjBpXjdBvClRl1HjRlEiFsgI4SWAXfU9oRsDzdc
CLyGsz/OKeR8KMrQc2kJ98t1Y2TrpJ7FOxoxRxkVD+3mHUvIVhm683WYViID78k+
85LikApIzfSDfYuWm3BLkOP1rB4FccylfX8xAXsH6LafY+ovwQIDAQABoAAwDQYJ
KoZIhvcNAQELBQADggEBAL00MIafHKkmzbdtMjeeiZIw5bZhgNdgSOI6208p7kDK
T6ZejYsj/qIoIgpqKCj+WNqR2SxsCXaMd1W54vZIwWglBXHtsAXAEFzQrtEArXbn
s2oBI/v83ReSHxrQHohkPxTlkPQaFsI3+lhZozP9y81g/d4Kc/Rjdj/6kxERSyBe
ufbIikpx0abfPaSb44WC2oAIkmRlPamgm0B03rLuDA31uUvYWl/zO2PIsYgeiksw
8x0hpeZInjYFtPZmfKmtmDw1DsuUIwvG/Nf9djScdrGCsR9vYZV7LODQR0+FZ/nL
zB8GD9NTCd3NF+SZ9uq4EUtiVsptAu/dXCpishpKJQ8=
-----END CERTIFICATE REQUEST---
```

Command History

Release	Modification
2.3.0	This command is introduced.

Configuration File Commands

You can use the configuration file commands described in this section to save the running configuration to the repository and to load the running configuration from the repository to Cisco CSP 2100. If you had to perform a clean installation of Cisco CSP 2100 for any reason, these commands enable you to quickly restore the Cisco CSP 2100 configuration settings. For information about saving a running configuration and then loading it, see the Cisco Cloud Services Platform Configuration Guide.

save config-file

To save a running configuration, use the save config-file command.

save config-file *filename*

Syntax Description

Parameter	Description
filename	Name of the file in which the configuration is saved. This file is saved in the Cisco CSP 2100 repository. To view the file, you can use the show repository command. To copy the file from Cisco CSP 2100 repository to a remote location, you can use the copy image command.

Command Modes

EXEC command mode (csp#)

Global configuration (config)

Example

```
csp# save config-file savefile.sav
csp#
```

Command History

Release	Modification
2.1.0	This command is introduced.

load config-file

To load a configuration from a file, use the load config-file command.

load config-file *filename*

Syntax Description

Parameter	Description
filename	Name of the configuration file available in the Cisco CSP 2100 repository. Note: You must also copy the appropriate files, such as the service ISO file (specified in iso_name) and banner files, required by the saved configuration file to the Cisco CSP 2100 repository.

Command Modes

EXEC command mode (csp#)

Global configuration (config)

Example

```
csp# load config-file savefile.sav
csp#
```

Command History

Release	Modification
2.1.0	This command is introduced.

Cluster Commands

cluster

To create or modify a cluster, use the cluster command. Clusters enable you to make configuration changes to all other Cisco CSP 2100 members of a cluster by using the web interface of a Cisco CSP 2100 cluster member. If you configure CSP 2100 cluster through the cluster command, the same configuration needs to be repeated on every cluster member. However, if you configure CSP 2100 cluster from the web interface, the same configuration is automatically pushed to the remaining cluster members. To delete a cluster, use the no form of this command.

cluster *name*

Note: When creating a cluster, you must configure the local node in the cluster. After creating a cluster, assign members to this cluster by using the node command.

Note: All cluster member nodes must have at least one common user account with same username and password. When these credentials are used for logging in, you can view the entire cluster information.

Syntax Description

Parameter	Description
name	Cluster name

Command Modes

Global configuration (config)

Usage Guidelines

After you are satisfied with the configuration, enter the commit command to save the running configuration to the startup configuration persistently through reboots and restarts.

Examples

```
csp# config terminal
csp(config)# cluster my_cluster
csp(config-cluster-cluster1)# node 192.0.2.10
csp(config-cluster-cluster1)# node 192.0.2.11
csp(config-cluster-cluster1)# commit
csp(config-cluster-cluster1)# exit
csp(config)# exit
csp#

csp# config terminal
csp(config)# no cluster my_cluster
csp(config)# exit
csp#
```

Command History

Release	Modification
2.5.0	The cluster command has been deprecated.
1.0	The cluster command is introduced.

node

To add a node to a cluster, use the node command. To delete a node from a cluster, use the no form of this command.

node *ip-address*

Syntax Description

Parameter	Description
ip-address	IP address of the cluster node.

Command Modes

Cluster configuration (config-cluster-*cluster-name*)

Usage Guidelines

After you are satisfied with the configuration, enter the commit command to save the running configuration to the startup configuration persistently through reboots and restarts.

Example

```
csp# config terminal
Entering configuration mode terminal
csp(config)# cluster my_cluster
csp(config-cluster-cluster1)# node 192.0.2.10
csp(config-cluster-cluster1)# node 192.0.2.11
csp(config-cluster-cluster1)# commit
Commit complete.
csp(config-cluster-cluster1)# exit
csp(config)#
csp#
```

Command History

Release	Modification
2.5.0	The node command has been deprecated.
1.0	The node command is introduced.

show running-config cluster

To display the running configuration information for all clusters or a specific cluster, use the show running-config cluster command.

show running-config cluster [*name*]

Syntax Description

Parameter	Description
name	Cluster name

Command Modes

EXEC mode

Example

```
csp# show running-config cluster my_cluster
```

```
clusters my_cluster
node 192.0.2.11
 !
node 192.0.2.13

!
csp#
```

Command History

Release	Modification
2.5.0	The show running-config cluster command has been deprecated.
1.0	The show running-config cluster command is introduced.

show cluster

To display the configuration information for a cluster, use the show cluster command.

show cluster

Command Modes

EXEC mode

Example

```
csp#show cluster
NAME   MEMBER   IP   STATE
--------------------------
my_cluster 192.0.2.11 UP detected at Thu Aug 11 10:33:01 2016
192.0.2.13 UP detected at Thu Aug 11 10:33:01 2016
csp#
```

Command History

Release	Modification
2.5.0	The show cluster command has been deprecated.
1.0	The show cluster command is introduced.

show cluster version

To display the system supported version for a cluster, use the show cluster version command.

show cluster version

Command Modes

EXEC mode

Example

```
csp#show cluster version
System supported Cluster Version: 3
```

Command History

Release	Modification
2.8.0	The show cluster version command is introduced.

Factory Default Reset Command

factory-default-reset all

To reset Cisco CSP 2100 to factory-default configuration, use the factory-default-reset all command.

factory-default-reset all

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC command mode (csp#)

Usage Guidelines

When you run this command, it deletes VMs and volumes, files including logs, images, certificates, and erases all configuration. Connectivity is lost and admin password is changed to factory default password.

After factory reset process is complete, Cisco CSP 2100 reboots automatically and you are prompted with the configuration services questionnaire similar to clean installation. For more information about how to set up your Cisco CSP through clean installations, see the *Cisco Cloud Services Platform Quick Start Guide*.

Note: We recommend that you do not perform any operation for around 15 to 20 minutes while the factory reset process is in progress.

After factory-reset of ovs-dpdk enabled device, the device resets back to factory default ovs-dpdk disabled setting. For more information about the ovs dpdk configuration, see the OVS DPDK commands.

Example

```
csp# factory-default-reset all
Are you sure you want to perform factory reset? [yes,no] yes
csp# commit
```

Command History

Release	Modification
2.2.5	This command is introduced.

Installation and Upgrade Commands

Release 2.1.0 and Later Releases

system

To install or upgrade Cisco CSP 2100 by using an ISO image or to reboot the Cisco CSP 2100, use the system command.

system [install [iso [mode {clean-install | software-update}] [update image *imagename*]]] [reboot]

Note:

- To upgrade the Cisco CSP 2100 software by using the system install iso update image *imagename* command, Cisco FlexFlash must be enabled in the Cisco Integrated Management Controller (CIMC). To enable the Cisco FlexFlash or to check that the Cisco FlexFlash is enabled, in the CIMC, click Storage > Cisco FlexFlash and then click the Virtual Drive Info tab. For detailed configuration information about the CIMC, see Cisco Integrated Management Controller Configuration Guides.
- You cannot use the system install iso update image *imagename* command to upgrade the Cisco CSP 2100 software from Release 2.1.x to Release 2.2.0. Use the CIMC console to upgrade the Cisco CSP 2100 software from Release 2.1.x to Release 2.2.0. You can use this command to upgrade from Release 2.2.0 to later versions.

Syntax Description

Parameter	Description
install	Specifies that it is an ISO or RPM installation.
iso	Specifies that the installation is done using an ISO file.
mode	Specifies the installation mode for ISO installation. This parameter only specifies the installation mode; it does not initiate the installation. Valid modes are: • clean-install: Specifies to not retain any existing configurations and settings in the new installation. • software-update: Specifies to retain the existing configurations and settings in the new installation.
update image *imagename*	Initiates an ISO installation and specifies the name of the Cisco CSP 2100 ISO software update image available in the Cisco CSP 2100 repository.
reboot	Reboots the Cisco CSP 2100.

Command Modes

EXEC command mode (csp#)

Usage Guidelines

When you run this command, it takes around 15 minutes for Cisco CSP 2100 to prepare the image and then reboot to complete the installation. The SSH connection to the Cisco CSP 2100 is dropped when the reboot happens. You can reconnect to the Cisco CSP 2100 only after the reboot.

Examples

```
csp# system install iso mode software-update
csp# system install iso update image csp-2100-210.iso
This command will take several minutes and reboot the system. Is the install mode set correctly? Are you
sure ? [no,yes] yes
Connection to 192.0.2.1 closed by remote host.
Connection to 192.0.2.1 closed.
```

Command History

Release	Modification
2.1.0	This command is introduced.

Release 1.0 and 2.0.0

system install mode

To specify the installation mode for installing Cisco CSP 2100 by using an ISO image, use the system install mode command. This command only specifies the installation mode. It does not initiate the Cisco CSP 2100 installation.

system install mode {clean-install | update-software}

Syntax Description

Parameter	Description
clean-install	Specifies to not retain any existing configurations and settings in the new installation.
update-software	Specifies to retain the existing configurations and settings in the new installation.

Defaults

update-software mode

Command Modes

EXEC command mode (csp#)

Example

```
csp# system install mode clean-install
csp#
```

Command History

Release	Modification
2.1.0	This command is removed.
1.0	This command is introduced.

package-install update

To upgrade the Cisco CSP 2100 software by using a package file, use the package-install update command.

package-install update package-file *filename*

Syntax Description

Parameter	Description
package-file *filename*	Name of the package file available in the Cisco CSP 2100 repository.

Command Modes

EXEC command mode (csp#)

Usage Guidelines

When you run this command, the CLI is restarted. The results of the package-install update command are included in the csp_update_rpm.out log file in the log directory.

To check the upgrade status, run the package-install show-upgrade-status command described in the next section.

Example

```
csp# package-install update package-file cisco-csp-1.0.0-10.el7.x86_64.rpm
results: software update process will continue in background...
csp#
```

Command History

Release	Modification
2.1.0	This command is removed.
1.0	This command is introduced.

package-install show-upgrade-status

To check the status of the software upgrade done through the package-install update command, use the package-install show-upgrade-status command.

package-install show-upgrade-status

Command Modes

EXEC command mode (csp#)

Usage Guidelines

When you run this command, it may show intermediate update status, such as, `stopping services`. When the software upgrade process is completing, the CLI session is terminated. After logging in to the CLI, when you run this command again, the status shows the `Install Complete` message along with the timestamp indicating the time when the software upgrade process finished.

Examples

```
csp# package-install show-upgrade-status
upgrade-status : (Thu Jul 23 09:29:59 EDT 2015) Stopping services...

Welcome to the Cisco Cloud Services Platform CLI
admin connected from 192.0.2.1 using ssh on csp
csp# package-install show-upgrade-status
upgrade-status : (Thu Jul 23 09:30:14 EDT 2015) Install Complete
csp#
```

Command History

Release	Modification
2.1.0	This command is removed.
1.0	This command is introduced.

Patch Upgrade Commands

Before using the patch upgrade command, ensure that the following conditions are met:

- The patch package file must reside in the CSP repository. You can place the package file by using either GUI based file upload or copy through CSP CLI.
- The CSP releases mechanisms include the following workflow for patch upgrade:

  For example: Suppose for CSP release, CSP 2.X.Y, where X is the minor version and Y is the patch version. A patch upgrade can be applied to CSP if the patch minor version matches with the current minor version of target CSP and patch version is later than the current patch version of CSP.

patch-upgrade rel-notes

To list the bugs addressed by patch package file, use the system install patch-upgrade rel-notes command.

system install patch-upgrade rel-notes package-file *filename*

Syntax Description

Parameter	Description
package-file *filename*	Name of the package file available in the Cisco CSP 2100 repository.

Command Modes

EXEC command mode (csp#)

Example

```
csp# system install patch-upgrade rel-notes package-file csp-2100-nightly-70.tar.gz
results RELEASE NOTES
results =============
results CSCvXXXXX - Vm not booting when NFS is down
results CSCvYYYYY - Cluster certs not working with FQDN
csp#
```

Command History

Release	Modification
2.6.0	This command is introduced.

patch-upgrade update

To update the CSP software from current version to its next patch version by using patch package file, use the system install patch-upgrade update command.

system install patch-upgrade update package-file *filename*

Syntax Description

Parameter	Description
package-file *filename*	Name of the package file available in the Cisco CSP 2100 repository.
force *force*	Enables or disables the upgrade of CSP software during failure. Valid values are true and false.

Command Modes

EXEC command mode (csp#)

Example

```
csp# system install patch-upgrade update package-file csp-2100-70.tar.gz force true
Are you sure you want to install this patch-upgrade software update? [no,yes] yes
results Starting patch upgrade
results Performing validation checks on the upgrade package file
results Validation checks passed, upgrading csp from 02.05.00.06 to 02.05.01
results Installing upgrade software in the background, check installation status after 5 mins
```

Command History

Release	Modification
2.6.0	This command is introduced.

patch-upgrade check-status

To check the status of patch upgrade operation process, use the system install patch-upgrade check-status command.

system install patch-upgrade check-status

Syntax Description

None

Command Modes

EXEC command mode (csp#)

Example

```
csp# system install patch-upgrade check-status
results update_status: 12/02/2019, 18:05:04 - Validating upgrade tar ball - success
results update_status: 12/02/2019, 18:05:04 - Patch upgrade in progress
results update_status: 12/02/2019, 18:05:25 - Patch upgrade complete
csp#
```

Command History

Release	Modification
2.6.0	This command is introduced.

NTP Server Commands

ntp

To add an NTP server, use the ntp command. To delete an NTP server, use the no form of this command.

ntp *ntp_server*

Syntax Description

Parameter	Description
ntp_server	Hostname or IP address of the NTP server

Command Modes

Global configuration (config)

Examples

Example for using the IP address of the NTP server

```
csp# config terminal
csp(config)# ntp 1.2.3.4
csp (config-ntp-1.2.3.4)# commit
Commit complete.
csp (config-ntp-1.2.3.4)# end
```

Example for using the host name of the NTP server

```
csp# config terminal
csp(config)# ntp time.cisco.com
csp (config-ntp-time.cisco.com)# commit
Commit complete.
csp (config-ntp-time.cisco.com)# end
```

Command History

Release	Modification
2.0.0	This command is introduced.

show ntp

To display the status of the NTP server, use the show ntp command.

show ntp

Command Modes

EXEC mode

Example

```
csp# show ntp
remote           refid           st t when poll reach   delay   offset  jitter
==============================================================================
 1.2.3.4         .INIT.          16 u    -   64    0    0.000    0.000   0.000
*gmt-mgmt.cisco. 192.0.2.1       2  u   66  64    1   77.745    0.666   0.000
```

Command History

Release	Modification
2.0.0	This command is introduced.

show running-config ntp

To display the running configuration information for all NTP servers or a specific NTP server, use the show running-config ntp command.

show running-config ntp [*ntp_server*]

Syntax Description

Parameter	Description
ntp_server	Host name or IP address of the NTP server

Command Modes

EXEC mode

Example

```
csp# show running-config ntp
ntp 1.2.3.4
!
ntp time.cisco.com
!
```

Command History

Release	Modification
1.0	This command is introduced.

OVS DPDK Commands

ovs-dpdk enable

To enable or disable the Open vSwitch (OvS) with Data Plane Development Kit (DPDK) mode, use the ovs-dpdk enable command.

ovs-dpdk disable enable

Ensure that the following points are considered when enabling ovs-dpdk configuration.

- ovs-dpdk support is enabled only for 10G interfaces.
- Management interface does not support ovs-dpdk configuration.
- At least 2 vhost CPUs should be free for enabling DPDK.
- 32GB free host memory should be available.
- CPU pinning must be enabled.

- 10G NICs supported for DPDK are Niantic and Fortville.

Command Modes

EXEC command mode (csp#)

Usage Guidelines

By default, ovs-dpdk is disabled on upgrade and clean install modes. DPDK offers poll mode drivers that enables direct transfer of packets between user space and physical interface, and bypass kernel network stack.

Starting with release 2.5.0, live edit of vNICs is supported when ovs-dpdk is enabled. After a service is deployed with DPDK interface, you can edit dpdk enabled interface to another dpdk enabled interface when VM is powered on. You cannot edit from non-dpdk interface to dpdk interface or vice versa.

Note: The system reboots on enabling or disabling ovs-dpdk.

Example

```
csp# ovs-dpdk enable
csp#
```

Command History

Release	Modification
2.3.0	This command is introduced.

show ovs-dpdk

To display the status of the ovs dpdk, use the show ovs-dpdk command.

show ovs-dpdk

Command Modes

EXEC mode

Example

```
csp# show ovs-dpdk
```

Command History

Release	Modification
2.5.0	Live edit of vNICs is supported when ovs-dpdk is enabled.
2.3.0	This command is introduced.

TPM Encryption Command

tpm-encryption

To enable TPM based disk encryption for sesitive directories of CSP, use the tpm encryption command. By default, tpm encryption command is disabled.

tpm encryption [enable | disable]

Syntax Description

Parameter	Description
disable	Disables tpm based disk encryption on CSP.
enable	Enables tpm based disk encryption on CSP.

Command Modes

Global configuration (config)

Command History

Release	Modification
2.6.0	This command is introduced.

show tpm

To display the status of the tpm based encryption, use the show tpm command.

show tpm

Command Modes

EXEC mode

Example

```
csp# show tpm
tpm hardware-support true
tpm encryption-status encryption_not_configured
```

Command History

Release	Modification
2.6.0	This command is introduced.

Password Expiration Command

password-expiry

To enable or disable password expiry for CSP host, use the password expiry command. By default, the password expiry is enabled for CSP.

password-expiry [enable | disable]

Syntax Description

Parameter	Description
disable	Disables expiry of password on CSP. Therefore, you are not prompted to change password.
enable	Enables expiry of password on CSP.

Parameter	Description
	Default password state is enable.

Command Modes

Global configuration (config)

Command History

Release	Modification
2.4.0	This command is introduced.

show password-expiry

To display the status of password expiry for CSP, use the show password-expiry command.

show password-expiry

Command Modes

EXEC mode

Example

