Cisco Cloud Services Platform Quick Start Guide, Release 2.5.0

First Published: 2018-10-15

Last Modified: 2019-08-26

Information About Cisco Cloud Services Platform

Cisco Cloud Services Platform is a software and hardware platform for data center network functions virtualization. This open kernel virtual machine (KVM) platform, with Red Hat Enterprise Linux (RHEL) 7.3 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.

Setting Up Your CSP and Configuring Services

Summary Steps

Setting up your Cisco Cloud Services Platform (Cisco CSP) and creating services consists of the following high-level steps:

Procedure

Step 1 Upgrade the Cisco CSP software or perform the initial setup.

Step 2 Log in to the Cisco CSP 2100.

Step 3 Generate and install an SSL certificate.

Step 4 Access Cisco CSP through the web interface.

Step 5 Upload the service image to the Cisco CSP.

Step 6 Create a service.

Step 7 Verify the service instance.

Upgrading the Cisco CSP Software

You can upgrade the Cisco CSP software by installing an ISO image through any of the following methods:

- Using the Cisco Integrated Management Controller (CIMC) KVM console: Map the ISO image to the Virtual CD/DVD by using the CIMC console and then install the image. The ISO image installation through CIMC console is useful for clean installations because the CIMC KVM or a direct console connected to the Cisco CSP system is required to perform the tasks described in Performing the Initial Setup, on page 2.

- Using the Cisco CSP 2100 CLI or REST APIs: Copy the update ISO image to the repository, specify the installation mode, and then install the image. The ISO image installation through CLI or REST APIs is more useful for software updates because the CIMC KVM or direct console support is not required to configure the system. After the installation is complete and the system reboots, the Cisco CSP 2100 system can be accessed through Secure Shell (SSH).

Note Ensure that network connectivity is not lost while installation is in progress. Network issues might result in installation getting stuck in one of the various stages. In such a scenario, reinstall the ISO image, which means re-attach the ISO image to the KVM console and reboot Cisco CSP.

Performing the Initial Setup

You can install the CSP software either by:

- Filling out the questionaire through manual install.
- Using PnP manager in NSO to load the Day-0 configuration file on CSP. This process is also known as zero touch provisioning.

Before you begin

- Make sure that the Cisco CSP is set up correctly and is cabled for network access. For information about setting up the Cisco CSP, see the *Cisco Cloud Services Platform Hardware Installation Guide*.
- Choose a hostname for your Cisco CSP.
- Obtain the following information about the Cisco CSP from your network administrator:
    - Port channel or physical network interface card (pNIC) to be used as the management interface
    - VLAN values for the management port channel, the management interface, and the dedicated service management interface (optional)
    - Two pNIC members for the port channel to be used as the management interface (optional)
    - Password for the admin user
    - Management IP address
    - Netmask for the management interface
    - Default gateway IP address
    - Domain name server (DNS) (optional)
    - Domain name
    - Port channel or pNIC to be used as the dedicated service management interface (optional)
    - Two pNIC members for the port channel to be used as the dedicated service management interface (optional)

To perform zero touch provisioning, ensure that the following components are available:

- Standard NSO (version 4.7) with PnP manager.
- DHCP server (Windows or Linux) with option 43 (vendor-specific information) configuration.
- CSP LOM Ports connected to upstream switch either as access port or in portchannel.

  CSP-2K series: LOM ports should be used for management.

  CSP-5K series: LOM/slot 1 (1G) ports should be used for management.

Procedure

Step 1 Turn on the Cisco CSP.

Step 2 Enter **admin** as the username and **admin** as the password.

You are prompted with whether CSP software installation should be carried out by the manual install or PnP manager modes.

Step 3 Enter yes or no depending on whether to exit PnP and continue with manual install or perform installation through zero touch provisioning. If you enter yes, continue from Step 4, else you are logged out of the CSP device. You can log in back with the box credentials mentioned in the Day-0 file. Meanwhile, the following action occurs for CSP software installation though PnP manager mode:

a) CSP communicates with DHCP server to get IP address and login credentials of the PnP server.
b) After PnP credentials are learnt by CSP, CSP contacts the PnP server.
c) The PnP server registers CSP as a claimed device.
d) The Day-0 configuration file stored in PnP is applied to CSP.
e) Run the following PnP configuration command for zero touch provisioning:

admin@ncs# show running-config pnp

```
pnp server ip-address 0.0.0.0 <--- Mandatory so that any csp host can contact
pnp server port 9191                    <--- Standard Port where pnp listens
pnp server use-ssl false                <---- Since http is supported now
pnp logging directory /var/log/ncs
pnp logging serial all
!
pnp map FCH1943V236                     <--- Serial Number of the device
serial FCH1943V236
device-name csp                         <--- You can give anything for name
username admin
password $8$s/i2wtF7my6NxsECnFlGXQhGCcWokl6kAr+q0KOWgnU=  <----- admin , this will be
encrypted and stored automatically
device-type netconf
port 2022
day0-template [ csp_163.xml ]           <--- Day0 config file under the /opt/cisco/nso
apply-config-upgrade true
mgmt-ip-address 10.193.75.163
commit-queue false
dev-snmp false
use-relative-url true
!
pnp cfg-location /opt/cisco/nso         <--- path for nso
```

