Cisco Cloud Services Platform 2100 Quick Start Guide, Release 2.1.0

First Published: 2016-08-17

Last Modified: 2017-08-03

Setting Up Your Cisco CSP 2100 and Configuring Services

Summary Steps

Setting up your Cisco Cloud Services Platform 2100 (Cisco CSP 2100) and creating services consists of the following high-level steps:

Step 1 Upgrade the Cisco CSP 2100 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 the Cisco CSP 2100 through the web interface.

Step 5 Upload the service image to the Cisco CSP 2100.

Step 6 Create a service.
You must define the host, image, network type, and any additional information required by the service. Optionally, you can define high availability, the VLAN configuration, vNIC drivers, and default resources.

Step 7 Verify the service instance.

Upgrading the Cisco CSP 2100 Software

You can upgrade the Cisco CSP 2100 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 2100 system is required to perform the tasks described in Performing the Initial Setup, on page 2.
- Using the Cisco CSP 2100 CLI: Copy the update ISO image to the repository, specify the installation mode, and then install the image. The ISO image installation through CLI 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).

Upgrading the Cisco CSP 2100 Software Using CLI

To upgrade the Cisco CSP 2100 software using CLI, do the following:

Step 1 Copy the update ISO image to the repository by running the **copy image** *source_filename destination_filename* command.

Step 2 Specify the installation mode by running the **system install iso mode** {**clean-install** | **software-update**} command. By default, the installation mode is set to **software-update** and existing configurations and settings are retained in the new installation. If you do not want to retain the existing configurations and settings, you can change the installation mode to **clean-install**.

Note Only clean installation is supported in Release 2.1.0. Upgrade from Cisco CSP 2100 Release 1.0 and 2.0.0 to Release 2.1.0 is not supported.

Step 3 Initiate the installation by running the **system install iso update image** *imagename.iso* command.

Performing the Initial Setup

Before You Begin

- Make sure that the Cisco CSP 2100 is set up correctly and is cabled for network access. For information about setting up the Cisco CSP 2100, see the *Cisco Cloud Services Platform 2100 Hardware Installation Guide*.
- Choose a hostname for your Cisco CSP 2100.
- Obtain the following information about the Cisco CSP 2100 from your network administrator:
  - Physical network interface card (pNIC) number to be used as the management interface
  - Management IP address (appears as the mgmt0 interface on the platform)
  - Netmask for the management interface
  - Default gateway IP address
  - Domain name server (DNS) (optional)
  - Domain name

- Password for the admin user

Step 1 Turn on the Cisco CSP 2100.

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

Step 3 Enter the pNIC interface number that you want to use for the management interface. The Linux naming convention designates the four 1-GB Ethernet ports as enp4s0f0, enp4s0f1, enp4s0f2, and enp4s0f3 and the two 10-GB Ethernet ports as enp7s0f0 and enp7s0f1. In addition, there are two 1-GB onboard Ethernet interfaces named enp1s0f0 and enp1s0f1.

Note We recommend that you choose one of the 1-GB Ethernet ports as the management interface, so that you can use the higher bandwidth interface for services.

Step 4 Enter yes or no to specify the shared or dedicated mode for the management pNIC:

- If you want to share the management pNIC with service VMs, enter **yes**. The pNIC carries the traffic for the management port and any service using this pNIC.
- If you do not want to share the management with service VMs, enter **no**. The pNIC carries the traffic only for the management port.

Step 5 Enter **yes** to save the settings.

Step 6 Enter a password for the admin user and then enter the password again for verification.

Step 7 Enter the hostname.

Step 8 Enter the IP address of the management interface.

Step 9 Enter the netmask of the management interface.

Step 10 Enter the IP address of the default gateway.

Step 11 For the DNS, do one of the following:

- If you do not have a DNS, enter **no** and proceed to the next step.
- If you have a DNS, enter **yes** and enter the IP address of the DNS.

Step 12 Enter the domain name; for example, cisco.com.

Step 13 Enter **yes** to save the settings.

Your specified settings are saved and you are connected to the Cisco CSP 2100 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 2100 features, you must log out and then log in to the Cisco CSP 2100.