```
csp# show password-expiry
```

Command History

Release	Modification
2.4.0	This command is introduced.

Port Isolation Command

To allow or prevent communication between VNF management ports, use the port isolation command. By default, the command allows communication between VNF management interfaces.

vm switching-mode protected [protected | VEB]

Syntax Description

Parameter	Description
protected	Prevents communication between VNF management ports. Traffic between VNF management ports are blocked.
VEB	Allows communication between VNF management ports. Default mode is VEB.

Command Modes

Global configuration (config)

Example

```
csp# config terminal
```

```
csp(config)# vm switching-mode protected
```

Command History

Release	Modification
2.2.5	This command is introduced.

pNIC Commands

pnic

To modify the configuration of an Ethernet pNIC or to create a port channel, use the pnic command. To set an Ethernet pNIC to its default settings or to delete a port channel, use the no form of the command.

pnic *name* [member_of *portchannel_name*] [adminstatus {up | down}] [lldp {enabled | disabled}] [link-state-tracking {enabled | disabled}] [type port-channel] [bond_mode {active-backup | balance-slb | balance-tcp}] [lacp_type {active | passive | off}] [sr-iov [numVFs *numVFs*] [switchMode *switchmode*]] [trunks *vlan_num*]

Starting from 2.8.0, you can configure the port-channels that have SR-IOV enabled pNICs as subordinate interfaces. The SR-IOV enabled port-channels cannot be assigned to VNFs during deployment because these port-channels are not intended to carry data traffic.

Note: After creating a port channel, you must assign pNICs to the port channel. Similarly, before deleting a port channel, you must unassign the pNICs assigned to it. For more information, see the *Usage Guidelines* section and the *Examples* section.

Syntax Description

Parameter	Description
name	Name of the pNIC or port channel. PNICs are named in Eth<pcie slot>-<port> format. The slot 0 corresponds to LOM port and slot 9 corresponds to mLOM ports. Valid values for Ethernet pNICs are Eth0-1, Eth1-4, Eth1-2.
member_of *portchannel_name*	Associates the pNIC with the specified port channel. Starting from
adminstatus	Shuts down or re-enables a disabled pNIC. Valid values are up and down. This parameter is not available if the pNIC is configured as a passthrough interface.
promiscuous	Specifies the promiscuous mode. Valid values are enabled and disabled. Default is disabled. This parameter is available only when the pNIC is configured as a passthrough interface. When promiscuous mode is enabled, traffic is passed to the vNIC independent of the packet MAC address.

Parameter	Description
lldp	Specifies the LLDP mode. Valid values are enabled and disabled. Default is enabled.
link-state-tracking	Specifies the link state tracking mode. Valid values are enabled and disabled.
type	Specifies the type. Valid values are ethernet and port-channel. Default is ethernet.
bond_mode	Specifies the mode of the bond. Valid values are the following: • balance-slb: In this mode, load balancing is done between the pNIC members of a port channel based on the MAC address. This is the default mode. • active-backup: In this mode, load balancing is done between two members of a port channel. One pNIC acts as the active member and carries all the traffic. The other pNIC acts as the backup member and carries traffic only when the active pNIC fails. • balance-tcp: In this mode, load balancing is done between the pNIC members of a port channel based on the L2, L3, and L4 protocol information such as destination MAC address, IP address, and TCP port. This mode requires the upstream switch to support 802.3ad with successful LACP negotiation. Default is balance-slb.
lacp_type	Specifies the link aggregation control protocol (LACP) for the bond. Valid LACP types are active, passive, and off. Default is off.
sr-iov	Provides SR-IOV support. Note: SR-IOV feature is supported only with 10G and 40G interfaces.
numVFs *numVFs*	Specifies the number of VFs. Up to 63 VFs are supported on a 10G interface, and up to 64 VFs are supported on a 40G interface. Note: • You cannot disable the SR-IOV support if any existing service is already using this feature. To disable the SR-IOV support, use 0 or no pnic *pnic_name* sr-iov numvfs. • To add more VFs to a pNIC, you first need to disable the SR-IOV support and then enable it. • VF interfaces come up only when the physical pNIC is up and running.
switchMode *switchmode*	Specifies the switch mode. Valid values are: • VEB: Virtual Ethernet Bridge mode

Parameter	Description
	• VEPA: Virtual Ethernet Port Aggregator (VEPA) mode. This mode is reserved for switches with a VEPA-capable hardware, that is, switches that support IEEE 802.1Qbg. Default mode is VEB.
trunks *vlan_num*	Specifies the VLANs. Valid range is from 1 to 4096. Default is VLAN 1. Enter VLANs separated by commas, VLAN ranges separated by dashes, or a combination of both.

Command Modes

Global configuration (config)

Usage Guidelines

Port channel creation consists of the following steps:

1. Create a port channel.

   pnic *portchannel_name* type port-channel [bond_mode {active-backup | balance-slb | balance-tcp}] [lacp-type {active | passive | off}] [trunks *vlan_num*]

   Note: If you enable LACP on the port-channel and SR-IOV on pNIC, CSP notifies the VNF when one of the subordinate pNICs links goes down.

2. Assign two or more pNIC members to this port channel by using the member_of parameter:

   Note: Starting from 2.8.0, you can associate the SR-IOV enabled pNICS to the port-channel.

   pnic *name* member_of *portchannel_name*

Port channel deletion consists of the following two steps:

1. Unassign the pNICs assigned to a port channel.

   pnic *name* no member_of

2. Delete the port channel.

   no pnic *portchannel_name*

After you are satisfied with the configuration, enter the commit command to save the running configuration to the startup configuration persistently through reboots and restarts.

Examples

```
Example for modifying an Ethernet pNIC
csp# config terminal
Entering configuration mode terminal
csp(config)# pnic Eth0-1
csp(config-pnic-Eth0-1)# lldp enabled
csp(config-pnic-Eth0-1)# link-state-tracking enabled

csp(config-pnic-Eth0-1)# commit
Commit complete.
csp(config-pnic-Eth0-1)# exit
```

Example for creating a port channel

```
csp# config terminal
csp(config)# pnic pch1
csp(config-pnic-pch1)# type port_channel
csp(config-pnic-pch1)# commit
Commit complete.
csp(config-pnic-pch1)# exit

csp(config)# pnic Eth1-4 member_of pch1
csp(config-pnic-Eth1-4)# commit
Commit complete.
csp(config-pnic-Eth1-4)# exit
csp(config)# pnic Eth1-4 member_of pch1
csp(config-pnic-Eth1-4)# commit
Commit complete.
csp(config-pnic-Eth1-4)# exit
```

Example for configuring port channel that have SR-IOV enabled pNIC

```
csp#
csp# config terminal
csp(config)# pnic sriov_pch
csp(config-pnic-sriov_pch)# type port_channel
csp(config-pnic-sriov_pch)# lacp_type active
csp(config-pnic-sriov_pch)# bond_mode active-backup
csp(config-pnic-sriov_pch)# commit
Commit complete.
csp(config-pnic-sriov_pch)#


csp(config)#
csp(config)# pnic Eth1-2 sr-iov numvfs 5
csp(config-pnic-Eth1-2)# sr-iov switchmode veb
csp(config-pnic-Eth1-2)# commit
Commit complete.
csp(config-pnic-Eth1-2)#
csp(config)# pnic Eth1-4
csp(config-pnic-Eth1-4)# sr-iov numvfs 5
csp(config-pnic-Eth1-4)# sr-iov switchmode veb
csp(config-pnic-Eth1-4)# commit
Commit complete.


csp(config)# pnic Eth1-2 member_of sriov_pch
csp(config-pnic-Eth1-2)# exit
csp(config)# pnic Eth1-4 member_of sriov_pch
csp(config-pnic-Eth1-4)#
csp(config)# commit
Commit complete.
```

Example for deleting a port channel

```
csp(config)# pnic Eth1-2
csp(config-pnic-Eth1-2)# no member_of
csp(config-pnic-Eth1-2)# commit
Commit complete.
csp(config-pnic-Eth1-2)# exit
csp(config)# pnic Eth1-3
csp(config-pnic-Eth1-3)# no member_of
csp(config-pnic-Eth1-3)# commit
Commit complete.
csp(config-pnic-Eth1-3)# exit
csp(config)# no pnic pch1
csp(config)# commit
Commit complete.
csp(config)#
```

Command History

Release	Modification
2.5.0	The pNIC name has been changed to the new format,

Release	Modification
	Eth<slot>-port.
2.4.0	The SR-IOV feature support for 40G interface and no form of pnic *pnic_name* sr-iov numvfs has been added.
2.3.1	The link-state-tracking parameter has been added.
2.1.0	The adminstatus, promiscuous, sr-iov, numVFs, switchMode parameters are added.
2.0.0	The passthrough parameter is removed.
1.0	This command is introduced.

pnic description

To allow you to configure a description on individual pNICs, use the pnic description global configuration command. To remove the configured description, use the no form of this command.

pnic *name* {description *new description*}

no pnic *name* description

Syntax Description

Parameter	Description
name	Name of the pNIC.
description *new description*	Specifies a description for an individual pNIC. Valid values are a string up to 256 characters, underscores, dashes, periods, spaces, and commas. Note: While using spaces, ensure that you use double quotes to enclose the description string.

Command Modes

Global configuration (config)

Example

```
csp(config)# pnic Eth0-1 description "mgmt-pnic, vlan 72"
csp(config-pnic-Eth0-1)# commit
Commit complete.

csp(config)# no pnic Eth1-0 description
csp(config)# commit
Commit complete.
```

Command History

Release	Modification
2.5.0	The PNIC name has been changed to the new format, Eth<slot>-port.

2.3.0	This command is introduced.

show pnic description

To display the description about individual pNICs, use the show pnic description command.

show pnic *name* description

Syntax Description

Parameter	Description
name	Name of the pNIC.

Command Modes

EXEC mode

Example

```
csp# show pnic Eth0-1 description "management PNIC"
VF                        INUSE     SERVICE
IDX  NAME                 FLAG      OWNER
-------------------------------------------
0    Eth2-2_vf0_130s16f1  not-used  none
1    Eth2-2_vf1_130s16f3  not-used  none
2    Eth2-2_vf2_130s16f5  not-used  none
3    Eth2-2_vf3_130s16f7  not-used  none
4    Eth2-2_vf4_130s17f1  not-used  none
5    Eth2-2_vf5_130s17f3  not-used  none
6    Eth2-2_vf6_130s17f5  not-used  none
7    Eth2-2_vf7_130s17f7  not-used  none
```

Command History

Release	Modification
2.5.0	The PNIC name has been changed to the new format, Eth<slot>-port.
2.3.0	This command is introduced.

show pnic

To display all statistics, or only slot or port information about a specific pNIC or all pNICs, use the show pnic command.

show pnic [pnic *name*] [slot | port]

Syntax Description

Parameter	Description
pnic *name*	Specifies the name of the pNIC for which the information is displayed.
slot	Displays the slot information about all pNICs or a specific pNIC.
port	Displays the port information about all pNICs or a specific pNIC.

Command Modes

EXEC mode

Example

```
csp# show pnic
Name          Link   Admin  MTU     Mac               Passthrough    Speed   Rx Bytes      Packets
Errors   Dropped  Mbps   Broadcast Multicast TX Bytes      Packets    Errors   Dropped  Collisions Mbps
Broadcast Multicast
================================================================================================================
================================================================================================================
=========
Eth0-1        up     up     9216    88:f0:31:26:fd:fa none          1G      2473699608    1763195    0
1        0.03   4030      13460     76954973      307601     0        0        0          0.032 16
180
Eth0-2        down   up     9216    88:f0:31:26:fd:fb none          1G      0             0          0
0        0.0    0         0         0             0          0        0        0          0.0   0
0
Eth1-1        up     up     9216    a0:36:9f:3b:95:a4 none          1G      1832063       14950      0
0        0.003  2997      10889     56516         316        0        0        0          0.0   0
316
Eth1-2        up     up     9216    a0:36:9f:3b:95:a5 none          1G      51100         175        0
0        0.0    0         175       31924         180        0        0        0          0.0   0
180
Eth1-3        up     up     9216    a0:36:9f:3b:95:a6 none          1G      52192         174        0
0        0.0    0         174       31920         180        0        0        0          0.0   0
180
Eth1-4        up     up     9216    a0:36:9f:3b:95:a7 none          1G      50808         174        0
0        0.0    0         174       31743         179        0        0        0          0.0   0
179
Eth2-1        down   up     9216    90:e2:ba:76:ce:1c none          10G     0             0          0
0        0.0    0         0         0             0          0        0        0          0.0   0
0
Eth2-2        up     up     9216    90:e2:ba:76:ce:1d none          10G     1910907       16543      0
1        0.004  3910      13361     52893         269        0        0        0          0.0   0
0
```

Command History

Release	Modification
2.5.0	The PNIC name has been changed to the new format, Eth<slot>-port.
2.2.3	The slot and port parameters are added.
1.0	This command is introduced.

show running-config pnic

To display the running configuration information for all pNICs or a specific pNIC, use the show running-config pnic command.

show running-config pnic [*name*] [adminstatus | bond_mode | lacp_type | lldp | link-state-tracking | member_of | trunks | type | sr-iov | promiscuous]

Syntax Description

Parameter	Description
name	Name of the pNIC.
adminstatus	Displays the pNIC with up or down status.
bond_mode	Displays the mode for the bond.
lacp_type	Displays the LACP for the bond.
lldp	Displays the LLDP mode.
link-state-tracking	Displays the link-state-tracking mode.
member_of	Displays the port channel with which a pNIC is associated.
trunks	Displays the VLANs.
type	Displays the pNIC type.
sr-iov	Displays the SR-IOV configuration for the pNIC.
promiscuous	Displays the pNICs with enabled or disabled promiscuous mode.

Command Modes

EXEC mode

Example

```
csp# show running-config pnics
pnics pnic Eth4-1
 type ethernet
 sr-iov numVFs 0
 sr-iov switchMode VEB
 lldp enabled
!
pnics pnic Eth4-1
 type ethernet
 sr-iov numVFs 0
 sr-iov switchMode VEB
 lldp enabled
!
pnics pnic Eth4-1
 type ethernet
 sr-iov numVFs 0
 sr-iov switchMode VEB
 lldp enabled
!
pnics pnic Eth4-1
 type ethernet
 sr-iov totalvfs 7
 lldp enabled
 link-state-tracking enabled
 description test
!
```

Command History

Release	Modification
2.5.0	The PNIC name has been changed to the new format, Eth<slot>-port.
2.3.1	The link-state-tracking parameter has been added.
2.1.0	The adminstatus, sr-iov, and promiscuous parameters are added.
2.0.0	The passthrough parameter removed is from this command.
1.0	This command is introduced.

show lldp

To display LLDP statistics and LLDP neighbors for all pNICs or a specific pNIC, use the show lldp command.

show lldp [stats | neighbors] [pnic *name*]

Syntax Description

Parameter	Description
stats	Displays LLDP statistics.
neighbors	Displays LLDP neighbors.
pnic *name*	Specifies the pNIC name.

Command Modes

EXEC mode

Examples

```
csp# show lldp
NAME        DEVICE ID     HOLDTIME  CAPS  PLATFORM                                                  PORTID
-------------------------------------------------------------------------------------------------------
Eth4-0    sw-lab-n5k-1  120       B     Cisco Nexus Operating System (NX-OS) Software  Ethernet105/1/45
Eth4-1    sw-lab-n5k-1  120       B     Cisco Nexus Operating System (NX-OS) Software  Ethernet105/1/46
Eth4-2    -             -         -     -                                                         -
Eth4-3    -             -         -     -                                                         -
Eth7-0    -             -         -     -                                                         -
Eth7-1    -             -         -     -                                                         -
           TX      DISCARD  ERROR  RX      DISCARDED  UNREC
NAME       FRAMES  RX       RX     FRAMES  TLVS       TLVS   AGEOUTS
-----------------------------------------------------------------
Eth4-0   13197    0        0      0        0          0      0
Eth4-1   13197    0        0      13206    0          0      0
Eth4-2    -       -        -      -       -          -      -
Eth4-3    -       -        -      -       -          -      -
Eth7-0   10365    0        0      0       0          0      0
Eth7-1   10368    0        0      753     0          0      0

csp# show lldp stats
           TX      DISCARD  ERROR  RX      DISCARDED  UNREC
```

```
NAME        FRAMES  RX       RX     FRAMES  TLVS       TLVS   AGEOUTS
-------------------------------------------------------------------------
Eth4-0    13197   0        0      0       0          0      0
Eth4-1    13197   0        0      13206   0          0      0
Eth4-2    -       -        -      -       -          -      -
Eth4-3    -       -        -      -       -          -      -
Eth7-0    10365   0        0      0       0          0      0
Eth7-1    10368   0        0      753     0          0      0
```

```
csp# show lldp neighbors
NAME        DEVICE ID     HOLDTIME  CAPS  PLATFORM                                        PORTID
-------------------------------------------------------------------------------------------------------
Eth4-0    sw-lab-n5k-1  120       B     Cisco Nexus Operating System (NX-OS) Software  Ethernet105/1/45
Eth4-1    sw-lab-n5k-1  120       B     Cisco Nexus Operating System (NX-OS) Software  Ethernet105/1/46
Eth4-2    -             -         -     -                                              -
Eth4-3    -             -         -     -                                              -
Eth7-0    -             -         -     -                                              -
Eth7-1    -             -         -     -                                              -
```

Command History

Release	Modification
2.5.0	The PNIC name has been changed to the new format, Eth<slot>-port.
1.0	This command is introduced.

show port-channel bond

To display information about a port channel, use the show port-channel bond command.

show port-channel bond *name*

Syntax Description

Parameter	Description
name	Specifies the name of the port channel.

Command Modes

EXEC mode

Example

```
csp# show port-channel bond mgmt_pch
---- mgmt_pch ----
bond_mode: balance-slb
bond may use recirculation: no, Recirc-ID : -1
bond-hash-basis: 0
updelay: 0 ms
downdelay: 0 ms
next rebalance: 6044 ms
lacp_status: off
active slave mac: 90:e2:ba:c2:6b:40(Eth0-1)

slave Eth0-1: enabled
        active slave
        may_enable: true

slave Eth0-1: enabled
        may_enable: true
```

```
        hash 11: 6 kB load
```

Command History

Release	Modification
2.5.0	The PNIC name has been changed to the new format, Eth<slot>-port.
2.2.0	This command is introduced.

show sr-iov

To display SR-IOV configuration for pNICs, use the show sr-iov command.

show sr-iov

Command Modes

EXEC mode

Example

```
csp show sr-iov
pnic-name   # Allowed VFs  # Enabled VFs  # In service use VFs  Bridge mode
----------  -------------  -------------  --------------------  -----------
     Eth0-1             7              0                     0          veb
     Eth0-2             7              0                     0          veb
     Eth1-1             7              0                     0          veb
     Eth1-2             7              0                     0          veb
     Eth1-3             7              0                     0          veb
     Eth1-4             7              0                     0          veb
     Eth2-1            63              0                     0          veb
     Eth2-2            63              0                     0         vepa
```

Command History

Release	Modification
2.5.0	The PNIC name has been changed to the new format, Eth<slot>-port.
2.1.0	This command is introduced.

support show ovs

To display detailed information about ovs, use the support show ovs command in privileged EXEC mode.

support show ovs

Command Modes

EXEC mode

Example

```
csp support show ovs
    1e5fb2e9-23c1-4d8d-aa68-39591cf6cd64
    Bridge "br-Eth0-1"
        Port "Eth0-1"
```

```
            tag: 1
            Interface "Eth0-1"
        Port "br-Eth0-1"
            Interface "br-Eth0-1"
                type: internal
        Port "Eth0-1_ll1"
            Interface "Eth0-1_ll1"
        Port "mgmt0"
            tag: 1
            Interface "mgmt0"
                type: internal
    Bridge "br-pc1g"
        Port "pc1g"
            tag: 1
            Interface "Eth0-2"
            Interface "Eth1-1"
        Port "Eth0-2_ll1"
            Interface "Eth0-2_ll1"
        Port "Eth1-1_ll1"
            Interface "Eth1-1_ll1"
        Port "br-pc1g"
            Interface "br-pc1g"
                type: internal
```

Command History

Release	Modification
2.5.0	This command is introduced.

pnic-breakout

To list or convert card mode or both into XL710, use the pnic-breakout command.

pnic-breakout

Command Modes

EXEC mode

Example

In the EXEC mode, the command lists breakout mode and interfaces within it.