Example:

The following example shows the prompts described for the zero touch provisioning procedure.

```
localhost login: admin
Password:


                ****************************************************************************************************
                **********************************************
                **********************************************
                ****                                      ****
                ****  Cisco Cloud Services Platform       ****
                ****         Version 2.5.0          ****
                ****         Built on 2019-10-08          ****
                ****  Cisco Systems Inc, copyright 2019   ****
                ****                                      ****
                **********************************************
                **********************************************
                **********************************************


Verifying server information ...

        System Information
        Manufacturer: Cisco Systems Inc
        Product Name: UCS-C220-M3S
        Version: A

PNIC Remote Connectivity Information from LLDP
==================================================
PNIC Eth1-0   : system = No lldp detectd      intf = No lldp detected         state = up

PNIC Eth1-0   : system = No lldp detectd      intf = No lldp detectd          state = up

PNIC Eth0-1   : system = lab142-Q15-n5k       intf = Ethernet101/1/32         state = up

PNIC Eth3-0   : system = lab142-Q15-n5k       intf = Ethernet102/1/32         state = up

PNIC Eth3-3   : system = lab142-Q15-n5k       intf = Ethernet101/1/31         state = up

PNIC Eth3-2   : system = lab142-Q15-n5k       intf = Ethernet102/1/31         state = up

PnP Status: Successfully applied day0 config
Do you want to exit Plug and Play (PnP) and continue manual install(yes or no)?no
```

Example:

A sample of the Day-0 file stored in PnP is:

```
config xmlns="http://tail-f.com/ns/config/1.0">
<resources xmlns="http://www.cisco.com/ns/test/resource">
  <resource>
    <resource_name>csp</resource_name>
    <ip_address>10.10.10.27</ip_address>
    <netmask>255.255.255.0</netmask>
    <default_gw>10.10.10.1</default_gw>
    <mgmt_mtu>1500</mgmt_mtu>
    <mgmt_pnic>MGMTPCH</mgmt_pnic>
    <mgmt_pnic_mode>shared</mgmt_pnic_mode>
    <mgmt_vlan>1</mgmt_vlan>
    <host_name>xyz000-csp-150</host_name>
    <dns_server>171.70.168.183</dns_server>
    <domain_name>cisco.com</domain_name>
  </resource>
  </resources>
```

```
</config>
```

Example:

A sample of the DHCP configuration file on Linux is:

```
subnet 10.193.72.0 netmask 255.255.248.0 {
 option subnet-mask 255.255.248.0;
 option domain-search "cisco.com";
 option domain-name-servers 171.70.168.183;
 option routers 10.193.72.1;
 range 10.193.75.165 10.193.75.166;
}
option vendor-encapsulated-options
"Ciscopnp:5A;K4;B2;I10.193.75.144;J9191;Nadmin;OSfish@123;Z171.68.38.65;6A"

K = Protocol [4: HTTP]                    <--- ONLY HTTP is Supported
B = Address Type [1-FQDN, 2-IPV4]         <--- NO IPV6 Support.
I = Remote [ServerIp]
J = Remote Server Port
N = Username
O = Password
Z = NTP server address
```

Step 4 Enter yes or no depending upon whether you want to use a port channel for the management interface. Configuring a port channel as the management interface ensures that you always have connectivity with the Cisco CSP. You can connect to Cisco CSP even when one of the pNICs is down. Do one of the following:

- To use a port channel as the management interface, enter **yes** and go to Step 4.
- To use a pNIC as the management interface, enter **no** and go to Step 5.

Step 5 Do the following to use a port channel as the management interface:

a) Enter a name for the port channel.
b) Enter the name of the first pNIC.
c) Enter the name of the second pNIC.

Note Both specified pNICs should be of same speed.

d) Enter the bond-mode. Valid values are balance-slb, active-backup, and balance-tcp.
e) Enter the value for the link aggregation control protocol (LACP) for the bond. Valid values are active, passive, and off.
f) Enter a VLAN value for the port channel. Valid range is from 1 to 4094.

Step 6 Enter the pNIC interface number that you want to use as the management interface.

Step 7 Enter yes or no to specify the shared or dedicated mode for the management interface. Do one of the following:

- To share the management interface with service VMs, enter **yes**. The management interface pNIC carries the management traffic of Cisco CSP and the management and data traffic of any service using this pNIC.
- To not share the management interface with service VMs, enter **no**. The management interface pNIC carries only the management traffic of Cisco CSP.