The following example shows the prompts described in this procedure.

```
localhost login: admin
Password:

                    ***********************************************
                    ***********************************************
                    ***********************************************
                    ****                                       ****
```

```
                ****  Cisco Cloud Services Platform 2100  ****
                ****         Version 2.1.0             ****
                ****         Built on 2016-08-04          ****
                ****  Cisco Systems Inc, copyright 2016   ****
                ****                                      ****
                **********************************************
                **********************************************
                **********************************************


Verifying server information ...

        System Information
        Manufacturer: Cisco Systems Inc
        Product Name: CSP-2100
        Version: 2.1.0

PNIC Remote Connectivity Information from LLDP
==================================================
PNIC enp8s0     : system = No lldp detectd      intf = No lldp detected         state =
down

PNIC enp1s0f1   : system = sw-lab-n5k-3         intf = Ethernet100/1/46         state = up

PNIC enp1s0f0   : system = sw-lab-n5k-3         intf = Ethernet100/1/48         state = up

PNIC enp9s0     : system = No lldp detectd      intf = No lldp detected         state =
down

PNIC enp130s0f0 : system = sw-lab-n5k-3         intf = Ethernet100/1/45         state = up

PNIC enp130s0f1 : system = sw-lab-n5k-3         intf = Ethernet100/1/47         state = up

PNIC enp130s0f2 : system = No lldp detectd      intf = No lldp detected         state =
down

PNIC enp130s0f3 : system = No lldp detectd      intf = No lldp detected         state =
down


Choose a PNIC for the management interface: enp8s0, enp1s0f1, enp1s0f0, enp9s0, enp130s0f0,
 enp130s0f1, enp130s0f2, enp130s0f3 : enp130s0f0
Allow management interface to be shared with service VMs (yes or no)?: y

        Shared Management Interface Physical NIC        : enp130s0f0

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

Please enter a password for the CSP-2100 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:

Broadcast message from root@localhost.localdomain (ttyS0) (Tue Aug  9 14:58:19 2016):