```
csp# pnic-breakout list-intf
results Devno PCI CMODE PNICS
results ------------------------------
results 1 5e 4x10 ['Eth1-1-1', 'eth11-1-2', 'Eth1-1-3', 'Eth1-1-4']
```

Command Modes

Change card mode

In the change card mode, the command converts the mode of XL710 card.

pnic-breakout update nic_mode_pair [devno *devno*] [mode *mode*]

Syntax Description

Parameter	Description
devno *devno*	Specifies the device number that is listed when using the list-intf command.
mode *mode*	Specifies one of the supported modes for XL710 card such as, 2x40, 4x10.

Example

```
csp# pnic-breakout update nic_mode_pair [ devno 1 mode 2x40 }
```

Command History

Release	Modification
2.5.0	This command is introduced.

Radius Commands

radius-server host

To configure a RADIUS server to be used for authentication, use the radius-server host command. To remove the RADIUS server, use the no form of this command.

radius-server host *hostname* key *key_value* shared-secret *secret* [auth-port *auth-port*] [acct-port *acct-port*]

To configure Cisco attribute-value (AV) pair privilege level (class) on RADIUS server, see the csp-users users command.

Syntax Description

Parameter	Description
hostname	Hostname or IPv4 address of the RADIUS server.
key *key_value*	Specifies a preshared key for the RADIUS server. Supported key value are as follows: • 0: Clear text preshared key • 7: Encrypted preshared key
shared-secret *shared-secret*	Specifies the preshared secret to authenticate communication between the RADIUS server and the Cisco CSP 2100. The preshared secret is alphanumeric, case sensitive, and has a maximum of 63 characters.
auth-port *auth-port*	Configures the RADIUS server to perform the authentication functions and associates a specific host with the port that receives the RADIUS authentication messages. The default port is 1812. The valid range is from 0 to 65535.
acct-port *acct-port*	Configures the RADIUS server to perform the accounting functions and associates a specific host with the port that receives the RADIUS accounting messages. The default port is 1813. The valid range is from 0 to 65535.

Command Modes

Global configuration (config)

Example

```
csp# config t
csp# radius-server host rad1 key 0 shared-secret myRaDIUSpassword auth-port 1645 acct-port 1646
```

Command History

Release	Modification
2.2.0	This command is introduced.

radius-server retransmit

To define the number of retransmits allowed before reverting to local authentication, use the radius-server retransmit command. By default, retransmission to a RADIUS server is tried only once before reverting to local authentication. To reset the number of retransmits to the default value, use the no form of this command.

radius-server retransmit *count*

Syntax Description

Parameter	Description
count	Number of retransmits allowed before reverting to local authentication. The default number of retransmits is 1 and the valid range is from 0 to 5.

Command Modes

Global configuration (config)

Example

```
csp# config t
csp# radius-server retransmit 3
```

Command History

Release	Modification
2.2.0	This command is introduced.

radius-server timeout

To define the duration to wait for a response from a RADIUS server before declaring a timeout failure, use the radius-server timeout command. To reset the timeout duration to the default value, use the no form of this command.

radius-server timeout *seconds*

Syntax Description

Parameter	Description
seconds	Timeout interval for the RADIUS server. The default timeout interval is 3 seconds and the valid range is from 1 to 10 seconds.

Command Modes

Global configuration (config)

Example

```
csp# config t
csp# radius-server timeout 6
```

Command History

Release	Modification
2.2.0	This command is introduced.

show running-config radius-server

To display the running configuration information for the RADIUS server, use the show running-config radius-server command.

show running-config radius-server

Command Modes

EXEC mode

Example

```
csp# show running-config radius-server
radius-server retransmit 1
radius-server timeout 3
radius-server host 172.23.180.126
 key           7
 shared-secret wawyanb123
 auth-port 1812
 acct-port 1813
!
```

Command History

Release	Modification
2.2.0	This command is introduced.

Repository Commands

copy core

To copy a core file from Cisco CSP 2100, use the copy core command.

copy core *source_file destination_file*

Syntax Description

Parameter	Description
source_file	The name of the file to be copied.
destination_file	Destination URL and the name with which the file is copied in the following format:

	`user@host:file.`

Command Modes

EXEC mode

Examples

```
csp# copy core core.6566 user1@myhost: core.6566
```

Command History

Release	Modification
2.1.0	This command is introduced.

copy log

To copy a log file from Cisco CSP 2100, use the `copy log` command.

`copy log` *source_file destination_file*

Syntax Description

Parameter	Description
source_file	The name of the file to be copied.
destination_file	Destination URL and the name with which the file is copied in the following format: `user@host:file.`

Command Modes

EXEC mode

Examples

```
csp# copy log messages user1@myhost:messages
```

Command History

Release	Modification
2.1.0	This command is introduced.

copy image

Release 1.0 and Release 2.0.0

To copy an image file to the local repository, use the `copy image` command.

`copy image source` *location*

Syntax Description

Parameter	Description
`source` *location*	Specifies the location and the name of the image file in the following format: `user@host:file`.

Release 2.1.0 and Later Releases

To copy an image file to and from the Cisco CSP 2100, use the copy image command.

copy image *source_file destination_file*

Syntax Description

Parameter	Description
source_file	Source URL and the name of the source file to be copied in the following format: `user@host:file`. The source can be either local or remote.
destination_file	Destination URL and the name with which the file is copied. The destination can be either local or remote. If you want to retain the same name as the source file name, specify a period (.) instead of the filename.

Command Modes

EXEC mode

Examples

```
Example for copying to the repository in Release 1.0 and 2.0.0
csp# copy image source user1@myhost:Tiny_ssh.iso

Example for copying to the repository in Release 2.1.0 and later releases
csp# copy image user1@myhost:/Tiny_ssh.iso .

Example for copying from the repository in Release 2.1.0 and later releases
csp# copy image Tiny_ssh.iso user1@myhost:/Tiny_ssh.iso
```

Command History

Release	Modification
2.1.0	The destination_file parameter is added to this command and the source parameter is removed.
2.0.0	This command is introduced.

Release 2.3.1 and Later Releases

To copy an image file to and from the Cisco CSP, use the copy image command.

copy image *source_file destination_file*

Syntax Description

Parameter	Description
source_file	Name of the source file to be copied in any of the following formats: The source can be either local, remote, or nfs. remote - `user@host:file` nfs – `nfs:nfsname/filename`

	local - `filename`
destination_file	Name with which the file is copied. The destination can be either local, remote, or nfs. The destination file can be copied in any of the following formats: remote - `user@host:file` nfs - `nfs:nfsname/filename` local - `filename`

Command Modes

EXEC mode

Examples

Example where source is NFS and destination is local

```
csp# copy image nfs:nfs/csr1000v-universalk9.03.16.00.S.155-3.S-ext.qcow2
```

Example where source is remote and destination is NFS

```
csp# copy image abcdex@171.0.209.30:/data/debug/dplugdisk nfs:nfs/dplugdisk
```

Example where source is remote and destination is local

```
csp# copy image abcdzzz@171.68.209.35:/auto/asr9k_thor1/Halcyon/release/v2_3_1/dplugdisk
```

Command History

Release	Modification
2.3.1	This command is introduced.

delete image

To delete an image file from the local repository, use the delete image command.

delete image [service_images/] *filename*

Syntax Description

Parameter	Description
service_images	Specifies that the image file resides in the service_images directory.
filename	Name of the image file.

Command Modes

EXEC mode

Example

```
csp# delete image n1000v-dk9.5.2.1.SV3.1.4.iso
```

Command History

Release	Modification
2.0.0	This command is introduced.

show images

To display information about all files or all image files available in the repository, use the show images command.

show images [all]

Syntax Description

Parameter	Description
all	Displays all files available in the repository. If you do not use this parameter, only image files available in the repository are displayed.

Command Modes

EXEC mode

Example

```
csp# show images
Local storage:
      File Name                                       Last Modified              Size
n1000v-dk9.5.2.1.SV3.1.4.iso                    Mon Feb 15 23:17:48 2016       231815168
csr1000v-universalk9.03.16.00.S.155-3.S-ext.iso Mon Feb 15 23:32:49 2016       355221504
Cisco-vWAAS-150-6.1.1-npe-b-10.ova              Tue Feb 16 07:25:50 2016       857241600
nam-app-x86_64.6-2-1.iso                        Mon Feb 15 02:06:40 2016       386881536

Remote storage: nfs0
            File Name                  Last Modified             Size
asav951.qcow2                    Tue Feb  2 22:23:07 2016       159973376
daynfs.iso                       Tue Feb  2 22:30:05 2016          360448
TinyCore-current.iso             Thu Feb  4 14:39:25 2016        15728640
```

Command History

Release	Modification
2.0.0	This command is introduced.

rename image

To rename an image file available in the local repository, use the rename image command.

rename image filename *filename*

Syntax Description

Parameter	Description
filename	Specifies the image file to be renamed.
filename	Name of the new image file.

Command Modes

EXEC mode

Example

```
csp# rename image n1000v-dk9.5.2.1.SV3.1.4.iso n100v9.5.2.1.iso
```

Command History

Release	Modification
2.6.1	This command is introduced.

show repository

To display information about all files available in the repository, use the show repository command.

show repository

Command Modes

EXEC mode

Example

```
csp# show repository
Local storage:
File Name                                       Last Modified                Size
n1000v-dk9.5.2.1.SV3.1.4.iso                    Mon Feb 15 23:17:48 2016      231815168
vwaas150Rem.tmpl                                Tue Feb 16 05:08:52 2016      862
csr1000v-universalk9.03.16.00.S.155-3.S-ext.iso Mon Feb 15 23:32:49 2016      355221504
vwaas150.tmpl                                   Tue Feb 16 00:30:49 2016      864
vWAASRem4-clone.tar.gz                          Tue Feb 16 05:53:25 2016      827251427
Cisco-vWAAS-150-6.1.1-npe-b-10.ova              Tue Feb 16 07:25:50 2016      857241600
dplugdisk                                       Mon Feb 15 06:57:10 2016      101442560
nam-app-x86_64.6-2-1.iso                        Mon Feb 15 02:06:40 2016      386881536

Remote storage: nfs0
    File Name                        Last Modified                Size
asav951.qcow2                    Tue Feb  2 22:23:07 2016       159973376
daynfs.iso                       Tue Feb  2 22:30:05 2016          360448
TinyCore-current.iso             Thu Feb  4 14:39:25 2016        15728640
rhel70-exported.tar.gz           Fri Feb 12 08:56:38 2016       547068607
asav12.tmpl                      Tue Feb  2 22:23:06 2016             684
day0.cfg                         Tue Feb  2 22:24:25 2016              99
```

Command History

Release	Modification
2.0.0	This command is introduced.

create file-name

To create a new text file that resides in the local repository, use the create file name command. The new files does not overwrite existing files or can be edited after creation. These new files are not copied to other nodes in cluster mode.

create file-name *file-name* content *content*

Syntax Description

Parameter	Description
file-name	Name of the text file. If the specified name of the text file exists, creating a file process is aborted. Valid values are alphanumeric, underscore, dash, period. The range is from 1 to 80

Parameter	Description
	characters.
content	Text to be included in file. Valid values are a string up to 4096 characters and spaces are allowed in the content. Note: Ensure that you use double quotes to enclose the content string.

Command Modes

EXEC mode

Examples

```
csp# create file-name hello_world.txt content "some real content\n and a new line"
```
The output of this command is:

```
Created file: hello_world.txt
```

Command History

Release	Modification
2.3.0	This command is introduced.

Resource Commands

resource

To modify a resource, use the resource command.

resource csp-2100 [default_gw *default_gw*] [dns_server *dns_server*] [dns *dnsip*] [domain_name *domain_name*] [host_name *host_name*] [ip_address *ip_address*] [ip-receive-acl *source_ip_address* [service *service*] priority *priority* action *action*] [log_severity {debug | info | notice | warning | error | critical | alert | emerg}] [mgmt_mtu *mgmt_mtu*] [mgmt_pnic *pnic_name*] [mgmt_pnic_mode *mgmt_pnic_mode*] [mgmt_vlan *vlan_num*] [netmask *netmask*] [host-vnic *host-vnic*] [syslog_server *ip/hostname*] [rsyslog_tcp_port *rsyslog_tcp_port*] [rsyslog_udp_port *rsyslog_udp_port*] [rsyslog_udp_only {true | false}] [service-mgmt-pnic *pnic_name*] [storage *name* storagetype nfs storage_space_total_gb *storage_space* server_ip *server_ip* server_path *server_path*]

Caution: When you change the value of the default_gw, ip_address, netmask, or mgmt_pnic parameter, the entire system network is reset which affects the traffic across all services. This may result in traffic loss until all physical interfaces come out of reset. In addition, when you change the values of the network management parameters, it may impact the connection to Cisco CSP 2100. Refer to the usage guidelines section for more information.

Syntax Description

Parameter	Description
csp-2100	Name of the resource. For each Cisco CSP 2100, there is only one resource and the resource name is set to csp-2100.
default_gw *default_gw*	Specifies the default gateway.
dns_server *dns_server* (deprecated)	Specifies the DNS server (deprecated).

Parameter	Description
dns *dnsip*	Specifies multiple DNS servers. Note: Ensure that a reachable DNS server is configured in CSP. It prevents configuration errors during service creation through GUI and REST API.
domain_name *domain_name*	Specifies the domain name.
host_name *host_name*	Specifies the host name.
ip_address *ip_address*	Specifies the IP address.
ip-receive-acl source_*ip_address*	Specifies the IPv4 IP address of the source network for Access Control List (ACL) access to the management interface. When the management ACL access is enabled, only specified source networks can access the management interface. When no ACL rule is defined, Cisco CSP 2100 allows all types of traffic. If the source network is specified as 0.0.0.0/0, the configuration is applicable to all source networks.
service *service*	Specifies the service type for the management ACL access. Valid values are: • ssh: Includes port 22 and port 2024. • https: Includes port 80, port 443 and all ports to access the service console. • snmp: Includes port 161 and configured NET-SNMP port. • netconf: Includes port 2022. This port is required for communication between nodes of a cluster. • icmp: Provides ability to ping the host. You can specify one, more than one, or all service types in this parameter. To specify multiple service types, enter the values within the square brackets []; for example, service [snmp https]. If you do not specify any specific service, the configuration is applicable to all services.
priority *priority*	Specifies the priority for the ACL rule. Each ACL rule must have a unique priority value. Valid range is from 0 to 65,535. ACL rule with priority 0 has the highest priority. Whenever an ACL rule with priority 0 is matched, Cisco CSP 2100 performs the action associated with this ACL rule and does not look up any lower priority ACL rules.
action *action*	Specifies the action for the packets received from a source network. Valid values are: • accept: Accept the packets. • reject: Reject the packets and return the error to the source

Parameter	Description
	network. • drop: Drop packets immediately and do not send any information to the source network.
log_severity	Specifies the severity level for log messages. Valid values are debug, info, notice, warning, error, critical, alert, and emerg. Default is info.
mgmt_mtu *mgmt_mtu*	Specifies the maximum transmission unit (MTU) size for the management interface. By default, the MTU size for the management interface (mgmt0) is 1500 bytes. To support jumbo frames, you can configure the MTU size of up to 9000 bytes. Note: To maintain connectivity, when you change MTU setting on CSP 2100, ensure that similar MTU configuration is also applied to the upstream switch.
mgmt_pnic *pnic_name*	Specifies the management pNIC for Cisco CSP 2100. You can specify a pNIC or a port channel as the management pNIC.
mgmt_pnic_mode *mgmt_pnic_mode*	Specifies the mode for the management pNIC. Valid values are shared and dedicated. Default is shared. In shared mode, the management interface pNIC can be shared with any service VMs. The management interface pNIC carries the management traffic of Cisco CSP 2100 and the management and data traffic of any service using this pNIC. In dedicated mode, the management interface pNIC carries only the management traffic of Cisco CSP 2100. In shared mode, you can change the management interface pNIC to any available pNIC. In dedicated mode, you can change the management interface pNIC only to a pNIC that is not associated with any service. Note: If you try to change the mode of the management interface pNIC to dedicated while a service is currently using it, you get the "`Management PNIC already in service use`" error. Similarly, if the management interface pNIC is in dedicated mode and you try to create a service using the management pNIC, you get the "`PNIC is dedicated to management`" error.
mgmt_vlan *vlan_num*	Specifies the management VLAN corresponding to the management (mgmt0) interface. Valid range is from 1 to 4094.
netmask *netmask*	Specifies the netmask.
host-vnic *host-vnic*	Specifies an additional host vnic to create an alternate network for the host to communicate. You can use this to create a dedicated network for NFS traffic. A host-vnic configuration requires an external PNIC, which is separate from the CSP management. The IP and route configuration of the host-vnic communicates through that

Parameter	Description
	PNIC.
syslog_server *ip/hostname*	Specifies the IPv4 IP address or host name of the remote syslog servers. This IP address or host name must be reachable from Cisco CSP 2100. You can configure the Cisco CSP 2100 syslog as a client to send internal log messages to multiple remote syslog servers on TCP and UDP ports or only UDP port. The remote syslog servers should be capable of receiving RFC-5424 formatted logging messages. If the rsyslog_udp_only parameter is not set to true, you must specify both transport ports. Note: You can send log messages to a maximum of eight syslog servers.
rsyslog_tcp_port *rsyslog_tcp_port*	Specifies the TCP port for the remote rsyslog server. Note: You must configure the remote syslog server and specify the same TCP port for transport. For example, if you have specified port 9020 as rsyslog_tcp_port, then on the remote syslog server, configure the TCP port for 9020. You cannot set this parameter if the rsyslog_udp_only parameter is set to true.
rsyslog_udp_port *rsyslog_udp_port*	Specifies the UDP port for the remote rsyslog server. Note: You must configure the remote syslog server and specify the same UDP port for transport. For example, if you have specified port 514 as rsyslog_udp_port, then on the remote syslog server, configure the UDP port for 514.
rsyslog_udp_only	Specifies that the remote syslog server uses only UDP transport. Valid values are true and false. Note: When you set this parameter to true, you cannot set the rsyslog_tcp_port parameter.
service-mgmt-pnic *pnic_name*	Specifies the single pNIC or port channel to be used as the dedicated service management interface. Following are the guidelines for the dedicated service management interface: • Only one dedicated service management interface can be active at a time. • The specified pNIC cannot be a member of a port channel. • The specified pNIC cannot be same as the Cisco CSP 2100 management pNIC (mgmt_pnic). • The dedicated service management interface can be changed only when it is not in use. In addition, the port or the port channel that you are planning to assign as the dedicated service

Parameter	Description
	management interface should not be in use. • The dedicated service management interface can be used by multiple services and on multiple vNICs in the same service. • The dedicated service management interface is deleted only when it is not in use.
storage *name*	Specifies the storage space name.
storagetype	Specifies the storage type. Valid value is nfs.
storage_space_total_gb *storage_space*	Specifies the total storage space (in GB).
server_ip *server_ip*	Specifies the IP address of the server.
server_path *server_path*	Specifies the path on the server. Note: The NFS mount should be writable by all users.

Command Modes

EXEC mode

Usage Guidelines

When you change the values of network management parameters, you might lose the connection to Cisco CSP 2100. In case the connection is lost, use a physical serial console connection or the Cisco Integrated Management Controller (CIMC) KVM Console to correct the error.

Examples

Syslog Servers With Both UDP and TCP Ports