Step 8 Enter yes or no depending upon whether you want to specify a VLAN for the management interface. Do one of the following:

- To specify a VLAN for the management interface, enter **yes** and then enter a VLAN value. Valid range is from 1 to 4094.

- To skip specifying a VLAN for the management interface, enter **no**. The VLAN for the management interface is set to 1 by default.

Step 9 Enter **yes** to save the settings.

Step 10 Enter a new password for the **admin** user and then enter the password again for verification.

Step 11 Enter the hostname.

Step 12 Enter the IP address of the management interface.

Step 13 Enter the netmask of the management interface.

Step 14 Enter the IP address of the default gateway.

Step 15 Enter yes or no depending upon whether you want to specify the DNS. Do one of the following:

- To specify a DNS, enter **yes** and enter the IP address of the DNS.
- To skip specifying a DNS, enter **no**.

Step 16 Enter the domain name; for example, `cisco.com`.

Step 17 Enter **yes** to save the settings.

Step 18 Enter yes or no to configure the dedicated service management interface. Do one of the following:

- To configure a port channel as the dedicated service management interface, enter **yes** and go to Step 18.
- To configure a pNIC as the dedicated service management interface, enter **no** and go to Step 19.

Step 19 Do the following to configure a port channel as the dedicated service management interface:

a) Enter a name for the port channel.
b) Enter the name of the first pNIC.
c) Enter the name of the second pNIC.

Note Both specified pNICs should be of same speed.

d) Enter the bond-mode. Valid values are balance-slb, active-backup, and balance-tcp.
e) Enter the value for the link aggregation control protocol (LACP) for the bond. Valid values are active, passive, and off.
f) Enter a VLAN value for the dedicated service management port channel. Valid range is from 1 to 4094.

Step 20 Enter the pNIC interface number that you want to use as the dedicated service management interface.

Step 21 Enter **yes** to save the settings.

Your specified settings are saved and you are connected to the Cisco CSP console.

Note The **config terminal** command fails when you run it after performing the initial setup for a new installation. This happens because the admin user is not assigned to a group at the initial login. To run this command and configure Cisco CSP features, you must log out and then log in to the Cisco CSP.

The following example shows the prompts described for the manual installation procedure.

```
localhost login: admin
Password:
```

```
                **********************************************
                **********************************************
                **********************************************
                ****                                      ****
                ****  Cisco Cloud Services Platform       ****
                ****         Version 2.5.0                ****
                ****         Built on 2018-10-8          ****
                ****  Cisco Systems Inc, copyright 2019   ****
                ****                                      ****
                **********************************************
                **********************************************
                **********************************************


Verifying server information ...

        System Information
        Manufacturer: Cisco Systems Inc
        Product Name: CSP
        Version: 2.5.0

PNIC Remote Connectivity Information from LLDP
==================================================
PNIC Eth1-0   : system = No lldp detectd      intf = No lldp detected         state = down

PNIC Eth1-1   : system = sw-lab-n5k-3         intf = Ethernet100/1/46         state = up

PNIC Eth7-0   : system = sw-lab-n5k-3         intf = Ethernet100/1/48         state = up

PNIC Eth7-1   : system = No lldp detectd      intf = No lldp detected         state = down

PNIC Eth4-0   : system = sw-lab-n5k-3         intf = Ethernet100/1/45         state = up

PNIC Eth4-1   : system = sw-lab-n5k-3         intf = Ethernet100/1/47         state = up

PNIC Eth4-2   : system = No lldp detectd      intf = No lldp detected         state = down

PNIC Eth4-3   : system = No lldp detectd      intf = No lldp detected         state = down

Enable port channel for mgmt pnic (yes or no): no

Choose a PNIC for the management interface: Eth1-0, Eth1-1, Eth7-0, Eth7-1, Eth4-0, Eth4-1,
 Eth4-2, Eth4-3:
Eth4-0
Allow management interface to be shared with service VMs (yes or no)?: yes

        Shared Management Interface Physical NIC        : Eth4-0

Define a vlan for the mgmt interface(yes or no)?: yes
Choose a vlan for the management interface, valid values are between 1 and 4094: 180

       Management vlan set to        : 180

Do you want to save these settings (yes or no)?: yes

Please enter a password for the CSP admin user
The password must:
have at least 8 characters and at most 64 characters
have at least 1 digits
have at least 1 special character[allowed _-~#@=+^]
have at least 1 upper case character
have at least 1 lower case character
not have two or more same characters consecutively
not be an exact dictionary word match
```

```
Password:
Enter it again for verification:
Password:

Enter your hostname: csp1
Enter your management IP address: 1.2.3.4
Enter your netmask: 255.255.255.0
Enter your default gateway: 1.2.3.1
Do you want to configure a Domain Name Server (DNS) (yes or no)?: yes
Enter your Domain Name Server (DNS): 5.6.7.8
Enter your domain name: cisco.com

        System Hostname                 : csp1
        Management IP Address           : 1.2.3.4
        Management Netmask              : 255.255.255.0
        Management Gateway              : 1.2.3.1
        Domain Name Server (DNS)        : 5.6.7.8
        Domain Name                     : cisco.com

Do you want to save these settings (yes or no)?: yes

Saving configuration...........

Do you wish to configure s Dedicated Service Management Port (yes or no)?: yes
Do you want to set the service mgmt port up as port channel (yes or no)?: yes
Port channel name: SRV-MGMT
Choose the first PNIC for the service mgmt port channel: Eth1-0, Eth1-1, Eth7-0, Eth7-1,
Eth4-0, Eth4-1, Eth4-2,Eth4-3: Eth1-0

        Service Mgmt Pnic member 1 set to        : Eth1-0

Choose the second PNIC for the service mgmt port channel: Eth1-0, Eth1-1, Eth7-0, Eth7-1,
Eth4-0, Eth4-1, Eth4-2, Eth4-3: Eth1-0

        Service Mgmt Pnic member 2 set to        : Eth1-0

Choose bond-mode for service mgmt port-channel(balance-slb or active-backup or balance-tcp)?:
 balance-slb
Choose lacp-type for service mgmt port-channel (active or passive or off)?: active
Choose vlan trunk for service mgmt port-channel: 72

        Service Mgmt Port Channel: SRV-MGMT
        Service Mgmt Member 1    : Eth1-0
        Service Mgmt Member 2    : Eth1-1
        Service Mgmt Bond Mode   : balance-slb
        Service Mgmt LACP type   : active
        Service Mgmt VLAN Trunk  : 72

Do you want to save these settings (yes or no)?: yes
CSP expects HyperThreading to be disabled in BIOS
No Cavium card in the system
No Cavium card in the system
Welcome to the Cisco Cloud Services Platform CLI

TAC support: http://www.cisco.com/tac
Copyright (c) 2018-2019, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
```

```
admin connected from 127.0.0.1 using console on csp1
csp1#
```