*** admin password has just been changed ***
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)?: y
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)?: y

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

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) 2015-2016, 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 2100

You can log in to the Cisco CSP 2100 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 2100 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 2100 Web Interface, on page 6.

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 2100. The default self-signed certificate installed on the Cisco CSP 2100 is only for temporary use.

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 2100 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 2100 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 2100 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 2100 Command Reference Guide*.

Step 7 Provide the required information in the prompt.
After you provide the required information, the SSL certificate is installed.

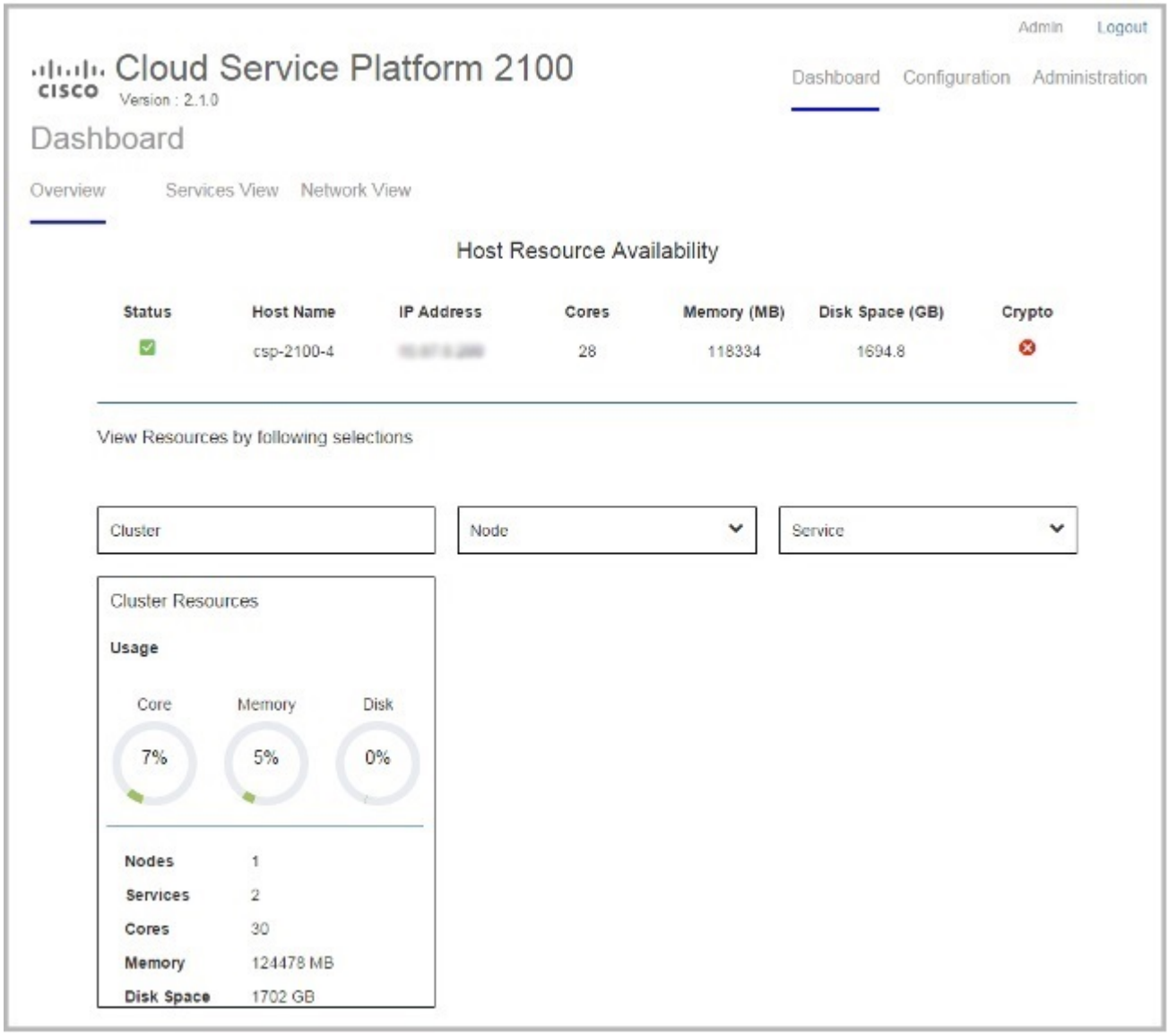
To verify that the certificate is installed, follow the instructions in the next section to log in to the Cisco CSP 2100 web interface using a web browser. After logging in, click the lock icon in the address bar to see information about the installed certificate.

Accessing the Cisco CSP 2100 Web Interface

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 Step 5 of Performing the Initial Setup, on page 2. The hostname should also match the hostname specified in Step 2 of Generating and Installing an SSL Certificate, on page 5.

Step 2 Enter the username **admin** and the password.
The Cisco CSP 2100 web interface is displayed.



Overview of the Cisco CSP 2100 Web Interface

The Cisco CSP 2100 web interface consists of the following tabs and pages:

- **Dashboard**: The **Dashboard** page consists of the following tabs and pages:
  - **Overview**: Use the **Overview** page to view information about the host resources. You can filter resources by clusters, nodes, and services.
  - **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 pNIC statistics for host members.

- **Configuration**: The **Configuration** page consists of the following tabs and pages:
  - **Services**: Use the **Services** page to create or configure services, change the power mode of a service, and export a service. You can create a new service using a template, save a service as a template, and delete a template by using the **Service Creation** page.