```
csp# resource csp-2100
csp(config-resource-csp-2100)# syslog_server 10.1.1.20
csp(config-resource-csp-2100)# rsyslog_udp_port 514
csp(config-resource-csp-2100)# rsyslog_tcp_port 9020
csp(config-resource-csp-2100)# commit
```

Syslog Servers With UDP Port

```
csp# resource csp-2100
csp(config-resource-csp-2100)# syslog_server syslog.cisco.com
csp(config-resource-csp-2100)# rsyslog_udp_port 514
csp(config-resource-csp-2100)# rsyslog_udp_only
csp(config-resource-csp-2100)# commit
```

IP Receive ACL Example

```
csp# resource csp-2100
csp(config-resource-csp-2100)# ip-receive-acl 192.168.0.0/16 service [ snmp https ] action drop priority
0
csp(config-ip-receive-acl-192.168.0.0/16)# commit
```

Host VNIC for dedicated NFS network

```
csp# config
Entering configuration mode terminal
csp(config)# resource csp-2100
csp(config-resource-csp-2100)# host-vnic nfs-network
csp(config-host-vnic-nfs-network)# description "host network for dedicated nfs"
```

Commands

```
csp(config-host-vnic-nfs-network)# vnic-ip 30.30.30.30
csp(config-host-vnic-nfs-network)# vnic-netmask 255.255.255.0
csp(config-host-vnic-nfs-network)# vnic-vlan 30
csp(config-host-vnic-nfs-network)# external-pnic Eth2-2
csp(config-host-vnic-nfs-network)# route 40.40.40.0/24 next-hop 30.30.30.1
csp(config-route-40.40.40.0/24)# commit
Commit complete.
```

Command History

Release	Modification
2.5.0	• New command, dns has been introduced. • The host-vnic parameter has been introduced.
2.2.5	The syslog_server parameter is introduced and rsyslog_ip parameter is removed.
2.2.0	The ip-receive-acl, mgmt_vlan, and service-mgmt-pnic parameters are added.
2.1.0	The mgmt_mtu and mgmt_pnic_mode parameters are added.
2.0.0	The storage and rsyslog_udp_only parameters are added.
1.0	This command is introduced.

resource csp-2100 description

To add a description for the CSP resource, use the resource csp-2100 description global configuration command. To remove the configured description, use the no form of this command.

resource csp-2100 {description *new description*}

no resource csp-2100 description

Syntax Description

Parameter	Description
description *new description*	Specifies a description for a CSP resource. Valid values are a string up to 256 characters, underscores, dashes, periods, spaces, and commas. Note: While using spaces, ensure that you use double quotes to enclose the description string.

Command Modes

Global configuration (config)

Example

```
csp(config)# resource csp-2100 description "dev box"
csp(config-resource-csp-2100)# commit
Commit complete.

csp(config)# no resource csp-2100 description
csp(config)# commit
Commit complete.
```

Command History

Release	Modification
2.3.0	This command is introduced.

show resource csp-2100 description

To display the description about the CSP 2100 resource, use the show resource csp-2100 description command.

show resource csp-2100 description

Syntax Description

None

Command Modes

EXEC mode

Command History

Release	Modification
2.3.0	This command is introduced.

show version

To display information about the current CSP 2100 version, use the show version command.

show version

Command Modes

EXEC mode

Example

```
csp# show version
Cisco Cloud Services Platform Software, 2100 Software (CSP-2100), Version 2.0.0 Build:6
TAC Support: http://www.cisco.com/tac
Copyright (c) 2015 by Cisco Systems, Inc
Compiled Wednesday 10-February-2016 14:48

Linux osp51 3.10.0-327.el7.x86_64 #1 SMP Thu Oct 29 17:29:29 EDT 2015 x86_64 x86_64 x86_64 GNU/Linux
Red Hat Enterprise Linux Server release 7.2 (Maipo)
CSP-2100 uptime is 11 hours, 29 minutes, 20 seconds

Cisco UCSC-C220-M3S, Version C220M3.1.5.3b.0.082020130601, processor Intel(R) Xeon(R) CPU E5-2609 0 @
2.40GHz
8 CPUs with 58657016 kB / 65800168 kB of memory
L1d cache 32K, L1i cache 32K, L2 cache 256K, L3 cache 10240K

8 - Total Physical Interfaces (PNICs)
   6 -  1 Gbps Physical Interfaces (PNICs) Up
   2 - 10 Gbps Physical Interfaces (PNICs) Down/Unconnected
csp#
```

Command History

Release	Modification
1.0	This command is introduced.

show resource csp-2100 hardware

To display information about the csp-2100 hardware, use the show resource csp-2100 hardware command in EXEC mode.

show resource csp-2100 hardware

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC mode

Example

```
csp# show resource csp-2100 hardware
hardware entity 1
entity_name           UCSC-C220-M4S
entity_descr          "Cisco Cloud Services Platform"
entity_class          chassis
entity_parent         0
entity_parent_rel_pos -1
vendor_type           1.3.6.1.4.1.9.12.3.1.3.1831
hw_version            74-12419-01
fw_version            ""
sw_version            02.02.06.420
serial_number         FCH20057RFX
mfg_name              "Cisco Systems Inc"
asset_id              ""
is_fru                0
osp_part_size         1884126032
osp_part_used         18386312
last_change_time      1526368467
csp#
```

Command History

Release	Modification
2.1.1	This command is introduced.

show running-config resource

To display the running configuration information for a resource, use the show running-config resource command. For each Cisco CSP 2100, there is only one resource and the resource name is set to csp-2100.

show running-config resource [csp_version | disk_space_total_gb | disk_space_used_gb | default_gw | dns_server | dns | domain_name | host_name | ip_address | log_severity | ip-receive-acl | mgmt_mtu | mgmt_pnic | mgmt_vlan | netmask | host-vnic | num_cpus_total | num_cpus_used | num_service | ram_total_mb | ram_used_mb | syslog_server | rsyslog_tcp_port | rsyslog_udp_port | rsyslog_udp_only | service-mgmt-pnic]

Syntax Description

Parameter	Description
csp_version	Displays the version of Cisco CSP 2100.
disk_space_total_gb	Displays the total amount of available disk space.
disk_space_used_gb	Displays the total amount of disk space in use.
default_gw	Displays the default gateway.
dns_server (deperecated)	Displays the DNS server (deprecated).
dns	Displays multiple DNS servers.
domain_name	Displays the domain name.
host_name	Displays the host name.
ip_address	Displays the IP address.
log_severity	Displays the severity level for log messages.
ip-receive-acl	Displays information about the management ACL configuration.
mgmt_mtu	Displays the MTU size.
mgmt_pnic	Displays the management pNIC.
mgmt_pnic_mode	Displays the mode for the management pNIC.
mgmt_vlan	Displays the management VLAN corresponding to the management (mgmt0) interface. If the management VLAN is set to the default value of 1, it is not shown in the command output.
netmask	Displays the netmask.
host-vnic	Displays the host-vnic configuration.
num_cpus_total	Displays the total number of virtual CPUs.
num_cpus_used	Displays the total number of used virtual CPUs.
num_service	Displays the number of services.
ram_total_mb	Displays the total amount of available RAM.
ram_used_mb	Displays the total amount of used RAM.
syslog_server	Displays IP addresses or host names of multiple remote rsyslog servers.
rsyslog_tcp_port	Displays the TCP port for the remote rsyslog server.
rsyslog_udp_port	Displays the UDP port for the remote rsyslog server.
rsyslog_udp_only	Indicates that the remote syslog server uses only UDP transport.

Parameter	Description
service-mgmt-pnic	Displays the dedicated management port for services.

Command Mode

EXEC mode

Usage Guidelines

The output of this command includes only those parameters that are configured. For example, if you have not configured the parameters related to the remote rsyslog server, these parameters are not displayed in the output.

Example

```
csp# show running-config resource
resource csp-2100
 ip_address          192.0.2.130
 netmask             255.255.255.0
 default_gw          192.0.2.1
 mgmt_mtu            1500
 mgmt_vlan           180
 mgmt_pnic           Eth4-0
 host_name           osp-ucs54
 dns_server          192.0.2.122
 domain_name         cisco.com
 csp_version         001.000.000
 num_cpus_used       1
 num_cpus_total      6
 ram_used_mb         2048
 ram_total_mb        60176
 disk_space_used_gb  4
 disk_space_total_gb 397
 num_service         1
 log_severity        info
 service-mgmt-pnic   Eth130-1
 ip-receive-acl 192.168.0.0/16
  service [ https snmp ]
  action  drop
  priority 0
  !
  dns 171.70.168.183
  !
  dns 8.8.8.8
  !
  !
```

Command History

Release	Modification
2.5.0	The host-vnic parameter has been introduced.
2.2.5	The syslog_server parameter is introduced and rsyslog_ip parameter is removed.
2.2.0	The ip-receive-acl, mgmt_vlan, and service-mgmt-pnic parameters are added.
2.1.0	The mgmt_mtu and mgmt_pnic_mode parameters are added.
2.0.0	The rsyslog_udp_only parameters are added.

Release	Modification
1.0	This command is introduced.

Service Commands

login service

To locally access the service console, use the login service command.

Note: The command cannot be used by operator group users.

login service *name*

Syntax Description

Parameter	Description
name	Name of the service

Command Modes

EXEC mode

Example

```
csp# login service vsm-sf
```

Command History

Release	Modification
2.3.1	The permissions are modified across user groups.
2.0.0	This command is introduced.

service

To create a service, import a service, or export a service, use the service command. To delete a service or return to its default settings, use the no form of this command.

service *name* [day0_filename *day0_filename*] [emulator-pin *emulator-pin*] [day0-dest-filename *day0-dest-filename*] [day0-volume-id *day0-volume-label*] [disk_loc *disk_loc*] [disk_size *disk_size*] [disk-resize {enable | disable}] [disk_storage_name *disk_location*] [disk_type *disk_type*] [firmware {legacy | uefi}] [secure-boot {true | false}] [image_storage_name *image_location*] [ip *vnf_mgmt_ip*] iso_name *iso_name id* [cache-mode {none | writethrough}] key *key_value* vnc_password *vnc_password* [export [cancel] [exported_service_name *exported_name* [exported_location {local | nfs } exported_nfs_location *nfs_mount_name* export_live {true | false}]]] mac_id *mac_id* [monitor {pause | resume}] [memory *memory*] [novnc-port *port_num*] [numcpu *numcpu*] [power {off | on | reboot | reset}] {description *new description*} [monitoring status {enabled | disbaled} boot-time *boot-time* poll-interval *poll-interval* failure-retry-cnt *failure-retry-cnt* [recovery-policy ip-monitoring {reboot|shutdown|none} link-state-monitoring {shutdown|none}] max-recovery-retries *max-recovery-retries*] [properties *properties*] [serial_port *serial_port* serial_type {telnet | console} service_port *service_port*] [storage_disk *id* storage_disk_location *disk_location* storage-disk-image-file *image_file_name* storage_disk_format {raw | qcow2} storage_disk_device {disk | cdrom} stor-

age_disk_space_total_gb *disk_space* storage_disk_type *disk_type*] [uuid *uuid*] [vm_type generic] [vnc_password *password*] [vnic]

To import a service using an exported image available in the Cisco CSP 2100 repository, specify the name of the exported service in the iso_name parameter. For all other parameters, specify the values that the exported service used.

Starting with release 2.3.0, the description parameter can be configured for a specific service. To remove the service description, use the no form of this command.

Starting with release 2.3.0, you can configure the monitoring service to monitor the VNF.

Starting with release 2.3.0, the VNC password can be encrypted with the key field.

Starting with release 2.2.5, ISO volume label can be configured only for the first day0 ISO file.

Starting from release 2.6.0, a service export can be canceled.

Starting from release 2.8.0, you can configure the firmware type and secure boot for the VNF when creating a service.

Starting from release 2.9.0, you can edit the disk_storage_name and storage_disk_location parameters on power off. The value of both these fields should be the same in case of an imported VNF. On committing a change, the VNF is moved to the "disk_migration_in_progress" state until the migration is complete. The "support show disk-migration-status service-name vmname" parameter displays the progress of the disk migration.

Note: Before deleting a service, you must first set its power mode to off. You can export a service when the VM is powered on. If the export_live parameter is set to false, CSP pauses the VM in the background when export is in progress and resumes the VM when the export is complete. If export_live is set to true, the service of VM is exported live.

Syntax Description

Parameter	Description
name	Name of the service.
day0_filename *day0_filename*	Specifies the name of the day0 configuration text or ISO file. The day0 configuration file contains the configuration information that is applied when a service is created. The day0 configuration file must reside in the same directory in which the boot image is located. Starting with Release 2.3.0, you can specify an empty day0 filename. Starting with Release 2.3.0, you can specify up to eight day0 configuration files. When specifying multiple files, separate the file names only with a comma as shown in the following example: `"hello.txt,hello1.txt,config.txt"` Note: Do not use spaces between the file names or between the comma and file names.
emulator-pin *emulator-pin*	Specifies configuring individual CPU or range of CPUs for emulator thread pinning. You can configure for emulator thread pinning when powering on a VM. This means, you can perform live edit of this configuration. If not configured, the emulator threads are pinned through default round robin.

Parameter	Description

day0-dest-filename *day0-dest-filename*	Specifies the name of the day0 destination text or ISO file. The day0 destination file is required for the services that require a predefined configuration file name.
	
	Following are the guidelines for the day0 destination filename:
	
	• Starting with Release 2.3.0, you can specify up to eight day0 destination files. When specifying multiple files, separate the file names only with a comma as shown in the following example:
	
	`day0-dest-filename "/config/banner/,/config/banner/,/config/banner/"`
	
	• Starting with Release 2.3.0, you can specify folder structure format for the day0-dest-filename parameter. For example:
	
	`day0-dest-filename "/config/banner/,/config/banner/,/config/banner/"`
	
	Note: The folder structure must begin and end with a forward slash. If the folder structure does not end with a forward slash, the last string in the folder structure is considered as the destination filename. Also, the folder structure cannot include consecutive dots, such as ellipsis. You do not need to specify a value for the day0_filename and can only specify the folder structure for day0-dest-filename.
	
	• To use the same filename as the day0_filename, do not specify a value for the day0-dest-filename parameter. For example:
	
	`day0_filename myday0file`
	
	`day0_filename file1,file2 day0-dest-filename dest-file1,`
	
	When the value of day0-dest-filename parameter is blank or no value is specified, the filename specified in the day0_filename parameter is used for the day0-dest-filename parameter.
	
	• To maintain one to one mapping between the day0_filename and the day0-dest-filename parameter values, specify the same number of commas in the day0-dest-filename parameter values as you have specified in the day0_filename parameter values. For example, for the following values for the day0_filename parameter containing one comma: `day0_filename file1,file2,` the day0-dest-filename parameter values must also contain one comma as shown in the following examples:
	
	o `day0_filename file1,file2 day0-dest-filename ,`
	
	o `day0_filename file1,file2 day0-dest-filename dest-file1,dest-file2`
	
	o `day0_filename file1,file2 day0-dest-filename dest-file1,`
	
	o `day0_filename file1,file2 day0-dest-filename ,dest-file2`

Parameter	Description
day0-volume-id *day0-volume-label*	Specifies the volume label to be used for ISO file. Valid values are a string up to 32 characters and spaces are allowed in the volume label. Note: You can configure a volume label only for the first day0 ISO file if the first day0 filename configuration is available. All remaining ISO files are system assigned default volume labels.
disk_loc *disk_loc*	Specifies the image file to be used for service storage. This parameter is applicable only for Release 1.0.
disk_size *disk_size*	Specifies the total amount of disk space available (in GB) for this service. This parameter is not configurable when a QCOW2 image is selected in the iso_name parameter and the disk-resize parameter is set to false.
disk-resize	Enables or disables the resizing of bootable QCOW2 image. Valid values are true and false. Default value is false.
disk_storage_name *disk_location*	Specifies the location of the service image file. The default value is local. You can set the location to be an NFS storage mount point or gluster. Note: Gluster is supported when pyou create a cluster with the storage network enabled.
disk_type *disk_type*	Specifies the disk type. Valid choices are ide and virtio.
firmware	Specifies the firmware type of VNF. Valid values are legacy and uefi type. Default value is legacy.
image_storage_name *image_location*	Specifies the location of the boot image specified in the iso_name parameter. The location can be an NFS storage mount point. Default value is local. To specify the NFS location, the NFS storage must have been added using the resource command.
ip *vnf_mgmt_ip*	Specifies the VNF management IP address to be used in the service The VNF Management IP value entered in this parameter does not get configured in the service. This parameter serves only as a reference to the VNF management IP address mapped to a service.
iso_name *iso_name*	Specifies the ISO, OVA, or QCOW software image file, and zip file to be used to create the service. Note: With Cisco VSM and Cisco VSG services, only ISO image files are supported.
cache-mode *cache-mode*	Specifies the cache mode of a service. Valid values are none or writethrough. none: The I/O from the guest is not cached on the host, but may be kept in a writeback disk cache. Use this option for guests with large I/O requirements. This option is generally the best choice, and is the only option to support migration.

Parameter	Description
	writethrough: The I/O from the guest is cached on the host but written through the physical medium. This mode is slower and prone to scaling problems. You can use this option for small number of guests with lower I/O requirements. Suggested for guests that do not support a writeback cache.
vnc_password *vnc_password*	Specifies the VNC password that is being encrypted for the service. Ensure that the VNC password meets the following criteria: • a string between 8 to 64 characters. • at least one digit • at least one special character such as, _, -, ~, #, @, =, +, ^,] • at least one upper case character • at least one lower case character • no two or more same characters can be provided consecutively • should not match exactly with any dictonary word.
key *key_value*	Allows you to configure vnc password with the key field. Default value is zero. Note: VNC password is encrypted and saved with the key value set as seven after encryption. Note: The save and load feature where the VNC password with key 0 and weak strength has been configured before 2.2.5 does not work. However, the save and load feature with key 7 always work.
exported_service_name	Specifies a name for the exported service. If you do not specify a name, the following name is used by default: *service_name*-clone.
exported_location	Valid values are local or nfs. When you export a service, and exported_location is not set or set to "local", a file named *exported_service_name*.tar.gz or *service_name*-clone.tar.gz file is created in the Cisco CSP 2100 repository. It takes few minutes to create this file.
exported_nfs_location	When the exported_location parameter is set to "nfs", the exported_nfs_location parameter is a mandatory configuration and it should be a valid configured nfs mount. The exported file is then created in the repository of nfs mount.
export_live	Valid values are true or false. When export_live is not set or set to false, the VM is paused in the background by CSP when the export is in progress, which causes traffic loss. The VM resumes when export is complete. If export_live is

Parameter	Description
	set to true, the VM is exported live and there is no traffic loss.
mac_id	Specifies the MAC ID. The MAC ID is automatically generated. You cannot set this parameter.
monitor *action*	If monitoring is enabled for a VM and the VM is powered on, you can pause or resume the monitoring of the VM. Valid values are pause or resume.
memory *memory*	Specifies the memory allocated for the service. The default value is 2048.
novnc-port *port_num*	Specifies the port number for the service console. Each service must use a unique port number. Valid range is from 8721 to 8784. Note: Before changing the port of a service, you must set the power mode of the service to off.
numcpu *numcpu*	Specifies the number of virtual CPUs for this service.
power	Specifies the state of the power upon activation. Valid choices are off, on, reboot, and reset. The default value is off.
description *new description*	Specifies a description about the service. Valid values are a string up to 256 characters, underscores, dashes, periods, spaces, and commas. Note: While using spaces, ensure that you use double quotes to enclose the description string.
monitoring *status*	Enables or disables configuring monitoring. Valid values are Enabled and Disabled.
boot-time *boot time*	Specifies the time in seconds to be waited after deployment, until monitoring starts. Configure according to the VM boot time.
poll-interval *poll-interval*	Specifies the time interval in seconds at which the polling should be performed.
failure-retry-cnt *failure-retry-cnt*	Specifies the number of ping failures before recovery attempt. Valid range is from 0 to 999.
recovery-policy ip-monitoring	Specifies the recovery action to be taken when ip monitoring failure is detected. Valid values are reboot, shutdown, or none.
recovery-policy link-state-monitoring	Specifies the recovery action to be taken when link state failure is detected for the vNICs where the monitor-vnic is set to true. Valid values are shutdown or none.
max-recover-retries *max-recovery-retries*	Specifies the number of times recovery policy should be attempted. Valid range is from 0 to 16.
properties *properties*	Defines the properties of the service to be passed to the boot script of the image.
secure-boot	Enables or disables the secure boot for VNF when the firmware type is set to uefi. Valid values are true and false. Default value is false.

Parameter	Description
serial_port *serial_port*	Specifies a number for the serial port. Valid range is from 0 to 3.
serial_type *serial_type*	Specifies the type of the serial port. Valid values are console and telnet. The console value is valid only on serial number 0.
service_port *service_port*	Specifies the telnet port number for the telnet serial type. Valid range is from 1024 to 65,535.
storage_disk *id*	Specifies the ID of the storage disk. For releases earlier to 2.8.0, valid range is from 1 to 2. Starting from 2.8.0, the valid range is from 1 to 5.
storage_disk_location *disk_location*	Specifies the location of the storage disk. It can be a local location or an NFS-mounted location.
storage-disk-image-file *image_file_name*	Specifies the local or NFS-mounted ISO, RAW, or QCOW2 image file to be used as the additional storage disk for a service. A QCOW2 or RAW image is mounted as disk and an ISO image is mounted as CDROM. You can add up to two additional storage disks.
storage_disk_format	Specifies the format of the storage disk. Valid values are raw and qcow2. Default is raw.
storage_disk_device	Specifies the storage device. Valid values are disk or cdrom. Default is disk.
storage_disk_space_total_gb *disk_space*	Specifies the total amount of available disk space (in GB).
storage_disk_type *disk_type*	Specifies the storage disk type. Valid choices are ide and virtio. Default is ide.
uuid	Specifies a unique string to identify the service. The UUID value is automatically generated, when exporting the service.
vm_type	Indicates the type of virtual machine for the service. Valid value is generic.
vnc_password *password*	Specifies the VNC password for the service.
vnic	Specifies the vNICs associated with this service. For information about the vNIC parameters, see service name vnic command.

Command Modes

Global configuration (config)

Usage Guidelines

After you are satisfied with the configuration, enter the commit command to save the running configuration to the startup configuration persistently through reboots and restarts.

Examples