Logging In to the Cisco CSP

You can log in to the Cisco CSP by using one of the following modes: web interface (accessible through a web browser), CLI, or REST APIs (accessible through cURL tool or Windows PowerShell). However, before logging in to the web interface or using the REST APIs, you must install an SSL certificate using the CLI. For detailed information about the CLI and available commands, see the *Cisco Cloud Services Platform Command Reference Guide*.

Generating and Installing an SSL Certificate

Note For proof-of-concept (POC) or lab deployments, an SSL certificate is not required. You can skip this section and go to Accessing the Cisco CSP Web Interface, on page 10.

You must generate a Certificate Signing Request (CSR) to send to a Certification Authority (CA) to obtain an SSL certificate and use the CLI to install the SSL certificate on Cisco CSP. The default self-signed certificate installed on the Cisco CSP is only for temporary use.

Procedure

Step 1 Log in to the Cisco CSP 2100 CLI in EXEC mode.

Step 2 On the command prompt, use the following command to create a CSR:

```
csp# certificate request sha sha256 keysize 2048
```

After you enter the command, you are prompted for some information such as country name, state, city, email, common name, and so on. For detailed information about this command, see the *Cisco Cloud Services Platform Command Reference Guide* .

Note The common name is the DNS name of the host, including the domain name; for example, *myserver.mycompany.com*.

Step 3 Provide the required information in the prompt.

After you provide the required information, the following two files are generated in the `/osp/certificates` directory:

- `myhost.csr`—The server certificate request file
- `myPrivate.key`—The server key file

Note To enable the Cisco CSP to start without entering a password, the `myPrivate.key` file is not protected with a passphrase. However, you can use a passphrase to protect it. When the `myPrivate.key` file is protected with a passphrase, the administrator must enter the password every time the Cisco CSP starts.

Step 4 Send the `myhost.csr` file to a CA to obtain an SSL certificate.

After you submit the CSR to a CA, the CA generates an SSL certificate and sends a certificate file to you. The CA may also send a certificate chain file.

Step 5 Copy the SSL certificate files that you received from the CA to the `/osp/certificates` directory using the **scp** command from an external server.

Step 6 On the Cisco CSP 2100 command prompt, enter the following command to install the certificate:

```
csp# certificate install-certificate
```

After you enter the command, you are prompted for some information such as localhost (hostname including the domain name), key filename, certificate filename, and chain filename. For detailed information about this command, see the *Cisco Cloud Services Platform Command Reference Guide*.

Step 7 Provide the required information in the prompt.

After you provide the required information, the SSL certificate is installed.

To verify that the certificate is installed, follow the instructions in the next section to log in to the Cisco CSP web interface by using a web browser. After logging in, click the lock icon in the address bar to see information about the installed certificate.