  - **pNICs**: Use the **pNICs** page to configure pNICs, enable and select an SR-IOV interface. You can also configure a port channel or a passthrough as a network interface.
  - **Cluster**: Use the **Cluster** page to create and configure clusters.
  - **Repository**: Use the **Repository** page to upload or remove an image and to view all available images.
  - **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.

- **Administration**: The **Administration** page consists of the following tabs and pages:
  - **Password**: Use the **Password** page to change the password for the admin user.
  - **Host Config**: Use the **Host Config** page to configure the host, the NTP server, the management interface, or the session idle timeout.
  - **User Config**: Use the **User Config** page to create, modify, or delete a user.
  - **TACACS**: Use the **TACACS** page to create, modify, or delete a TACACS+ server.

Uploading Service Images Using the Cisco CSP 2100 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 2100.

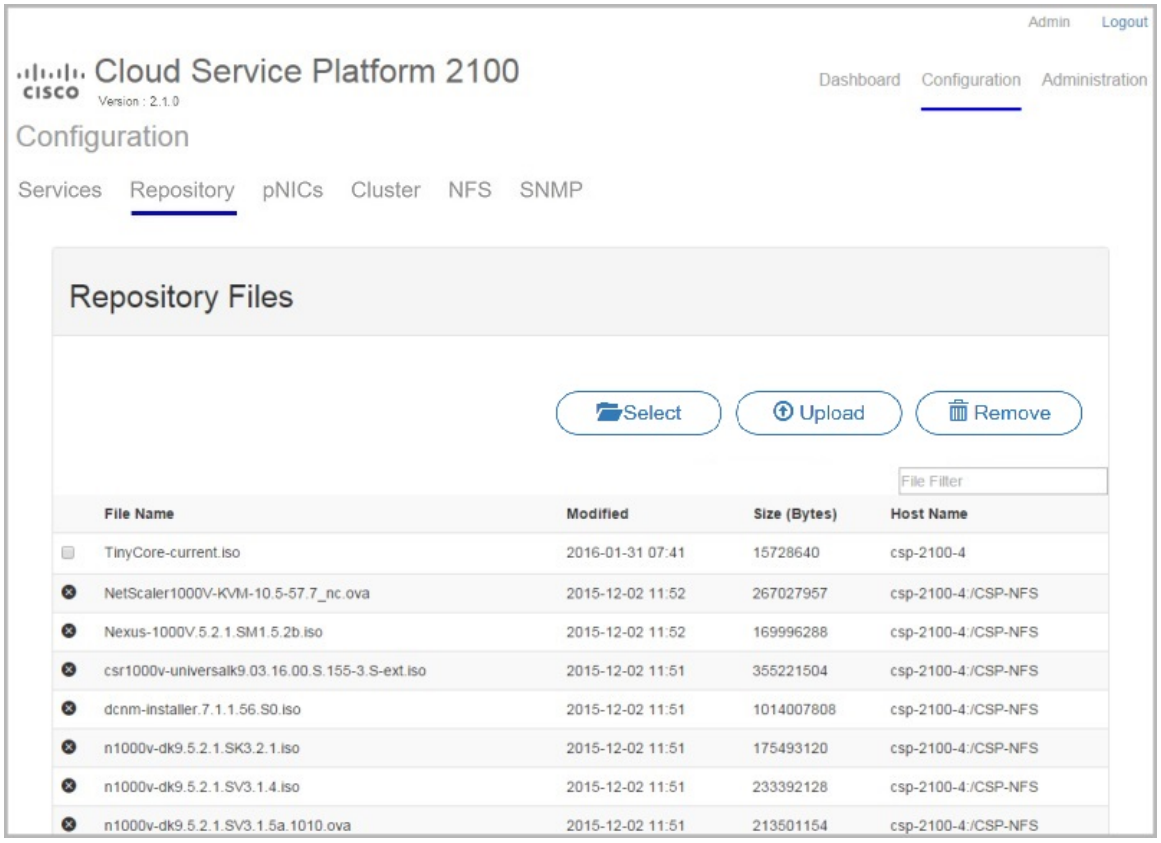
Step 1 Click the **Configuration** tab and then click the **Repository** tab.

Step 2 On the **Repository Files** page, click **Select**.

Step 3 Navigate to the service image, select a service image, and click **Open**.

Step 4 Click **Upload**.
After the service image is uploaded, the image name and other relevant information are displayed in the Repository Files table.

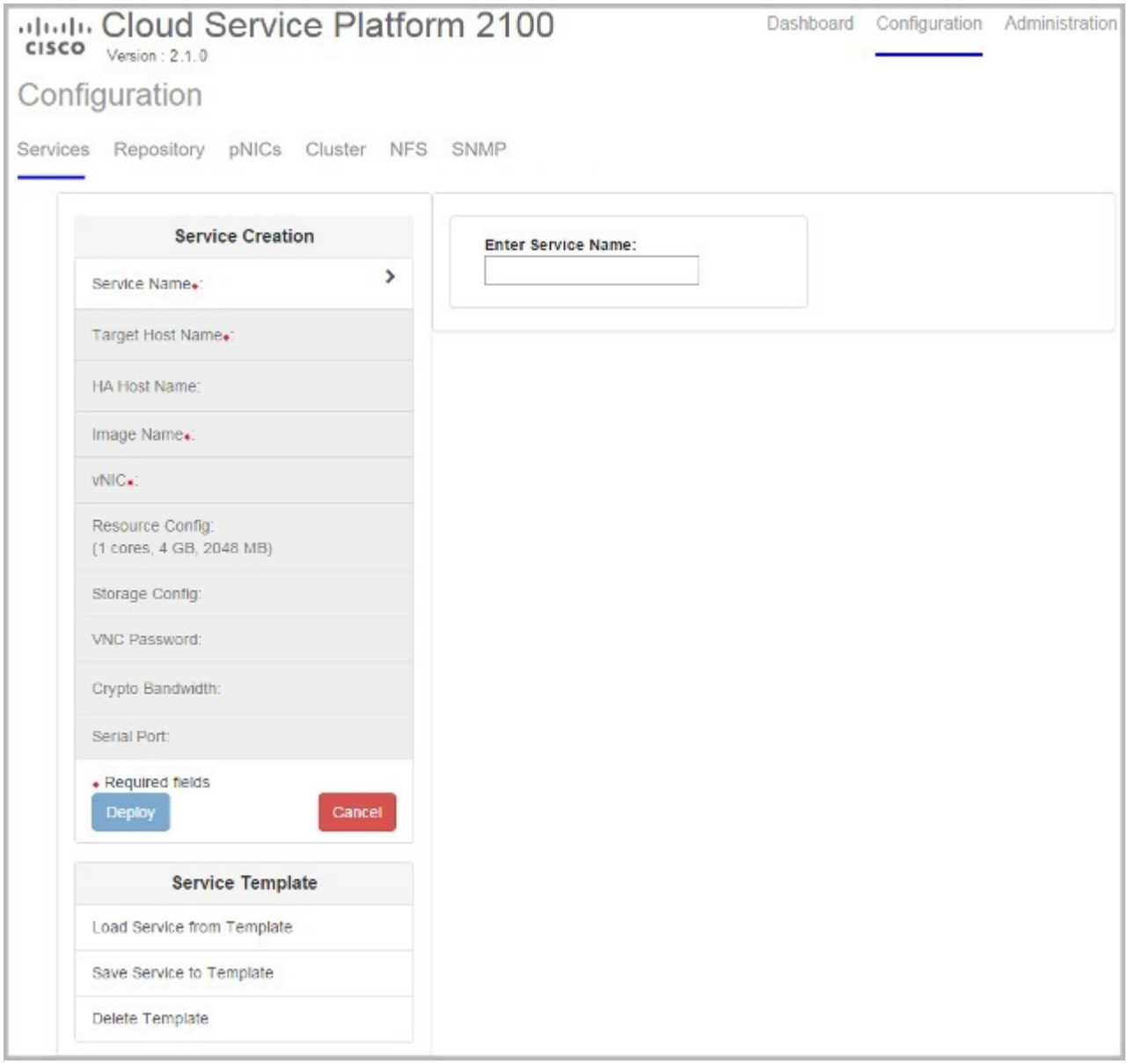
Tip You can also use this procedure to upload or copy the banner files and configuration files to the repository.



Creating a Service Instance

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

Step 2 On the **Services** page, click **Create**.
The **Service Creation** page is displayed.



Step 3 Enter a name for the service in the **Enter Service Name** field and press **Enter**.

Step 4 Click **Target Host Name** and choose a target host from the available hosts.

Step 5 (Optional) If you are configuring the target host with redundancy, click **HA Host Name** and choose another host from the available hosts. The selected hosts are configured as an HA pair.

Step 6 Click **Image Name** and choose an image file from the list.
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 Info**

Required area and click **Save**. For details about the additional information that your service requires, see the documentation for that service.