```
csp# config terminal
csp(config)# service CSR
csp(config-service-CSR)# memory 4096
```

```
csp(config-service-CSR)# numcpu 2
csp(config-service-CSR)# disk_size 4
csp(config-service-CSR)# iso_name csr1000v-universalk9.03.16.00.S.155-3.S-ext.iso
csp(config-service-CSR)# novnc-port 8721
csp(config-service-CSR)# storage_disk 1
csp(config-service-storage_disk-1)#   storage_disk_location       local
csp(config-service-storage_disk-1)#   storage_disk_format         raw
csp(config-service-storage_disk-1)#   storage_disk_device         disk
csp(config-service-storage_disk-1)#   storage_disk_space_total_gb 10.0
csp(config-service-storage_disk-1)#   storage_disk_type virtio
csp(config-service-storage_disk-1)#   exit
csp(config-service-CSR)# power on
csp(config-service-CSR)# vnic 0
csp(config-vnic-0)# vlan 200
csp(config-vnic-0)# tagged true
csp(config-vnic-0)# type access
csp(config-vnic-0)# model e1000
csp(config-vnic-0)# network_name Eth4-0
csp(config-vnic-0)# exit
csp(config-service-CSR)# vnic 1
csp(config-vnic-1)# vlan 201
csp(config-vnic-1)# tagged true
csp(config-vnic-1)# type access
csp(config-vnic-1)# model e1000
csp(config-vnic-1)# network_name Eth4-1
csp(config-vnic-1)# exit
csp(config-service-CSR)# vnic 2
csp(config-vnic-2)# vlan 202
csp(config-vnic-2)# tagged true
csp(config-vnic-2)# type access
csp(config-vnic-2)# model e1000
csp(config-vnic-2)# network_name enprs0r2
csp(config-vnic-2)# exit
csp(config-service-CSR)# exit
csp(config)# commit
csp# show service
NAME POWER  STATE  UPTIME CPU_LOAD DISK_USED_MB  MEM_USED_KB  ERROR
=============================================================================================================
CSR  on   deployed 17h39m59s  4       297.0        2028416     None
```

Day0 Configuration Example

```
csp# config terminal
csp(config)# service avi_test
csp(config-avi_test)# memory 4096
csp(config-avi_test)# iso_name se-pc-ss-ui.qcow2
csp(config-avi_test)# day0_filename avi_config1.yml,avi_config2.yml
csp(config-avi_test)# day0-dest-filename avi_meta_data_se_pc_1.yml,
csp(config-avi_test)# power on
csp(config-avi_test)# vnic 0
csp(config-vnic-0)# vlan 200
csp(config-vnic-0)# tagged true
csp(config-vnic-0)# type access
csp(config-vnic-0)# model e1000
csp(config-vnic-0)# network_name Eth4-0
csp(config-vnic-0)# exit
csp(config-avi_test)# exit
csp(config)# commit
```

Day0 Volume Label Example

```
csp# config terminal
csp(config)# service avi_test
csp(config-avi_test)# memory 4096
csp(config-avi_test)# iso_name se-pc-ss-ui.qcow2
csp(config-avi_test)# day0_filename avi_config1.yml
```

```
csp(config-avi_test)# day0-volume-id TEST
csp(config-avi_test)# power on
csp(config-avi_test)# vnic 0
csp(config-vnic-0)# vlan 200
csp(config-vnic-0)# tagged true
csp(config-vnic-0)# type access
csp(config-vnic-0)# model e1000
csp(config-vnic-0)# network_name Eth131-1
csp(config-vnic-0)# exit
csp(config-avi_test)# exit
csp(config)# commit
```

Service Description Example

```
csp# config terminal
csp(config)# service tiny1 iso_name tiny.iso power on description "tiny test descr" vnic 0 network_name
Eth130-0
csp(config-vnic-0)# commit
Commit Complete
csp(config-vnic-0)#
csp(config-vnic-0)#
csp(config-vnic-0)# exit
csp(config-service-tiny1)# description tiny new descr
csp(config-service-tiny1)# commit
Commit Complete
csp(config-service-tiny1)#
csp(config-service-tiny1)#
csp(config-service-tiny1)# no description
csp(config-service-tiny1)# commit
Commit Complete
```

Example for using Multiple Day0 Configuration and Day0 Destination File Names

```
csp# conig terminal
csp(config)# service config_tiny1 iso_name TinyCoreLinuxGUI.qcow2
csp(config-service-config_tiny1)# vnic 0 network_name Eth1-1
csp(config-vnic-0)# exit
csp(config-service-config_tiny1)# day0_filename "hello.txt,hello1.txt,config.txt"
csp (config-service-config_tiny1)# day0-dest-filename "/config/banner/,/config/banner/,/config/banner/"
csp(config-service-config_tiny1)# power on
csp(config-service-config_tiny1)# commit
Commit Complete
```

Example for using VNC Password Ecryption

```
csp# conig terminal
csp(config)# service vnc3 iso_name TinyCore-current.iso key 0 vnc_password vnc3pwd
csp(config-service-vnc3)# vnic 0 network_name Eth1-1
csp(config-vnic-0)# exit
```

Example for Service Monitoring

```
csp(config)# service csr
csp(config-service-csr)# iso_name csr1000v-universalk9.16.04.01.iso
csp(config-service-csr)# ip 10.193.75.160
csp(config-service-csr)# power on
csp(config-service-csr)# monitoring status enabled
csp(config-service-csr)# monitoring boot-time 600
csp(config-service-csr)# monitoring poll-interval 30
csp(config-service-csr)# monitoring failure-retry-cnt 5
csp(config-service-csr)# monitoring recovery-policy ip-monitoring reboot
csp(config-service-csr)# monitoring recovery-policy link-state-monitoring none
csp(config-service-csr)# vnic 0
csp(config-vnic-0)# network_name Eth4-0
csp(config-vnic-0)# exit
csp(config-service-csr)# commit
Commit Complete
```

Firmware and secure-boot Configuration Example

```
csp (config)# service uefivnf firmware uefi secure-boot true iso_name ubuntu-16.04-server-amd64.iso
csp (config-service-uefivnf)# commit
Commit Complete
```

Command History

Release	Modification
2.9.0	• The link-state-monitoring feature is added. Recovery-policy now has two leaf nodes: ip-monitoring and link-state-monitoring. • The monitor-vnic keyword is added to vNIC. This can be set to “true” to enable link-state-monitoring for the VNF.
2.8.0	The firmware and secure-boot parameters are added.
2.7.0	The services are exported in zip format and not tar.gz files.
2.4.1	The emulator-pin parameter is added.
2.3.1	• vnc_password strong strength validation and strong encryption scheme has been introduced. • The exported_location, exported_nfs_location, and export_live parameters has been added.
2.3.0	• The description parameter is added • The day0 file name and day0 destination file name support multiple files. • vnc_password encryption and key field is added. • VM monitoring parameters are added.
2.2.5	The day0-volume-id parameter is added.
2.2.4	The disk-resize and storage-disk-image-file parameters are added.
2.2.2	The day0-dest-filename parameter is added.
2.2.0	• The novnc-port and ip parameters are added. • The storage_disk_type parameter is added.
2.0.0	The export, day0_filename, disk_storage_name, image_storage_name, serial_ports, and storage_disks parameters are added. The disk_loc parameter is removed.
1.0	This command is introduced.

service name uuid

To retain a UUID when importing the service, use the service *name* uuid command.

service *name* iso_name *iso_name* memory *memory* numcpu *numcpu* uuid *uuid* vnic *vnic* network_name *network_name*

Syntax Description

Parameter	Description
Name	Name of the service.
iso_name *iso_name*	Specifies the ISO, OVA, or QCOW software image file, and zip file to be used to create the service. Note: With Cisco VSM and Cisco VSG services, only ISO image files are supported.
memory *memory*	Specifies the memory allocated for the service. The default value is 2048 (MB).
numcpu *numcpu*	Specifies the number of virtual CPUs for this service.
uuid *uuid*	Specifies a unique string to identify the service. The uuid value is automatically generated, when exporting the service.
vnic	Specifies the number for the vNIC. Valid range is from 0 to 23. In Release 2.2.3 and earlier releases, valid supported range is from 0 to 9.
network_name *network_name*	Specifies the name of the network. A network name is required for creating a vNIC. You can specify a pNIC name or a non-pNIC name as the network name. If the name of the network is not a pNIC name, then the network is virtual, and it is accessible only within services on the same Cisco CSP 2100.

Command Mode

Global configuration (config)

Usage Guidelines

Before exporting the service, you must note down the UUID of the service and during the import you can configure the UUID on the service that you have created.

Command History

Release	Modification
2.7.0	The option to retain a UUID of an exported service is introduced. The services are exported in zip format and not tar.gz files.

show service description

To display the description about a specific service, use the show service description command.

show service *name* description

Syntax Description

Parameter	Description
name	Name of the service.
description	Displays the description of the pNIC.

Command Modes

EXEC mode

Examples

```
csp # show service tiny1 description
description tiny test descr
csp #
```

Command History

Release	Modification
2.3.0	This command is introduced.

show service monitoring

To display the monitoring details about a specific service,.use the show service monitoring command.

show service *name* monitoring

Syntax Description

Parameter	Description
name	Name of the VM.
monitoring	Displays the monitoring details of the VM.

Command Modes

EXEC mode

Examples

```
csp # show service csr monitoring
vm_status vm_alive
monitoring total-recovery-count 0
monitoring monitor-action-state resumed
```

Command History

Release	Modification
2.3.0	This command is introduced.

service name vnic

To create vNICs associated with a service, use the service *name* vnic command.

service *name* vnic *nic_num* [mgmt-vnic {true | false}] [span-port {true | false}] [model {e1000 | virtio}] [native *vlan_num*] [network_name *network_name*] [tagged {true | false}] [type {access | passthrough | trunk}] [passthrough_mode {macvtap | pcie | sriov | none}] [vlan *vlan_num*] [spoofchk {on | off}] [monitor-vnic {true|false}]

Note:

- When a service has passthrough as well as non-passthrough vNICs, we recommend that you first define the non-passthrough vNICs and then define the passthrough vNICs.
- A network name is required for creating a vNIC. Therefore, you must either specify the network name in the network_name parameter or set the mgmt-vnic parameter to true. For more information, see the description of these parameters.

Syntax Description

Parameter	Description
name	Name of the service.
nic_num	A number for the vNIC. Valid range is from 0 to 23. In Release 2.2.3 and earlier releases, valid supported range is from 0 to 9.
mgmt-vnic	Configures the vNIC to use the dedicated service management interface. Valid values are true and false. When the value of this parameter is true, the configured dedicated service management interface (service-mgmt-pnic) is automatically specified as the value of the network_name parameter. No other value is supported in the network_name parameter. To remove the dedicated service management interface, specify false as the value of this parameter and specify a value in the network_name parameter.
span-port	Configures the vNIC to be spanned or not when you issue the span-ports tcpdump action start command from the CLI, REST, or web interface. This flag is always editable. Default is false. Note: Cannot be enabled on vNICs if the type parameter is configured as passthrough.
model	Specifies the model of the vNIC. Valid values are e1000 or virtio. Default is virtio. Note: For Cisco VSM and Cisco VSG services, you must specify the model as e1000.
native *vlan_num*	Specifies a native VLAN. Sets the native characteristics when the interface is in trunk mode. If you do not configure a native VLAN, the default VLAN 1 is used as the native VLAN.
network_name *network_name*	Specifies the name of the network. A network name is required for creating a vNIC. You can specify a pNIC name or a non-pNIC name as the network name. If the name of the network is not a pNIC name, the network is virtual, and it is accessible only within services on the same Cisco CSP 2100. If the mgmt-vnic parameter is set to true, the configured dedicated service management interface (service-mgmt-pnic) is automatically specified as the

Parameter	Description
	value of the network_name parameter. No other value is supported in the network_name parameter.
tagged	Specifies the tag setting for the port. Valid values are true and false.
type	Specifies the type of the port. Valid values are access, passthrough, and trunk. Default is access.
passthrough_mode	Configures the passthrough mode for a service. In the passthrough mode, a pNIC is not connected to a vSwitch and the data of the pNIC is directly passed to the configured service. Valid values are macvtap, pcie, sriov, and none. If the type parameter is configured as passthrough, the passthrough_mode parameter must be configured as macvtap, pcie, or sriov.
vlan *vlan_num*	Specifies the VLAN number. If the type parameter is configured as trunk, this parameter specifies a set of VLAN numbers and ranges. Note: You can configure a single VLAN on an SR-IOV VF interface. A VLAN tag is put on the VF interface when the vNIC using a SR-IOV VF is specified.
spoofchk	Specifies the spoofchk knob state on SR-IOV VF. Valid values are off, on. Note: This parameter can be only configured on SR-IOV VF.
monitor-vnic	Specifies when the vNIC has to be monitored, if VNF monitoring is enabled. If set to “true”, CSP monitors the link state of this vNIC, that is the link state of the *network_name*. If the link state goes down, the "recovery-policy link-state-monitoring” parameter is executed.

Command Modes

Service configuration (config-service)

Usage Guidelines

After you are satisfied with the configuration, enter the commit command to save the running configuration to the startup configuration persistently through reboots and restarts.

Examples

```
csp# config terminal
csp(config)# service vsm-sf vnic 1 network_name Eth130-0
csp(config-service-vsm-sf)# commit

csp# config terminal
csp(config)# service tiny3 vnic 2 mgmt-vnic true
csp(config-service-tiny3)# commit

csp# config terminal
csp(config)# service vsm-sf vnic 1 span-port true
csp(config-service-vsm-sf)# commit
```

Command History

Release	Modification
2.9.0	• The link-state-monitoring feature is added. Recovery-policy now has two leaf nodes: ip-monitoring and link-state-monitoring. • The monitor-vnic keyword is added to vNIC. This can be set to “true” to enable link-state-monitoring for the VNF.
2.3.1	The span-port, spoofchk parameters are added.
2.2.0	The mgmt-vnic parameter is added.
2.0.0	The passthrough_mode parameter added to this command.
1.0	This command is introduced.

show service pinning

To display the mapping between physical CPUs and virtual CPUs for a service, use the show service pinning command. You can view the emulator pinning and vhost-threads mapping. This information is consumed by the resource utilization graph on the GUI.

You can filter the service name, and view the CPU graph per service .

show service *name* pinning

Command Modes

EXEC mode

Example