Accessing the Cisco CSP Web Interface

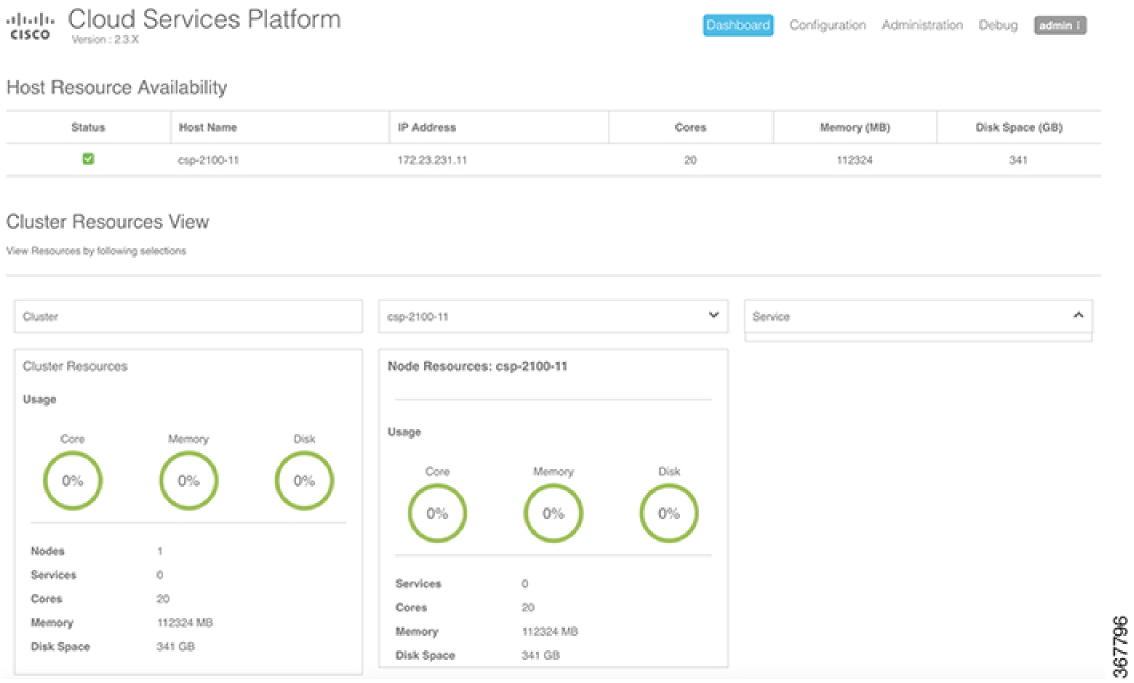
Procedure

Step 1 Enter **https://***hostname* or **https://***ip-address* in a web browser.

Note The hostname should resolve to the IP address that you entered as the management IP address in Performing the Initial Setup, on page 2. The hostname should also match the hostname specified in Generating and Installing an SSL Certificate, on page 9.

Step 2 Enter the username **admin** and the password.

The Cisco CSP web interface is displayed.



Host Resource Availability

Status	Host Name	IP Address	Cores	Memory (MB)	Disk Space (GB)
☑	csp-2100-11	172.23.231.11	20	112324	341

Cluster Resources View

View Resources by following selections

Cluster | csp-2100-11 | Service

Cluster Resources

Usage

Core 0% Memory 0% Disk 0%

Nodes	1
Services	0
Cores	20
Memory	112324 MB
Disk Space	341 GB

Node Resources: csp-2100-11

Usage

Core 0% Memory 0% Disk 0%

Services	0
Cores	20
Memory	112324 MB
Disk Space	341 GB

Overview of the Cisco CSP Web Interface

The Cisco CSP web interface consists of the following tabs and pages:

- **Dashboard**: The **Dashboard** tab consists of the following pages:
  - **Overview**: Use the **Overview** page to view information about the host resources. You can filter resources by clusters, nodes, and services. You can also veiw the node level redundancy in a cluster.
  - **Services View**: Use the **Services View** page to view information about the services traffic rate.
  - **Network View**: Use the **Network View** page to view information about statistics for a VNIC.
  - **PNIC** : Use the **PNIC Statistic** page to view information about statistics for a pNIC.
  - **VNIC** : Use the **VNIC** page to view information about statistics for a VNIC Rx statistics.
  - **Resource Utilization**: Use the **Resource Utilization** page to view statistical information about memory, disk, and CPU for a specific duration. You can choose a specific duration and get memory, disk, and CPU statistics for that time interval.
  - **Cluster Redundancy**: Use the **Cluster Redundancy** page to view the cluster migration report.
- **Configuration**: The **Configuration** page consists of the following pages:
  - **Repository**: Use the **Repository** page to upload or remove an image and to view all available images.