Step 7 Click **vNIC**.

Step 8 Click **vNIC** ***Number*** and do the following:

a) Click **VLAN** and enter the VLAN ID in the **Enter Vlan Range** field and press **Enter**. The valid range is from 0 to 4095.

b) Click **VLAN Type** and select a VLAN type. Valid choices are **Access**, **Trunk**, or **Passthrough**.

c) Click **VLAN Tagged** and select a value to specify whether frames should be tagged or not. Valid choices are **True** (tagged) or **False** (untagged).

d) Click **Native VLAN** and enter the VLAN ID for untagged traffic in the **Enter Native Vlan** field. The valid range is from 0 to 4095.

e) Click **Model** and choose the model number of the vNIC driver. Valid choices are **e1000** for the Intel Ethernet driver or **virtio** for the KVM driver.

f) Click **Network Name** and specify the name of the network in which the vNIC resides. Valid choices are:

- **Internal Network**: Create an internal network when you need to connect one service to another service. There is no connection to a physical network interface card (pNIC). To create an internal network, enter a name for the internal network in the **Enter Network Name** field.
- **External Network**: Create an external network when you want to connect to a pNIC directly (passthrough) or through a switch.

  To create an external network, select the name of the network interface that you want to use from the **Select Network Interface** table.

  You can also configure a port channel or a passthrough as a network interface as described in the following list and then select the port channel or the passthrough from the **Select Network Interface** table.

  - Click **Port Channel** and select a port channel in the **Available Port Channel Device** table.
  - Click **Passthrough** and in the **Passthrough Configuration** table, click the setting in the **Passthrough** column until the desired setting appears. Valid settings are **none**, **macvtap**, and **pcie**.

The name of the selected network interface appears in the **Network Name** field.

g) When you are satisfied with the vNIC configuration, click **Save**.

h) To add more vNICs, click **Add vNIC** and repeat Step 8.

Step 9 (Optional) Click **Resource Config** to change the service resource configuration.