```
csp# show service test1 pinning
pinning emu-map 1,2
VCPU  PCPU
------------
0     1
1     2
2     3
3     4

IND  PID    PCPU
------------------
  0.  13879  1
```

Command History

Release	Modification
2.6.0	This command is introduced.

span and tcpdump vnics

To span and tcpdump to pcap files for all span-port enabled vNICs, use the span-ports tcpdump action start/stop/show command.

span-ports tcpdump action {start | stop | show}

Syntax Description

Parameter	Description
action	Valid values are start, stop, and show. The show action gives you a list of each service coupled with its vNICs, their network_names and NIC numbers that are span-port enabled. The start action spans and then runs tcpdump to a pcap file for each vNIC shown by the show action. The stop action cleanly removes all the spanned ports, and finishes the tcpdump to pcap files.

Command Modes

EXEC mode

Usage Guidelines

- This is a global command for all span-port true vNICs.
- Using the start parameter of the command generates pcap files for each spanned vNIC as *tcpdump_<service name>_<nic number>.pcap*.
- The pcap files can be downloaded from the web interface at, Debug>TCP Dump>TCP Dump Files.
- After running the spanning/tcpdump, the spanning/tcpdump should be stopped with the stop action form of this command. The subsequent start or stop actions overwrites pcap files, if start or stop is run for the same vNICs.
- The pcap files have a maximum limit of 400K packets.
- There are no restrictions on a user to run this command.
- If there are no vNICs enabled for spanning on VNF vNICs, you should not use these commands. You can check the vNICs that are enabled for spanning with the action show command.

Examples

```
csp# span-ports tcpdump action show
{'tiny1': [['Eth130-3', '0'], ['Eth3-0', '2']]}

csp# span-ports tcpdump action start
tcpdump started

csp# span-ports tcpdump action stop
all tcpdumps stopped
```

Command History

Release	Modification
2.3.1	This command is introduced.

show running-config service

To display the running configuration information for all services or a specific service, use the show running-config service command.

show running-config service [*name*] [day0_filename |day0-dest-filename| day0-volume-id| disk_loc | disk_size | disk_storage_name | image_storage_name | iso_name | vnc_password | key | monitoring | description | macid | memory | novnc-port | numcpu | power | properties | serial_port | storage_disk | uuid | vm_type | vnc_password | vnics]

Syntax Description

Parameter	Description
name	Name of the service.
day0_filename	Displays the name of the Day0 configuration text file or iso file.
day0-dest-filename	Displays the name of the Day0 destination text or iso file.
day0-volume-id	Displays the volume label of the Day0 configuration text file or iso file.
disk_loc	Displays name of the image file used for service storage. This parameter is applicable only for Release 1.0.
disk_size	Displays the total amount of disk space available (in GB) for this service.
disk_storage_name	Displays the location of the service image file.
image_storage_name	Displays the location of the boot image.
iso_name	Displays the name of the ISO or OVA software image file.
vnc_password	Displays the encrypted VNC password.
key	Displays the key value, associated with the VNC password after encryption.
monitoring	Displays the monitoring details of the VM.
description	Displays a description about the service.
mac_id	Displays the MAC ID.
memory	Displays the number of bytes of memory allocated for the virtual service. The default value is 2048.
novnc-port	Displays the port number for the service console.
numcpu	Displays the number of virtual CPUs for this service.
power	Displays the state of the power upon activation.
properties	Displays the properties of the service to be passed to the boot script of the image.
storage_disk	Displays the storage disks.
uuid	Displays a unique string to identify the service.
vm_type	Displays the type of virtual machine on which the service is running.
vnc_password	Displays the services with VNC password.

Command Modes

EXEC mode

Usage Guidelines

None

Examples

```
csp# show running-config service
service EX1
 uuid      23e3fdec-2413-42b9-8b67-206cd3697159
 memory    2048
 numcpu    1
 macid     0
 disk_size 4
 iso_name  TinyCore-current.iso
 vnf-group  default-vnf-group
 vm_status vm_alive
 monitoring total-recovery-count 0
 monitoring monitor-action-state resumed
 key    7
 vnc_password  U2FsdGVkX1/0T6nxc+B0ta/O3AkJ0C5JWbjAz/eyoQDPuoF9pw1IhvjVM/LSRhxENc2rhLblhNH0cU4tuLeFnw==
 power     on
 day0_filename      config1.yml, config2.yml
 day0-dest-filename meta_data_se_pc_1.yml,
 day0-volume-id TEST
 novnc-port 8721
 vnic 0
  tagged       false
  type         access
  model        e1000
  network_name Eth4-0
 !
 vnic 1
  tagged       false
  type         access
  model        e1000
  mgmt-vnic    true
  network_name Eth4-1
 !
!
csp#
```

Command History

Release	Modification
2.3.1	vnc_password strong strength validation and strong encryption scheme has been introduced.
2.3.0	• The vnc_password and key parameters are added. • The description and monitoring parameters are added.
2.2.5	The day0-volume-id parameter is added.
2.2.2	The day0-dest-filename parameter is added.
2.2.0	The novnc-port parameter is added.
2.0.0	The export, day0_filename, disk_storage_name, image_storage_name, serial_ports,

	and storage_disks parameters are added to this command. The disk_loc parameter is removed from this command.
1.0	This command is introduced.

show service

To display statistics for all services or a specific service, use the show service command.

show service *name*

Syntax Description

Parameter	Description
name	Name of the service

Command Modes

EXEC mode

Example

```
csp# show service
NAME POWER STATE UPTIME CPU_LOAD DISK_USED_MB MEM_USED_KB IP CRYPTO_BW MB ERROR
test1 off deployed 0 None
test2 on deployed 6h47m3s 0 0.0 141264 0 None
test3 off deployed 0 None
test4 on deployed 5h48m16s 0 0.0 2147120 0 None
csp#
```

Command History

Release	Modification
1.0	This command is introduced.

show service vnic

To display the MAC addresses of vNICs, statistics of all vNICs or a specific vNIC, and VFs associated with a service, use the show service vnic command.

show service *name* vnic

Syntax Description

Parameter	Description
name	Name of the service

Usage Guidelines

- The vNIC or native OVS is displayed in the vnet-num format.
- The ovs-dpdk enabled vNIC is displayed as vhost-*servicename*-num format.

- The sriov interface is displayed as *pnic-name*_vf *number_bus-slot-func* format. For example, Eth1-1_vf2_7s14f2

Example

```
csp# show service test4 vnic
VF NETWORK    RX                                TX
NIC  MAC ADDRESS        NAME          PACKETS  BYTES    ERRORS  DROPPED  PACKETS  BYTES    ERRORS  DROPPED
-------------------------------------------------------------------------------------------------------
-
0    02:3C:17:B4:A5:0A  vnet1         49       3156     0       0        49       3156     0       0
1    02:4C:17:B4:A5:0A  vhost-csr2-1  2776     330556   0       0        2792     353188   0       0
2    02:5C:17:B4:A5:0A  vhost-csr2-2  2348     265242   0       0        2348     265242   0       0
csp#

csp# show service csr1 vnic
              RX                                  TX
NIC  MAC ADDRESS        VF NETWORK NAME      PACKETS  BYTES    ERRORS  DROPPED  PACKETS  BYTES    ERRORS
DROPPED
-------------------------------------------------------------------------------------------------------
--------
0    02:3C:17:B4:A5:08  vnet0                49       3156     0       0        49       3156     0       0
1    02:4C:17:B4:A5:08  Eth2-3_vf0_129s10    2792     375524   0       0        2776     341660   0       0
2    02:5C:17:B4:A5:08  Eth2-3_vf1_129s10f1  2348     284026   0       0        2348     274634   0       0
csp#
```

Command History

Release	Modification
2.6.0	Displays statistics of all NIC interfaces per service.
2.2.4	This command is introduced.

retain vm disk

You can deploy a service by using the .img file format and save the .img file of the service, before deleting it. If a VNF image is in NFS, the .img is saved in NFS and if VNF image is in the local repository, the .img file is saved in local repository. To save the .img file, use the retain vm disk command.

retain vm disk { true | false }

Syntax Description

Parameter	Description
name	Name of the service
disk { true | false }	Enables or disables the saving of the .img file of a service. Valid values are true and false. Default value is false.

Command Modes

Global configuration (config)

Usage Guidelines

You cannot save the .img file of the service in a powered on state and hence ensure that you power off the service to save it before deploying the service.

Example

```
csp# service test
csp# power off
csp# commit
csp# retain-vm-disk true
csp# commit
csp#
```

Command History

Release	Modification
2.5.0	This command is introduced.

telnet

To create a telnet session to a local service on a serial port or remotely access the serial port, use the telnet command.

telnet [*csp2100_mgmt_ip] service_port_number*

Syntax Description

Parameter	Description
csp2100_mgmt_ip	Cisco CSP 2100 management IP address. Use this parameter to remotely access the serial port using the management IP.
service_port_number	TCP port number for the telnet session.

Command Modes

EXEC mode

Examples

```
Example for remotely accessing the serial port
csp# telnet 10.10.1.1 1234

Example for locally accessing the serial port
csp# telnet 1234
```

Command History

Release	Modification
2.0.0	This command is introduced.

Session Commands

session idle-timeout

To set the idle timeout for sessions, use the session idle-timeout command. To revert to the default, use the no form of this command.

session idle-timeout *seconds*

Syntax Description

Parameter	Description
seconds	Number of seconds. The range is from 0 to 8182 seconds. Use 0 to disable the session idle timeout.

Defaults

600 seconds (10 minutes)

Command Modes

EXEC command mode (csp#)

Usage Guidelines

Only the members of admin-group group can configure the idle timeout for a session. The configured idle timeout is applicable to all users.

Example

```
csp# session idle-timeout 120
csp#
```

Command History

Release	Modification
2.1.0	This command is introduced.

SNMP Commands

show snmp agent

To display information about the SNMP agent, use the show snmp agent command.

show snmp agent

Syntax Description

None

Command Modes

EXEC mode

Example

```
csp# show snmp agent
snmp agent enabled
snmp agent sysDescr "Cisco CSP-2100"
snmp agent sysOID 1.3.6.1.4.1.9.12.3.1.3.1291
```

Command History

Release	Modification
2.1.0	This command is introduced.

show snmp traps

To display information about SNMP traps, use the show snmp traps command.

show snmp traps

Syntax Description

None

Command Modes

EXEC mode

Example

```
csp# show snmp traps
TRAP       TRAP
NAME       STATE
--------------------
linkDown   disabled
linkUp     disabled
```

Command History

Release	Modification
2.1.0	This command is introduced.

show snmp stats

To display SNMP statistics, use the show snmp stats command.

show snmp stats

Command Modes

EXEC mode

Example

```
csp# show snmp stats
snmp stats sysUpTime    108725690
snmp stats sysServices  70
snmp stats sysORLastChange 0
snmp stats snmpInPkts   2
snmp stats snmpInBadVersions 0
snmp stats snmpInBadCommunityNames 2
snmp stats snmpInBadCommunityUses 0
snmp stats snmpInASNParseErrs 0
snmp stats snmpSilentDrops 0
snmp stats snmpProxyDrops 0
```

Command History

Release	Modification
2.1.0	This command is introduced.

show running-config snmp

To display the running configuration information for SNMP, use the show running-config snmp command.

show running-config snmp

Command Modes

EXEC mode

Example

```
csp# show running-config snmp
snmp agent engineID 00:22:33:22:22:22:55
snmp community admin
community-access readOnly
!
snmp group g1 snmp 2 noAuthNoPriv
read test
write test
notify test
!
snmp user admin
user-version 2
user-group g1
!
```

Command History

Release	Modification
2.1.0	This command is introduced.

snmp agent

To specify the engine ID of an SNMP agent, use the snmp agent command.

snmp agent engineID *engine_id*

Note: You must configure SNMP agent before configuring SNMP community, group, user, host, or traps. Once configured, the engine ID cannot be deleted.

Syntax Description

Parameter	Description
engineID *engine_id*	Specifies the ID of the local or remote SNMP engine in hexadecimal format. Engine ID must be of minimum 5 octets.

Command Modes

Global configuration (config)

Example

```
csp# config terminal
csp# snmp agent engineID 00:22:33:22:22:22:55
```

Command History

Release	Modification
2.1.0	This command is introduced.

snmp community

To create an SNMP community, use the snmp community command. To remove the community, use the no form of this command.

snmp community *name* [community-access readOnly]

Syntax Description

Parameter	Description
name	SNMP community string to identify the community.
community-access	Specifies the access for this community. Only readOnly access is supported.

Command Modes

Global configuration (config)

Example

```
csp# config t
csp# snmp community public community-access readOnly
```

Command History

Release	Modification
2.1.0	This command is introduced.

snmp group

To create an SNMP group, use the snmp group command. To remove the SNMP group, use the no form of this command.

snmp group *name group_context_prefix* {1 | 2 | 3} {noAuthNoPriv | authNoPriv | authPriv} read *readview* write *writeview* notify *notifyview*

Syntax Description

Parameter	Description
name	Name of the SNMP group.
group_context_prefix	Specifies the context prefix. For SNMPv1 and SNMPv2c, only snmp context prefix is supported. For SNMPv3, starting with Release 2.2.2, you can specify any context prefix. You can also configure null context to run an SNMPv3 query without specifying the context name. To configure null context, use the \"\" character sequence as shown in the Examples section. In Release 2.2.1 and earlier releases, only snmp

Parameter	Description
	context prefix is supported with SNMPv3.
1 | 2 | 3	Specifies the SNMP version and the security level. Supported SNMP versions are as follows: • 1: SNMPv1 • 2: SNMPv2c • 3: SNMPv3
noAuthNoPriv | authNoPriv | authPriv	Specifies the security level for authentication and privacy. Supported security levels are as follows: • noAuthNoPriv: Security level that provides only user validation. • authNoPriv: Security level that provides authentication (MD5 or SHA). • authPriv: Security level that provides both authentication (MD5 or SHA) and encryption (AES or DES).
read *readview*	Specifies the name of the view for read access.
write *writeview*	Specifies the name of the view for write access.
notify *notifyview*	Specifies the name of the view for notify access.

Command Modes

Global configuration (config)

Example

```
csp# config t
csp# snmp group testgroup1 snmp 2 noAuthNoPriv read read-access write write-access notify notify-access

csp# config t
csp# snmp group testgroup2 \"\" 3 noAuthNoPriv read read-access write write-access notify notify-access
```

Command History

Release	Modification
2.1.0	This command is introduced.

snmp user

To configure a new user to an SNMP group, use the snmp user command. To remove the user, use the no form of this command.

snmp user *username* auth-protocol {md5 | sha} priv-protocol {aes | des} [passphrase *passphrase*] [user-group *groupname*] user-version {1 | 2 | 3}

Syntax Description

Parameter	Description
username	Name of the SNMP user.
auth-protocol	Specifies the authentication protocol. Valid values are: • MD5: Message Digest algorithm • SHA: Secure Hash algorithm
priv-protocol	Specifies the User-based Security Model (USM). Valid values are: • des: Data Encryption Standard algorithm • aes: Advanced Encryption Standard algorithm
passphrase *passphrase*	Specifies the passphrase. The minimum length required for a passphrase is 8 characters.
user-group *groupname*	Specifies the name of the SNMP group.
user-version	Specifies the SNMP version. Valid values are: • 1: SNMPv1 • 2: SNMPv2c • 3: SNMPv3

Command Modes

Global configuration (config)

Example

```
csp# config t
csp# snmp user public auth-protocol md5 priv-protocol des passphrase pass123 user-group 2 user-version 2
```

Command History

Release	Modification
2.1.0	This command is introduced.

snmp host

To configure an SNMP host, use the snmp host command. To remove the host, use the no form of this command.

snmp host *hostname* host-ip-address *ip_address* host-version *version* host-security-level *securitylevel* host-user-name *username* [host-port *port*]

Syntax Description

Parameter	Description
hostname	Name of the SNMP host.

Parameter	Description
host-ip-address *ip_address*	Specifies the IP address of the SNMP host.
host-version *version*	Specifies the version of the SNMP host. Supported SNMP versions are as follows: • 1: SNMPv1 • 2: SNMPv2c • 3: SNMPv3
host-security-level *securitylevel*	Specifies the security level for authentication and privacy. Supported security levels are as follows: • noAuthNoPriv: Security level that provides only user validation. • authNoPriv: Security level that provides authentication (MD5 or SHA). • authPriv: Security level that provides both authentication (MD5 or SHA) and encryption (AES or DES).
host-user-name *username*	Specifies the user name for the SNMP host.
host-port *port*	Specifies the port of the SNMP host. Default is port 162.

Command Modes

Global configuration (config)

Example

```
csp# config t
csp# snmp host host2 host-ip-address 2.2.2.2 host-port 162 host-version 2 host-security-level
noAuthNoPriv host-user-name public
csp# commit
```

Command History

Release	Modification
2.1.0	This command is introduced.

snmp enable traps

To enable a trap, use the snmp enable traps command. To disable a trap, use the no form of this command.

snmp enable traps *name*

Syntax Description

Parameter	Description
name	Name of the SNMP trap. Valid SNMP traps are linkDown and linkUp.

Command Modes

Global configuration (config)

Example

```
csp# config t
csp# snmp enable traps linkup
csp# commit
```

Command History

Release	Modification
2.1.0	This command is introduced.

show running-config snmp-server view

To display the running configuration information about family name and status of a Simple Network Management Protocol (SNMP) configuration and associated MIB, use the show running-config snmp-server view command in EXEC mode.

show running-config snmp-server view

Syntax Description

None

Command Modes

EXEC mode

Usage Guidelines

Use this command to display the SNMP server view configuration.

Example

The following example is a sample output that displays a view, myview, includes all MIB objects, except IF-MIB:

```
csp# show running-config snmp-server view

snmp-server view myview
  ALL included
  IF-MIB excluded
```

Command History

Release	Modification
2.3.0	This command is introduced.

show running-config snmp-server community

To display running configuration information about Simple Network Management Protocol (SNMP) community access strings, use the show running-config snmp-server community command in EXEC mode.

show running-config snmp-server community

Syntax Description

None

Command Modes

EXEC mode

Usage Guidelines

Community string consists of 1 to 32 alphanumeric characters and functions like a password enabling access to the SNMP entities.

To set up the community access string to permit access to the SNMP, use the snmp-server community command.

Example

The following example displays the community, mypublic, defined with read-write access to the view, myview:

```
csp# show running-config snmp-server community
snmp-server community mypublic view myview rw
```

Command History

Release	Modification
2.3.0	This command is introduced.

show running-config snmp-server group

To display the running configuration names of groups on CSP 2100 and the security model, and the status of the different views, use the show running-config snmp-server group EXEC command.

show running-config snmp-server group

Syntax Description

None

Command Modes

EXEC mode

Example

The following example displays the group name, mygroup, with security model v3, security level priv, and read-write option for myview:

```
csp# show running-config snmp-server group
snmp-server group mygroup v3 priv read myview write myview
```

Command History

Release	Modification
2.3.0	This command is introduced.

show running-config snmp-server user

To display running configuration information about each Simple Network Management Protocol (SNMP) username in the group, username table, use the show running-config snmp-server user EXEC command.

show running-config snmp-server user

Syntax Description

None

Command Modes

EXEC mode

Usage Guidelines

An SNMP user is a local user or remote user (remote defined in CLI). A remote user is usually associated with remote engineID setup. The user is designated using the snmp-server user command.

Example

The following example displays a local user, luser with sha authentication protocol and aes privacy protocol:

```
csp# show running-config snmp-server user luser
snmp-server user luser
mygroup v3
auth sha AFCAC136D0EB4681E797BAD6FD081B7334D8D8E8
priv aes 4627DCE3102B573C4CFCB076A3F2FCB3
```

The following example displays a remote user, v3user, in the remote trap server, 10.193.75.211 with security-model v3, md5 authentication protocol, and a remote engineID associated with the user:

```
csp# show running-config snmp-server user
snmp-server user v3user 10.193.75.211
remote 10.193.75.211 v3
auth md5 E89AF0F169151508D2E0BDB907048D71
engineID 000000090000d072dca0076d
```

Command History

Release	Modification
2.3.0	This command is introduced.

show running-config snmp-server host

To display running configuration information about the recipient details for Simple Network Management Protocol (SNMP) notification operations, use the show running-config snmp-server host command in EXEC mode.

show running-config snmp-server host

Syntax Description

None

Command Modes

EXEC mode

Usage Guidelines

The show running-config snmp-server host command displays details such as IP address of the Network Management System (NMS), notification type, SNMP version, and the port number of the NMS.

To configure these details, use the snmp-server host command.

Example

The following example displays a remote trap server, 10.193.75.211, with informs type of notification, version 3, authentication password of user v3user on port 162:

```
csp# show running-config snmp-server host
snmp-server host 10.193.75.211 informs version 3 auth v3user udp-port 162
```

Command History

Release	Modification
2.3.0	This command is introduced.

show running-config snmp-server enable

To display running configuration information about RFC 1157 Simple Network Management Protocol (SNMP) notifications, use the show running-config snmp-server enable EXEC command.

show running-config snmp-server user

Syntax Description

None

Command Modes

EXEC mode

Example

The following example displays information about trap function being enabled.