    - **Services**: Use the **Services** page to create a new service or configure existing services, change the power mode of a service, and export a service. You can create a new service using a template or save a service as a template.
    - **Service Template**: Use the **Services Templates** page to view all available service templates and delete a service template.
    - **pNICs**: Use the **pNICs** page to view information about pNICs and port channels and to configure or unconfigure a pNIC as the management interface.
    - **Port Channel**: Use the **Port Channel** page to create a port channel, delete or edit a port channel, and to configure or unconfigure a port channel as the management interface.
    - **SRIOV**: Use the **SRIOV** page to enable, disable, configure, or unconfigure an SR-IOV interface.
    - **System Settings**: Use the **System Settings** page to enable or disable CPU pinning.

- **Administration**: The **Administration** page consists of the following pages:
    - **Password**: Use the **Password** page to change the password for the **admin** user.
    - **Host**: Use the **Host** page to configure the host. You can configure the hostname, host domain name, DNS server, host IP, gateway IP, management MTU, management pNIC mode, and session idle timeout.
    - **NTP Server**: Use the **NTP Server** page to configure an NTP server.
    - **VNF Group**: Use the **VNF Group** page to configure a VNF group name of a service.
    - **User**: Use the **User** page to create, modify, or delete a local user.
    - **Cluster**: Use the **Cluster** page to create, configure, and delete clusters.
    - **NFS**: Use the **NFS** page to create and configure NFS storage.
    - **SNMP**: Use the **SNMP** page to create and configure SNMP agent, communities, users, groups, and traps.
    - **AAA**: Use the **AAA** page to specify the AAA authentication mode and to create, modify, or delete a TACACS+ or RADIUS server.
    - **IP Receive ACL**: Use the **IP Receive ACL** page to configure the Access Control List (ACL) access for the management interface. You can specify the source network IP address, service type, priority, and action for the packets received from the specified source network.
    - **Syslog**: Use the **Syslog** page to configure multiple syslog servers. You can send internal log messages to multiple remote syslog server on TCP and UDP ports, or only on UDP port.

Uploading Service Images Using the Cisco CSP Web Interface

Before you begin

Be sure to download the service image to your local machine or a location on your local network that is accessible to your Cisco CSP.

Procedure

Step 1 Click the **Configuration** tab and then choose **Repository**.

Step 2 On the **Repository Files** page, click the add button (+).

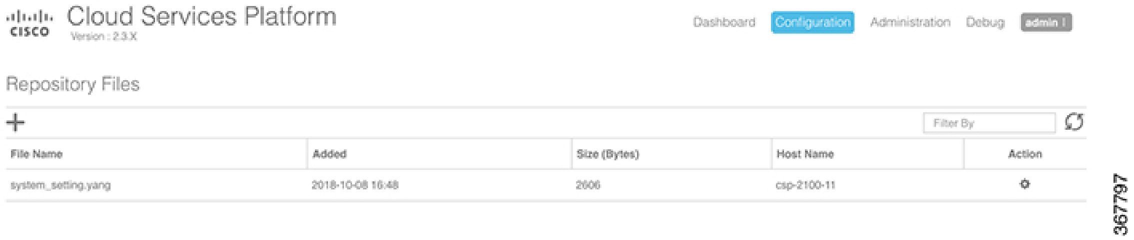
Step 3 Click **Browse**.

Step 4 Navigate to the service image, select a service image, and click **Open**.

Step 5 Click **Upload**.

After the service image is uploaded, the image name and other relevant information are displayed in the Repository Files table.

Tip You can also use this procedure to upload the banner files and the configuration files to the repository.



Repository Files

File Name	Added	Size (Bytes)	Host Name	Action
system_setting.yang	2018-10-08 16:48	2606	csp-2100-11	⚙

Creating a Service Instance

Procedure

Step 1 Click the **Configuration** tab and then choose **Services**.

Step 2 On the **Service** page, click the add (+) button.

The **Create Service** page is displayed.

Step 3 In the **Name** field, enter a name for the service.

Step 4 From the **Target Host Name** drop-down list, choose the target host.

Step 5 (Optional) In the **VNF Management IP** field, enter the VNF management IP address to be used in the service.

Note The VNF Management IP value entered in this field does not get configured in the service. This field serves only as a reference to the VNF management IP address mapped to a service.

Step 6 From the **Image Name** drop-down list, choose an image file for the service.

You can use an ISO or OVA, or a QCOW software image file to create the service.

Note With Cisco VSM and Cisco VSG services, only ISO image files are supported.

Depending on the type of image selected, additional fields are displayed. If your service requires additional information, as is the case with Cisco VSM and Cisco VSG services, you must enter this information in the **Additional Image Questionnaires** section. For details about the additional information that your service requires, see the documentation for that service.