The **Number of Cores**, **Disk Space (GB)**, and **RAM (MB)** fields show the resources currently available for your service. You can accept the default values or change them to different values as long as the new values do not exceed the available resources. You can also check the **NFS** check box to select an NFS location.

Note You can select an NFS location only if it has been added previously. To add an NFS location, click the **Configuration** tab and then click the **NFS** tab and provide the required information.

Step 10 (Optional) Click **Storage Config** and then click **Storage*Number*** and do the following:

a) Click **Location** and select a location in the **Storage Disk Location** field.

b) Click **Type** and choose a disk type. Valid choices are **disk** and **cdrom**.

c) Click **Format** and choose a disk format. Valid choices are **raw** and **qcow2**.

d) Click **Size (GB)** and enter the disk size in the **Enter storage size (GB)** field.

e) When you are satisfied with the storage configuration, click **Save**.

f) To add more storage space, click **Add Storage** and repeat Step 10.

Step 11 (Optional) Click **VNC Password** and enter a password in the **Enter VNC Password** field and the **Repeat 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 2100, the VNC console is accessible only through the web interface which is protected by a user name and a password.

Step 12 (Optional) If you are using the Cavium NITROX security processor card, click **Crypto Bandwidth** and specify the bandwidth.

Step 13 Click **Serial Port** and do the following:

a) Click **SerialPort*Number***.
b) Click **Type** and choose a port type. Valid choices are **telnet** and **console**.
c) Click **Service Port** and enter a value in the **Enter Service Port Number** field.
d) When you are satisfied with the serial port configuration, click **Save**.
e) To add more serial ports, click **Add Service Port** and repeat Step 13.

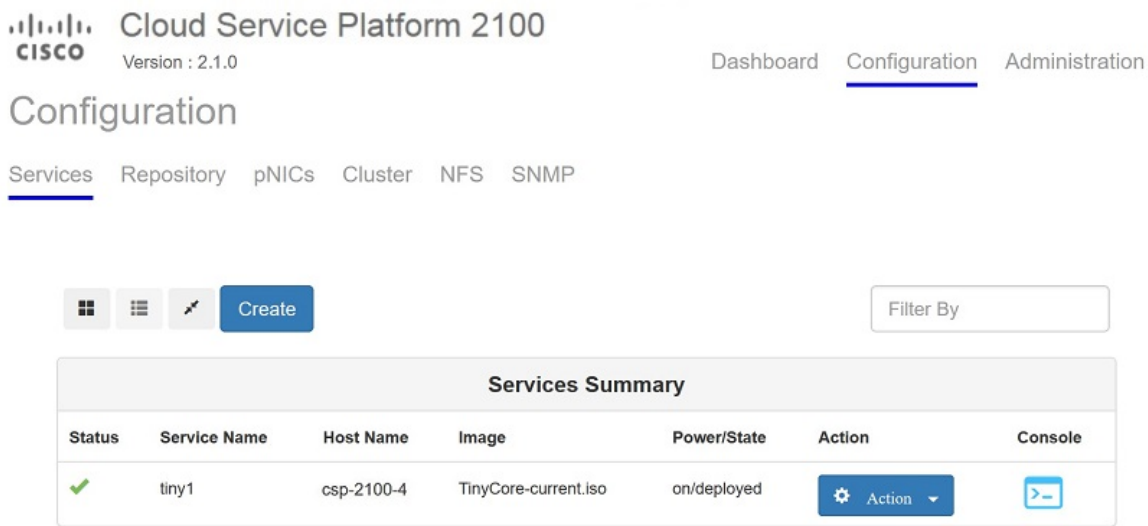
Step 14 Click **Deploy**.

Verifying Your Service Instance

Make sure that your service instance is up and running.

Step 1 Click the **Configuration** tab and then click the **Services** tab.
The **Services Summary** table shows the current status of services.

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


Cloud Service Platform 2100
Version : 2.1.0
Dashboard
Configuration
Administration
Configuration
Services
Repository
pNICs
Cluster
NFS
SNMP
Create
Filter By
Services Summary
Status
Service Name
Host Name
Image
Power/State
Action
Console
tiny1
csp-2100-4
TinyCore-current.iso
on/deployed
Action