```
csp# show running-config snmp-server enable
snmp-server enable traps
```

Command History

Release	Modification
2.3.0	This command is introduced.

show running-config snmp-server location

To display running configuration information about the Simple Network Management Protocol (SNMP) system location string, use the show running-config snmp-server location command in EXEC mode.

show running-config snmp-server location

Syntax Description

None

Command Modes

EXEC mode

Usage Guidelines

To configure system location details, use the snmp-server location command.

Example

The following example displays the location information configured in snmp-server location.

```
csp# show running-config snmp-server location
snmp-server location csp@rack24_of_lab3
```

Command History

Release	Modification
2.3.0	This command is introduced.

show running-config snmp-server contact

To display running configuration information about Simple Network Management Protocol (SNMP) system contact information, use the show running-config snmp-server contact command in EXEC mode.

show running-config snmp-sever contact

Syntax Description

None

Command Modes

EXEC mode

Usage Guidelines

To set the system contact information, use the snmp-server contact command.

Example

The following example displays contact information configured in snmp-server contact.

```
csp# show running-config snmp-server contact
snmp-server contact admin@cisco.com
```

Command History

Release	Modification
2.3.0	This command is introduced.

show running-config snmp-server engineID

To display running configuration information about the identification of the local Simple Network Management Protocol (SNMP) engine that have been configured on CSP 2100, use the show running-config snmp-server engineID command in EXEC mode.

show running-config snmp-server engineID

Syntax Description

None

Command Modes

EXEC mode

Usage Guidelines

An SNMP engine is a copy of SNMP that can reside on a CSP 2100 host locally.

Example

The following example displays the local CSP engineID, 000000090000641225a85355:

```
csp# show running-config snmp-server engineID
snmp-server engineID local 000000090000641225a85355
```

Command History

Release	Modification
2.3.0	This command is introduced.

snmp-server view

To create or update a view entry, use the snmp-server view global configuration command. To remove the specified Simple Network Management Protocol (SNMP) server view entry, use the no form of this command.

snmp-server view *view-name oid-enum* {included | excluded}

no snmp-server view *view-name*

Syntax Description

Parameter	Description
view-name	Label for the view record that you are updating or creating. The name is used to reference the record. Valid values are a string up to 32 characters.
oid-enum	Object identifier enum can be 13 predefined enum text strings. These predefined text strings are ALL, CISCO-ENTITY-EXT-MIB, CISCO-PROCESS-MIB, DISMAN-EVENT-MIB, ENTITY-MIB, HOST-RESOURCE-MIB, IF-MIB, IP-MIB, LIBVIRT-MIB, LM-SENSORS-MIB, SNMP-FRAMEWORK-MIB, SNMPv2-MIB, TCP-MIB and UDP-MIB. Only these 14 predefined MIBs can be defined in the view configuration. You can use "tab" key to view the list of predefined MIBs.
included | excluded	Type of view. You must specify either included or excluded.

Defaults

No view entry exists.

Command Modes

Global configuration (config)

Usage Guidelines

Other SNMP commands require a view as an argument. You use this command to create a view to be used as arguments for other commands that create records including a view.

Example

The following example defines a view with specific MIBs:

```
csp# config t
csp(config)# snmp-server view myview ALL included
```

```
csp(config-view-my-view)# exit
csp(config)# snmp-server view myview IF-MIB excluded
csp(config-view-my-view)# end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.
```

Command History

Release	Modification
2.3.0	This command is introduced.

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 global configuration command. To remove the specified community string, use the no form of this command.

snmp-server community *community-name* [view *view-name*] [ro | rw]

no snmp-server community *string*

Syntax Description

Parameter	Description
community-name	Community name that acts like a password and permits access to the SNMP protocol. Valid values are a string up to 32 characters.
view *view-name*	(Optional) Name of a previously defined view. The view defines the objects available to the community.
ro	(Optional) Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
rw	(Optional) Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects.

Defaults

By default, an SNMP community name permits view-name as ALL MIBs and read-only access to all objects.

Command Modes

Global configuration (config)

Examples

The following examples provides two ways to define a community name–the simple way for versions v1 and v2c and VACM way for user-specific security model.

```
csp# config t
csp(config)# snmp-server community mypublic rw view myview
csp(config)# end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.
```

Note: Here the view has already been defined and if no view has been defined, the default will be ALL MIBs.

```
csp# config t
csp(config)# snmp-server group mygroup v2c read myview write myview
```

```
csp(config)# end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.
csp# config t
Entering configuration mode terminal
csp(config)# snmp-server user mypublic mygroup v2c
csp(config)# end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.
```

Note: Here the community has been defined in snmp-server user in VACM way, need snmp-server group and snmp-server user. If no view has been defined, the default will be ALL MIBs with read-only access privilege.

Command History

Release	Modification
2.3.0	This command is introduced.

snmp-server group

To configure a new Simple Network Management Protocol (SNMP) group, or a table that maps SNMP users to SNMP views, use the snmp-server group global configuration command. To remove a specified SNMP group, use the no form of this command.

snmp-server group *group-name* {v1 | v2c | v3 {auth | noauth | priv}} [read *readview*] [write *writeview*] [notify *notifyview*]

no snmp-server group

Syntax Description

Parameter	Description
group-name	The name of the group. Valid values are a string up to 32 characters.
v1	The least secure of the possible security models.
v2c	The second least secure of the possible security models. It allows for the transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed.
v3	The most secure of the possible security models. If v3 has been configured, at least one of the security fields must be specified.
auth	Specifies authentication of a packet without encrypting it.
noauth	Specifies no authentication of a packet.
priv	Specifies authentication of a packet with encryption.
read	(Optional) The option that allows you to specify a read view.
readview	A string (not to exceed 32 characters) that is the name of the view that enables you only to view the contents of the agent.
write	(Optional) The option that allows you to specify a write view.

Parameter	Description
writeview	A string (not to exceed 32 characters) that is the name of the view that enables you to enter data and configure the contents of the agent.
notify	(Optional) The option that allows you to specify a notify view
notifyview	A string (not to exceed 32 characters) that is the name of the view that enables you to specify a notify, inform, or trap.

Defaults

The following are default values for different views:

- *readview*–Assumed to be ALL MIBs, unless you use the read option to override this state.
- *writeview*–Nothing is defined for the write view (that is, the null OID). You must configure write access.
- *notifyview*–Nothing is defined for the notify view (that is, the null OID). If a view is specified, any notifications in that view that are generated will be sent to all users associated with the group (provided an SNMP server host configuration exists for the user).

Command Modes

Global configuration (config)

Example

The following example shows configuring a SNMP group with an existing view, **myview**:

```
csp# config t
Entering configuration mode terminal
csp(config)# snmp-server group mygroup v3 priv read myview write myview
csp(config)# end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.
```

Command History

Release	Modification
2.3.0	This command is introduced.

snmp-server user

To configure a new user to a Simple Network Management Protocol (SNMP) group, use the snmp-server user global configuration command. To remove a user from an SNMP group, use the no form of the command.

snmp-server user *user-id group-id* [remote] {v1 | v2c | v3 [encrypted] [auth {md5 | sha} *auth-password*]} [*priv* {aes | des } *priv-password*] [engineID *engine-id*]

no snmp-server user

Syntax Description

Parameter	Description
user-id	The name of the user for v3 or community name for v1 and v2c. Valid values are a

Parameter	Description
	string up to 32 characters.
group-id	The name of the group for local or host name when remote host is configured. Valid values are a string up to 32 characters.
remote	(Optional) Specifies a remote host name, or the IPv4 address of trap server.
v1	Specifies that SNMPv1 should be used.
v2c	Specifies that SNMPv2c should be used.
v3	Specifies that the SNMPv3 security model should be used. Allows the use of the encrypted and/or auth keywords.
encrypted	(Optional) Specifies whether the auth-password or priv-password appears in encrypted format (a series of digits, masking the true characters of the string usually in hex key format).
auth	(Optional) Specifies which authentication level should be used.
md5	The HMAC-MD5-96 authentication level.
sha	The HMAC-SHA-96 authentication level.
auth-password	A string (between 8 to 64 characters) that enables the agent to receive packets from the host.
priv-password	Specifies the User-based Security Model (USM). Valid values are a string between 8 to 64 characters.
priv	(Optional) Specifies the privacy algorithm.
des	Specifies the use of the 56-bit DES algorithm.
aes	Specifies the use of AES algorithm.
engineID *engine_id*	(Optional) Specifies the ID of the local or remote SNMP engine in hexadecimal format. The length of the engine ID can be between 5 to 32 octets. Default value is local CSP engine ID for remote user key generation.

Defaults

The following are default behaviors for encryption, passwords:

- encryption–Not present by default. The encrypted keyword is used to specify that auth and priv passwords are in hex format, such as, 0011...ff and not text password.
- passwords–Assumed to be text strings.

Command Modes

Global configuration (config)

Example

The following example shows how to enter a plain-text password for the string mypassword0 and mypassword1 for user v3user in group-name mygroup, type the following command line:

```
csp# config t
Entering configuration mode terminal
csp(config)# snmp-server user v3user mygroup v3 auth md5 mypassword0 priv aes mypassword1
csp(config)# end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.
```

Note: While using the VACM way, the group and user commands must be used together with the user defined in the snmp-server user command. If no view has been defined, the default will be ALL MIBs with read-only access privilege.

Command History

Release	Modification
2.3.0	This command is introduced.

snmp-server host

To specify the recipient of a Simple Network Management Protocol (SNMP) notification operation, use the snmp-server host global configuration command. To remove the specified host, use the no form of this command.

snmp-server host *host-name* [traps | informs] version {1 | 2c | 3 {auth | noauth | priv}} *remote-id* [udp-port *port*]

no snmp-server host *host-name* [traps | informs]

Syntax Description

Parameter	Descriptio
host-name	Name or IPv4 of the host (the targeted recipient). Valid values are a string up to 32 characters.
traps	(Optional) Sends SNMP traps to this host. This is the default.
informs	(Optional) Sends SNMP informs to this host.

version	Version of the SNMP used to send the traps. Version 3 is the most secure model, because it allows packet encryption with the priv keyword. When you use the version keyword, one of the following must be specified:
	• 1–SNMPv1. This option is not available with informs.
	• 2c–SNMPv2C.
	• 3–SNMPv3. The following three optional keywords can follow the version 3 keyword. If version 3 has been configured, at least one of the security fields must be specified.
	  ○ auth (Optional) Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication.
	  ○ noauth (Default) The noAuthNoPriv security level. This is the default if the [auth | noauth | priv] keyword choice is not

Parameter	Descriptio
	specified. ○ priv (Optional) Enables Data Encryption Standard (DES) packet encryption (also called "privacy").
remote-id	When v1 or v2c are specified, enter the password-like community string sent with the notification operation. When version 3 is specified, enter the SNMPv3 username.
udp-port *port*	(Optional) UDP port of the host to use. The default is 162.

Defaults

This command is disabled by default. No notifications are sent.

Command Modes

Global configuration (config)

Examples

- The following example enables CSP 2100 to send all traps to the host myhost.cisco.com by using the community string public:

```
csp# config t
csp(config)# snmp-server enable traps
csp(config)# snmp-server host myhost.cisco.com public
```

- The following example enables CSP 2100 to send all inform requests to the host myhost.cisco.com by using the community string public:

```
csp# config t
csp(config)# snmp-server enable traps
csp(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Command History

Release	Modification
2.3.0	This command is introduced.

snmp-server enable traps

To enable the sending of RFC 1157 Simple Network Management Protocol (SNMP) notifications, use the snmp-server enable traps global configuration command. To disable RFC 1157 SNMP notifications, use the no form of this command.

snmp-server enable traps [snmp]

no snmp-server enable traps

Syntax Description

Parameter	Description
snmp	(Optional) Controls (enables or disables) RFC 1157 SNMP notifications.

Defaults

SNMP notifications are not enabled by default.

If you enter this command with none of the optional keywords, all RFC 1157 SNMP notifications are enabled (or disabled, if using the no form).

Command Modes

Global configuration (config)

Examples

The following example defines the SNMP v1 and v2c traps:

```
csp# config t
Entering configuration mode terminal
csp(config)# snmp-server user remotepublic 10.10.10.100 remote 10.10.10.100 v2c
csp(config)# end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.

csp# config t
Entering configuration mode terminal
csp(config)# snmp-server host 10.10.10.100 informs version 2c remotepublic
csp(config)# end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.
```

The following example defines the SNMP v3 traps:

```
csp# config t
Entering configuration mode terminal
csp(config)# snmp-server user remoteuser 10.100.100.100 remote 10.100.100.100 v3 auth sha mypassword0
priv aes mypassword1
csp(config)# end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.

csp# config t
Entering configuration mode terminal
csp(config)# snmp-server host 10.100.100.100 informs version 3 priv remoteuser
csp(config)# end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.
```

Command History

Release	Modification
2.3.0	This command is introduced.

snmp-server location

To set the system location string, use the snmp-server location global configuration command. To remove the system location string, use the no form of this command

snmp-server location *location-string*

no snmp-server location

Syntax Description

Parameter	Description
location-string	String that describes the system location information. The maximum length of the location string can be 255 characters.

Defaults

No system location string is set.

Command Modes

Global configuration (config)

Example

```
csp# config t
csp(config)# snmp-server location csp@rack24_of_lab3
```

Command History

Release	Modification
2.3.0	This command is introduced.

snmp-server contact

To set the system contact (sysContact) string, use the snmp-server contact global configuration command. To remove the system contact information, use the no form of this command

snmp-server contact *contact-string*

no snmp-server contact

Syntax Description

Parameter	Description
contact-string	String that describes the system contact information. The maximum length of the contact string can be 255 characters.

Defaults

No system contact string is set.

Command Modes

Global configuration (config)

Example

```
csp# config t
csp(config)# snmp-server contact admin@cisco.com
```

Command History

Release	Modification
2.3.0	This command is introduced.

snmp-server engineID

To configure a name for local Simple Network Management Protocol (SNMP) engine on CSP 2100, use the snmp-server engineID global configuration command. To remove the configured engine ID, use the no form of this command.

snmp-server engineID {local *engineid-string*}

no snmp-server engineID

Syntax Description

Parameter	Description
local	Specifies the local copy of SNMP on CSP 2100.
engineid-string	The name of a copy of SNMP. The length of the engineID string can be 12 octets.

Defaults

An SNMP engine ID is generated automatically and stored in the running configuration. Therefore, you can display the default or configured engine ID by using the show running-config snmp-server engineID EXEC command.

Command Modes

Global configuration (config)

Usage Guidelines

The engineID is 24 character and does not support trailing zeros. To configure an engine ID of 123400000000000000000000, you must specify the entire engineID; for example, snmp-server engineID local 123400000000000000000000.

Changing the value of snmpEngineID has important side-effects. A user's password (entered on the command line) is converted to an MD5 or SHA security digest. This digest is based on both the password and the local engine ID. The command line password is then destroyed, as required by RFC 2274. Because of this deletion, if the local value of engineID changes, the security digests of SNMPv3 users will be invalid, and the users will have to be reconfigured.

Command History

Release	Modification
2.3.0	This command is introduced.

Start, Stop Counter Commands

To provide traffic statistics data between a period for monitoring a specific physical interface in CSP or virtual interface in a service, use the start, stop counter command.

start-counters

To start the counters at a specific time with an optional period, use the start-counters command.

start-counters { all-intf | all-pnics | all-services | pnic | service | vnic | period }

Syntax Description

Parameter	Description
all-intf	For all interfaces including physical interfaces and virtual interfaces in services.
all-pnics	For all physical interfaces.
all-services	For all virtual interfaces inside the services.
pnic	Specifies a physical interface name.
service	Specifies a service name.
vnic	Specififes the interface associated with a service. This is optional parameter for a service.
period	Specifies the period for the counters to be recorded and the unit is in seconds.

Command Modes

EXEC mode

Examples

```
csp# start-counters all-intf
csp# start-counters pnic Eth0-1 period 20
csp# start-counters service myservice
csp# start-counters service myservice vnic 0
```

Command History

Release	Modification
2.6.0	This command is introduced.

stop-counters

To stop the counters at a specific time, use the stop-counters command.

stop-counters { all-intf | all-pnics | all-services | pnic | service | vnic }

Syntax Description

Parameter	Description
all-intf	For all interfaces including physical interfaces and virtual interfaces in services.
all-pnics	For all physical interfaces.
all-services	For all virtual interfaces inside the services.
pnic	Specifies a physical interface name.
service	Specifies a service name.
vnic	Specifies the interface associated with a service. This is optional parameter for a service.