Step 7 (Optional) Click **Day Zero Config** and in the **Day Zero Config** dialog box, do the following:

a) From the **Source File Name** drop-down list, select a day0 configuration text or ISO file.
b) In the **Destination File Name** field, specify the name of the day0 destination text or ISO file.

Step 8 (Optional) In the **Number of Cores** field, specify the number of cores. Make sure that the new value does not exceed the available resources.

Step 9 (Optional) If you want to resize the disk, check the **Do you want to resize disk?** check box.

This option is available only when a QCOW2 image is selected in the **Image Name** field.

Step 10 (Optional) In the **Disk Space (GB)** field, specify the disk space. Make sure that the new value does not exceed the available resources.

This field is not editable when a QCOW2 image is selected in the **Image Name** field and the **Do you want to resize disk?** check box is unchecked.

Step 11 (Optional) In the **RAM (MB)** field, specify the RAM. Make sure that the new value does not exceed the available resources.

Step 12 (Optional) If you want to deploy the service on an NFS storage, select the **NFS Storage** check box and then select an NFS storage from the **NFS** drop-down list.

Step 13 (Optional) In the **Disk Type** field, specify the disk type. Valid choices are IDE or VIRTIO.

Step 14 Click **VNIC** and in the **VNIC Configuration** dialog box, do the following:

a) In the **Interface Type** field, specify the type. Valid choices are Access, Trunk, and Passthrough.

Depending on the selected interface type, the fields of **VNIC Configuration** dialog box are displayed. The following table describes these fields based on the interface type.

Field	Interface Type	Description
VLAN	• Access • Trunk • Passthrough (only for SR-IOV and MACVTAP passthrough modes)	In the **VLAN** field, enter the VLAN ID. Valid range is from 1 to 1000 and from 1025 to 4094.
Native VLAN	Trunk	In the **Native VLAN** field, specify the VLAN ID. Valid range is from 1 to 1000 and from 1025 to 4094.
Model	• Access • Trunk • Passthrough (only for MACVTAP passthrough modes)	In the **Model** field, specify the model number of the vNIC driver. Valid choices are Virtio (for the KVM driver) and e1000 (for the Intel Ethernet driver).

Field	Interface Type	Description
Service Management Interface	• Access • Trunk • Passthrough	If you want to use the dedicated service management interface with this service, select the **Service Management Interface** check box. **Note** This check box is displayed only if a pNIC or a port channel has already been configured as the dedicated service management interface. When you select this check box, the **Network Name** field is automatically populated with the name of the configured dedicated service management interface and you do not need to specify the network name.
Network Type	• Access • Trunk	In the **Network Type** field, specify the network type. Valid choices are Internal and External. Create an internal network when you need to connect one service to another service and there is no connection to a physical network interface card (pNIC). Create an external network when you want to connect to a pNIC directly (passthrough) or through a switch.
Network Name	• Access • Trunk • Passthrough	In the **Network Name** field, specify the name of the network. To create an internal network, enter a name for the internal network in the **Network Name** field. To create an external network or to specify the network name for the passthrough mode , choose a network interface from the **Network Name** drop-down list.
Passthrough Mode	Passthrough	In the **Passthrough Mode** field, specify the passthrough mode. Valid choices are SR-IOV, PCIE, and MACVTAP.

b) When you are done with the vNIC configuration, click **Submit**.

To add more vNICs, click **VNIC** and repeat all tasks described in this step.

Step 15 (Optional) Click **Storage** and in the **Storage Configuration** dialog box, do the following:

a) In the **Device Type** field, select a storage type. Valid choices are **Disk** and **CDROM**.

Depending on the selected storage type, the fields of **Storage Configuration** dialog box are displayed. The following table describes these fields based on the storage type.

Storage Type	Field	Description
Disk	**Location**	In the **Location** field, select a location. You can select a local or remote location. A remote location is displayed only if you have already configured an NFS storage.
Disk	**Disk Type**	In the **Disk Type** field, specify the disk type. Valid choices are IDE and VIRTIO.
Disk	**Format**	In the **Format** field, specify the disk format. Valid choices are RAW and QCOW2.
Disk	**Do you want mount Image file as disk?**	Check the **Do you want mount Image file as disk?** check box to use a local or NFS-mounted ISO, RAW, or QCOW2 image file as the additional storage disk for a service.
Disk, CDROM	**Disk Image**	In the **Disk Image** field, select an ISO image file for **CDROM** device type or select a RAW or QCOW2 image file for **Disk** device type.
Disk, CDROM	**Size (GB)**	In the **Size (GB)** field, enter the disk size.

b) When you are done with the storage configuration, click **Submit**.

To add more storage, click **Storage** and repeat all tasks described this step.

Step 16 (Optional) In the **VNC Port** field, enter a VNC port for the service. Valid range is from 8721 to 8784.

Step 17 (Optional) In the **VNC Password** field, enter a password and then enter the same password in the **Confirm VNC Password** field.

Caution We strongly advise that you secure your remote access with a complex alphanumeric password for VNC.

Note The VNC console password is in clear text which might be indicated as a security issue. To ensure that the VNC console access is secure in Cisco CSP, the VNC console is accessible only through the web interface which is protected by a user name and a password.

Step 18 Click **Serial Port** and in the **Serial Port** dialog box, do the following:

a) In the **Type** field, specify the port type. Valid choices are **Telnet** and **Console**.
b) If you have selected Telnet type in Step a, then in the **Service Port Number** field, enter a value. Valid range is from 7000 to 8700.
c) When you are done with the serial port configuration, click **Submit**.

To add more serial ports, click **Serial Port** and repeat all tasks described in this step.

Step 19 (Optional) If you are configuring the services in redundancy, select the **HA Service Configuration** check box. The Cisco CSPs must be in the cluster mode. Do the following:

a) In the **Name** field, enter the name of the secondary service.
b) From the **HA Host Name** drop-down list, choose a Cisco CSP remote peer that is a part of the cluster.
c) In the **VNF Management IP** field, enter the VNF management IP address for the secondary service.

d) In the **VNC Port** field, enter a VNC port for the secondary service. Valid range is from 8721 to 8784.

e) Click **Secondary VNIC** to add a secondary VNIC.

The VNIC Configuration dialog box is displayed. For information about the fields of this dialog box, see Step 14.

All other parameters that need to be a configured in the secondary service are inherited from the already-configured primary service.

Step 20 Click **Deploy**.

The Service Test Creation dialog box is displayed indicating that the service is available.

Verifying Your Service Instance

Make sure that your service instance is up and running.

Procedure

Step 1 Click the **Configuration** tab and then choose **Services**.

The **Service** table shows the current status of services.

Step 2 Find your service instance in the **Service Name** column, and check that the state is deployed and the power status is on.

Configuring Multiple Syslog Servers

Ensure that CSP service instance is up and running.

Procedure

Step 1 Click the **Administration** tab, and then select **Syslog**.

Step 2 On the **Syslog** page, you can perform either of the following:

a) Select **UDP Only** if you are sending internal log messages only through the UDP port.

b) Clear **UDP Only** if you are sending internal log messages through both UDP and TCP transport ports.

Step 3 If you select UDP as the mechanism to send log messages, in the **UDP Port** field, specify the UDP port values of the remote syslog server.

Step 4 If you do not select UDP as the mechanism to send log messages, specify both TCP and UDP port values of the remote syslog server.

Step 5 To add a remote syslog server, click the + button.

Step 6 In the **Host** field, specify the IPv4 IP address or host name of the remote syslog server, and then click **Add**. The newly added host is displayed in a table.

Step 7 To add multiple syslog servers, repeat step 5 through step 6.

You can add up to eight syslog servers.

Node Failure Detection and Migration of VNFs to Alive Node

With node level redundancy in a cluster, if a node in a CSP cluster goes down, you can detect the node failure and then automatically deploy all the VNFs in the failed node to the other live nodes in a cluster.

Procedure

Step 1 To detect a node failure, click **Dashboard** > **Overview**

Under Cluster resources section, you can view the status of each of the nodes.

Step 2 To deploy all VNFs in the failed node to other live nodes, click **Administration** > **Cluster**.

Step 3 In the CSP Cluster page, to add a cliuster member, click the add (+) button.

Step 4 In the Add Cluster Member page, provide the values for number of nodes, cluster node 1 name or IP.

Step 5 Under the Advance Setting section, to enable node level redundancy for the new cluster, check **Enable Node Redundancy**.

To enable node redundancy for an existing cluster, check **Enable Node Redundancy** for a node name or IP.

Step 6 Set **Eviction Timeout** in seconds.

By setting the timeout, the eviction of VMs on the down node does not begin until the timeout expires.

Note The VMs are not deployed on a node that has a VM High Availability pair.

Step 7 To view the migration of deploying VNFs in a failed node to a live node, click **Dashboard** > **Cluster Redundancy** > **Migration Report**.

Ensure that there are a mimimum of three nodes in a cluster to enable the node level redundancy functionality.

Step 8 During upgrade, delete the cluster, and recreate it when all nodes are upgraded.

For VMs in HA mode, you must configure ha-key to include two VMs in HA.

What to do next

If a node in a cluster is down, and cluster settings are edited, the affected node cannot synchronize with the latest cluster settings. To avoid this issue, edit cluster settings only when all nodes in a cluster are up and working. If a node is down, delete that node from the cluster. All nodes in a cluster should have same settings for cpu-pinning and ovs-dpdk. For detailed information about these commands, see the *Cisco Cloud Services Platform Command Reference Guide*.

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 of this document are considered uncontrolled. See the current online version for the latest version.

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com go trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)