Command Modes

EXEC mode

Examples

```
csp# stop-counters all-pnics
csp# stop-counters pnic Eth0-1
csp# stop-counters service myservice
csp# stop-counters service myservice vnic 0
```

Command History

Release	Modification
2.6.0	This command is introduced.

show-counters

To show the counters recorded between start-counters and stop-counters, use the show-counters command.

show-counters { all-intf | all-pnics | all-services | pnic | service | vnic }

Syntax Description

Parameter	Description
all-intf	For all interfaces including physical interfaces and virtual interfaces in services.
all-pnics	For all physical interfaces.
all-services	For all virtual interfaces inside the services.
pnic	Specifies a physical interface name.
service	Specifies a service name.
vnic	Specifiifes the interface associated with a service. This is optional parameter for a service.

Command Modes

EXEC mode

Examples

```
csp# show-counters all-pnics
csp# show-counters pnic Eth0-1
csp# show-counters service myservice
csp# show-counters service tiny3 vnic 0

counters tiny3 0
tiny3: 0
start: 2019-10-30 20:14:52 stop: 2019-10-31 18:15:12
period: 0 days,22 hours,0 mins,20 secs
rx_bytes rx_packets rx_errors rx_dropped rx_multicast rx_broadcast
12711822 112579 0 0 0 0
tx_bytes tx_packets tx_errors tx_dropped tx_multicast tx_broadcast
2799612 8186 0 0 0 0
collisions
0
```

Command History

Release	Modification
2.6.0	This command is introduced.

System Commands

cpupin

To pin each VNF CPU to a particular system CPU, use the cpupin command.

Note: Toggling the cpupin configuration requires a reboot of the Cisco CSP 2100 host. Once the configuration is changed, ensure that you reboot Cisco CSP 2100.

cpupin {enable | disable}

Syntax Description

Parameter	Description
enable	Enables the VNF CPU pinning. This feature provides dedicated allocation of CPU resources across VNFs and host processes.
disable	Disables the VNF CPU pinning.

Command Modes

Global configuration (config)

Examples

```
csp(config)# cpupin enable
```

Command History

Release	Modification
2.2.4	This command is introduced.

cpupin-state

To display the current running state of the cpupin configuration, use the cpupin-state command . If the cpupin confguration has been toggled, cpupin-state will be updated after the reboot of the Cisco CSP 2100 host.

Syntax Description

This command has no arguments or keywords.

Command Modes

Global configuration (config)

Example

```
csp(config)# show cpupin-state
result
```

```
cpupin-state 1
```

Command History

Release	Modification
2.2.5	This command is introduced.

show system iostat

To display the disk I/O statistics, use the show system iostat command.

show system iostat [disk *name* | extend]

Syntax Description

Parameter	Description
disk *name*	Displays the statistics for the specified disk. You can specify multiple disks in the following format: "*name1 name2*".
extend	Displays the extended statistics.

Command Modes

EXEC mode

Examples

```
csp# show system iostat
result
Linux 3.10.0-693.el7.x86_64 (csp)         10/27/2020      _x86_64_        (32 CPU)
avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           0.05    0.00    0.05    0.21    0.00   99.70
Device:            tps    kB_read/s    kB_wrtn/s    kB_read    kB_wrtn
sda               2.65        49.15        19.76     526706     211820
sda1              0.01         0.31         0.00       3356          0
sda2              2.12        42.77        13.46     458361     144296
sda3              0.02         0.21         0.00       2292          0
sda4              0.00         0.05         0.00        535          0
sda5              0.03         0.21         0.01       2237        104
sda6              0.46         4.99         6.29      53453      67420
dm-0              0.50         2.79         0.25      29868       2706

csp# show system iostat extend
result
Linux 3.10.0-693.el7.x86_64 (csp)         10/27/2020      _x86_64_        (32 CPU)
avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           0.05    0.00    0.05    0.21    0.00   99.70
Device:         rrqm/s   wrqm/s     r/s     w/s    rkB/s    wkB/s avgrq-sz avgqu-sz   await r_await
w_await  svctm  %util
sda               0.10     1.96    1.50    1.15    49.00    19.75    51.92     0.02    5.95    5.71
6.27   0.87   0.23
sda1              0.00     0.00    0.01    0.00     0.31     0.00    72.17     0.00    4.11    4.11
0.00   1.33   0.00
sda2              0.10     1.14    1.22    0.89    42.64    13.46    53.00     0.01    6.46    6.41
6.53   0.88   0.19
sda3              0.00     0.00    0.02    0.00     0.21     0.00    25.90     0.00    1.82    1.82
0.00   1.62   0.00
```

```
sda4              0.00     0.00    0.00    0.00     0.05     0.00    50.95     0.00    1.90    1.90
0.00   1.71   0.00
sda5              0.00     0.00    0.03    0.00     0.21     0.01    16.43     0.00    2.38    2.11
6.94   1.49   0.00
sda6              0.00     0.81    0.21    0.25     4.97     6.28    48.75     0.00    4.15    2.69
5.37   1.25   0.06
dm-0              0.00     0.00    0.30    0.19     2.78     0.25    12.25     0.00    2.56    2.27
3.00   0.38   0.02

csp# show system iostat disk "sda1 sda2"
result
Linux 3.10.0-693.el7.x86_64 (csp)         10/27/2020      _x86_64_        (32 CPU)
avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           0.05    0.00    0.05    0.21    0.00   99.70
Device:            tps    kB_read/s    kB_wrtn/s    kB_read    kB_wrtn
sda1              0.01         0.31         0.00       3356          0
sda2              2.11        42.52        13.44     458361     144892
```

Command History

Release	Modification
2.2.4	This command is introduced.

TACACS+ Commands

tacacs-server host

To configure a TACACS+ server, use the tacacs-server host command. To delete a configured TACACS+ server, use the no form of this command.

tacacs-server host *hostname* [key *key_value*] shared-secret *shared-secret*

To configure Cisco attribute-value (AV) pair privilege level (priv-lvl) on TACACS+ server, see the csp-users users command.

Syntax Description

Parameter	Description
hostname	Hostname or IPv4 or IPV6 address of the TACACS+ server.
key *key_value*	Defines the type of the shared-secret key. Valid values are the following: • 0: The shared-secret key is specified in clear text. This is the default. • 7: The shared-secret key is specified in encrypted text.
shared-secret *shared-secret*	Specifies the preshared secret to authenticate communication between the TACACS+ server and Cisco CSP 2100. The preshared secret is alphanumeric, case sensitive, and has a maximum of 63 characters. If the specified shared-secret is in clear text, Cisco CSP 2100 encrypts the shared-secret and changes the key parameter to 7 (as shown in the Examples section). If the specified shared-secret is already encrypted, Cisco CSP 2100 does not make any change.

Command Modes

Global configuration (config)

Examples

```
csp(config)# tacacs-server host 10.10.10.2
csp(config-host-10.10.10.2)# key 0
csp(config-host-10.10.10.2)# shared-secret tac_test
csp(config-host-10.10.10.2)# commit
csp# show running-config tacacs-server
tacacs-server host 10.10.10.2
key           7
shared-secret sec_code
!
csp(config)# tacacs-server host 10.10.10.1
csp(config-host-10.10.10.1)# key 7
csp(config-host-10.10.10.1)# shared-secret already_ciphered
csp(config-host-10.10.10.1)# commit
csp# show running-config tacacs-server
tacacs-server host 10.10.10.1
key           7
shared-secret already_ciphered
!
```

Command History

Release	Modification
2.1.0	This command is introduced.

Time Zone Commands

clock timezone

To configure the time zone for Cisco CSP 2100, use the clock timezone command. To delete the configured time zone, use the no form of this command.

clock timezone *continent/city*

You can view the configured time zone by using the show running-config clock timezone command. When you delete the configured time zone, the time zone is set to the default: `America/New_York`.

Syntax Description

Parameter	Description
continent/city	Name of the continent and city separated by a forward slash (/).

Command Modes

Global configuration (config)

Example

```
csp# show running-config clock timezone
clock timezone America/New_York
```

Commands

```
csp# config t
csp# clock timezone Asia/Bangkok
csp# commit
```

Command History

Release	Modification
2.2.2	This command is introduced.

show running-config clock timezone

To display the time zone information, use the show running-config clock timezone command.

show running-config clock timezone

Command Modes

EXEC mode

Example

```
csp# show running-config clock timezone
clock timezone Asia/Bangkok
```

Command History

Release	Modification
2.2.2	This command is introduced.

Technical Support Information Commands

support show-tech operation generate-report

To generate technical support information to diagnose an issue or to attach to a Cisco TAC case, use the support show-tech operation generate-report command.

support show-tech operation generate-report

Command Modes

EXEC mode

Usage Guidelines

This command creates a csp_show_tech.tar.gz file in the log directory. This csp_show_tech.tar.gz file contains relevant log files and configuration files and it can take up to 15 minutes to create this file. If a csp_show_tech.tar.gz file already exists in the log directory, the existing file is overwritten when you run this command. You can copy the csp_show_tech.tar.gz file by using the following command:

copy log csp_show_tech.tar.gz *location*

where *location* is specified as user@host:file.

Example

```
csp# support show-tech operation generate-report
csp# copy log csp_show_tech.tar.gz user1@myhost:/myfile
```

Command History

Release	Modification
1.0	This command is introduced.

User Commands

Release 2.1.0 and Later Releases

csp-users users

To create a new user or modify an existing user, use the csp-users users command. To delete a user, use the no form of this command.

csp-users users user *username* password *password* **group** *group*

Only the members of the **admin-group** group can run this command to create a new user and delete or modify a user.

Note: Before Release 2.3.1, a user who is part of the admin-group can create user or groups. Starting with Release 2.3.1, the admin user has been moved to the superadmin group. Only an admin user can create users or groups and all users of admin-group can no longer create users or groups.

Note: Starting with release 2.2.2, you cannot use this command to change the password of a user. To change the password of a user, use the change-password users command.

Syntax Description

Parameter	Description
user *username*	Specifies the username. The user is considered as a local user and is authenticated locally by the Cisco CSP 2100. A user can also be defined remotely. In such cases, remote authentication is used to authenticate the user. Local authentication is used only if the remote authentication is not available. Local authentication is not used as the secondary authentication method if the remote authentication is rejected.
password *password*	Specifies the password in clear text. In running configuration, the password is displayed as a hashed entry. The password is mandatory.
group *group*	Specifies the group for a user. Valid values are admin-group, operator-group, service-group, vnf-operator-group, and one of the user created vnf-group. For TACACS+ and RADIUS configuration, following are the privilege levels (priv-lvl) or class that are assigned to various user groups: • admin-group—15 • operator-group—1 • service-group—7 • vnf-operator-group—a string, "vnf-operator-group"

	• user-created vnf-group—a string with the group name

Command Modes

Global configuration (config)

Example

```
Example for creating an operator group with its associated privilege level
csp# config t
csp# csp-users users user abc-oper
csp(config-user-abc-oper)# password newSecret@123456
csp(config-user-abc-oper)# group operator-group
csp(config-user-abc-oper)# commit
```

Command History

Release	Modification
2.3.0	Introduced a new VNF group, vnf-operator-group
2.1.0	This command is introduced.

change-password users

To change the password of a user, use the change-password users command.

change-password users username *username* old-password *old-password* new-password *new-password*

Syntax Description

Parameter	Description
username *username*	Specifies the username.
old-password *old-password*	Specifies the old password.
new-password *new-password*	Specifies the new password.

Command Modes

Global configuration (config)

Example

```
csp# config t
csp# change-password users username abc-oper
csp(config-user-abc-oper)# old-password oldSecret@123456
csp(config-user-abc-oper)# new-password newSecret@123456
csp(config-user-abc-oper)# commit
```

Command History

Release	Modification
2.2.2	This command is introduced.

show running-config csp-users

To display the running configuration information about Cisco CSP 2100 users, use the show running-config csp-users command.

show running-config csp-users

Note: Only the members of the admin-group group can run this command to view information about all users. Members of any other group can only get information about their own user ID.

Command Modes

EXEC mode

Example

```
csp# show running-config csp-users
csp_users users user abc-admin
 group admin-group
!
csp_users users user abc-oper
 group operator-group
!
csp_users users user abc-service
 group service-group
!
```

Command History

Release	Modification
2.1.0	This command is introduced.

Release 1.0 and 2.0.0

csp_users create-user

To change the password for the admin user, use the csp_users create-user command.

csp_users create-user *username* admin password *newpassword*

Note: This command is available only in Release 1.0 and Release 2.0.0. Starting with Release 2.1.0, the csp-users users command is introduced.

Syntax Description

Parameter	Description
username	Specifies the user for which the password needs to be changed. In Release 1.0 and Release 2.0, only admin user is supported.
password *newpassword*	Specifies the new password for the admin user. The new password overwrites the existing password.

Command Modes

EXEC mode

Example

```
csp# csp_users create-user username abc-oper password secret group operator-group
csp#
```

Command History

Release	Modification
2.1.0	This command is removed.
1.0	This command is introduced.

VNF User Group Commands

The VNF user group commands allow you to configure VNF user groups, add users to the VNF groups and associate VNFs (service VMs) to those users. The users within VNF group have full access to VNFs associated with their groups and do not have access to other VNFs. You can create maximum of 10 VNF user groups.

Note: The users cannot create new VNFs and has no CSP admin-group privileges.

csp-users groups

To create a new VNF user group or a user-created group, or modify an existing VNF or user-created user group, use the csp-users groups command. To delete a VNF or user-created user group, use the no form of this command.

csp-users groups group *groupname* type *grouptype*

no csp-users groups group *groupname*

Syntax Description

Parameter	Description
group *groupname*	Specifies the VNF group name or user-created group name of a service. Valid values are an alphanumeric string except admin-group, operator-group, service-group, and vnf-operator-group.
type *grouptype*	Specifies the group type that can be either, none, service, operator, or vnf-operator. The type, none gives permissions that is equivalent to type service. Each of these group types mimic the permissions of the base groups of the same prefix. This behavior means that the operator type vnf-groups has read-only permissions on VNFs that have this group as their vnf-group. It is similar to a base operator-group. Default is of type, service.

Note: To add users to the admin-group, operator-group, service-group, and vnf-operator-group groups, use the csp-users users command. Any CSP user under service-group have complete access to all VNFs.

Command Modes

Global configuration (config)

Usage Guidelines

Modify an existing VNF user group by using the following command to change the group type.

csp-users groups group *groupname* type *newgrouptype*

Example

```
Example for creating a VNF user group
csp# config terminal
csp (config) # csp-users groups group abc-test type service
csp(config-users-groups-abc-test)# commit
Commit complete.
csp(config-users-groups-abc-test)# exit

Example for creating a user-created group
csp# config terminal
csp (config) # csp-users groups group router-group type operator
csp(config-users-groups-router-group)# commit
Commit complete.
csp(config-users-groups-router-group)# exit
```

Command History

Release	Modification
2.3.1	This command is extended to include operator, vnf-operator group types.
2.3.0	This command is introduced.

service name vnf group

To associate services to VNF groups, use the service name vnf group command.

service *service-name* iso_name *vm-image* vnf-group *vnf-group-name*

Syntax Description

Parameter	Description
service *service-name*	Name of the service.
iso_name *vm-image*	Name of the ISO or VM image file.
vnf-group *vnf-group-name*	Name of the VNF group.

Command Modes

Global configuration (config)

Example

```
csp# config t
csp (config)# service vsm-sf iso_name TinyCore-current.iso vnf-group abc-test

Example for associating with a VNF user group
csp# config terminal
Entering configuration mode terminal
csp (config-service)# vnf-group abc-test
csp(config-pnic-Eth4-0)# commit
Commit complete.
csp(config-service-vnf-group-abc-test)# exit
```

Command History

Release	Modification
2.3.0	This command is introduced.

vNIC Commands

vNIC

To modify the configuration of a vNIC, use the vnic command.

vnic *nic_num* [bandwidth *bandwidth*] [adminstatus {up | down}]

Syntax Description

Parameter	Description
nic_num	A number for the vNIC. Valid range is from 0 to 23. In Release 2.2.3 and earlier releases, valid supported range is from 0 to 9.
bandwidth *bandwidth*	Specifies bandwidth in megabits per second and should be a positive integer. This parameter is not available if the vNIC is configured as a passthrough interface with passthrough modes, pcie and macvtap. The maximum bandwidth for an interface based on the configured value is controlled. For SRIOV, the actual bandwidth is closer to the configured value, and for OVS and DPDK it varies but maximum is the configured value.
adminstatus *adminstatus*	Shuts down or re-enables a disabled vNIC. Valid values are up and down. This parameter is not available if the vNIC is configured as a passthrough interface with passthrough modes, pcie and macvtap.

Command Modes

Global configuration (config)

Example

```
csp# config terminal
Entering configuration mode terminal
csp (config)# service a
csp (config-service-a)# vnic 0
csp(config-vnic-0)# adminstatus up
csp(config-vnic-0)# bandwidth 2000
csp(config-vnic-0)# commit
Commit complete.
csp(config-vnic-0)# exit
```

Command History

Release	Modification
2.6.0	This command is introduced.

show vnic_stat

To display statistics for all vNICs or a specific vNIC, use the show vnic_stat command.

show vnic_stat [*name*]

In the output of this command, the vNIC name is shown in the vnet*num* format. For each running service, the *num* value is increased (vnet0, vnet1, and so on) corresponding to the (first, second, and so on) vNIC for each service.

Starting with release 2.3.0, the MAC address field is not displayed. To view the MAC address field, use the show service vnic command.

Starting with release 2.6.0, use the show service vnic command to view statistics of all NIC interfaces.

Syntax Description

Parameter	Description
name	Name of the vNIC

Command Modes

EXEC mode

Example

```
csp# show vnic_stat vnet0
Name    Service     Rx Bytes    Packets     Errors    Dropped    Mbps    TX Bytes    Packets    Errors
Dropped    Mbps
================================================================================================================
================================================
vnet0   SMP_Service  37497750    108375          0        0       0.0     37064250    108375        0
0           0.0
csp#

csp-2100-4# show vnic_stat
Name    Service    Rx Bytes    Packets    Errors    Dropped    Mbps    TX Bytes    Packets    Errors
Dropped  Mbps
================================================================================================================
================================================
vhost-test1-1    test1 173394   507        0          0         0.0      333450      975        0
  0      0.0
vhost-test2-1    test2 173394   507        0          0         0.0           0        0        0
  0      0.0
vhost-test3-1    test3 173394   507        0          0         0.0      333108      974        0
  1      0.0
vhost-test4-0    test4 160056   468        0          0         0.0      318060      930        0
 29      0.0
vnet0   test1          173394   507        0          0         0.0           0        0        0
 0      0.0
vnet1   test2          173394   507        0          0         0.0           0        0        0
 0      0.0
vnet2   test3          173394   507        0          0         0.0       49432      167        0
 0      0.0
vnet3   test4          160056   468        0          0         0.0       345722     2673        0
```

```
0       0.001
```

Command History

Release	Modification
2.6.0	This command has been deprecated.
2.3.0	Removed MAC address field to be displayed.
1.0	This command is introduced.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.

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

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

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

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

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

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

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

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