Getting started

Converged Systems Advisor

NetApp
March 06, 2021

Table of Contents

Getting started

Quick start for Converged Systems Advisor

Getting started with Converged Systems Advisor agent and portal for Flexpod includes a few steps.

Prepare your environment

Verify support for your configuration. Prepare your environment.

Create accounts on FlexPod devices

Set up accounts in Cisco UCS Manager, on your Cisco Nexus switches, for your ONTAP systems, for VMware, and on the APIC. These accounts are used by the agent to collect configuration data.
Create accounts on Flexpod devices.

Grant CSA user privileges using a TACACS+ server

For those who use a TACACS+ server, you need to grant CSA user privileges for your switches, create a user privilege group and grant the group access to the specific set up commands needed by CSA.
Grant CSA user privileges using a TACACS+ server

Set up and deploy the agent

Deploy the Converged Systems Advisor agent on a VMware ESXi server. The agent collects configuration data about each device in your FlexPod converged infrastructure and sends that data to the Converged Systems Advisor portal.
Deploy the agent.

Add/share infrastructure in the portal

Add each FlexPod device to the Converged Systems Advisor portal to create an entire infrastructure that you can monitor. You can also share a converged infrastructure to enable another person to log in to the portal so they can view and monitor the configuration.
Add and share infrastructure in the portal.

Configure notifications

With a Premium license, you can set up notifications which alert you about changes to your FlexPod infrastructure through email notifications.
Configure notifications

Set a static IP address

If your environment does not have a DHCP server, you can set a static IP address on the Converged Systems Advisor agent.
Set a static IP address on the agent

Prepare your environment

To get started with Converged Systems Advisor, you must prepare your environment. Preparing your environment includes verifying support for your configuration and registering for a NetApp Support Site account.

You might want to learn how Converged Systems Advisor works before you get started.

Steps

1. Verify support in the NetApp Interoperability Matrix Tool:
   a. Verify that Converged Systems Advisor supports your FlexPod converged infrastructure.
   b. Verify that you have a supported VMware ESXi server for the Converged Systems Advisor agent.

      To minimize bandwidth usage, NetApp recommends installing the agent in the same data center as the FlexPod converged infrastructure.

2. Ensure that the network in which you install the agent allows connectivity between components:
   - The agent must have connectivity to each FlexPod component so it can collect configuration data.
   - The agent also requires an outbound internet connection to communicate with the following endpoints:
     - csa.netapp.com
     - docker.com
     - docker.io
3. Go to the NetApp Support Site and register for an account, if you do not have one.

   A NetApp Support Site account is required to configure the agent and to access the portal.

Create accounts for FlexPod devices

To get started, set up accounts for FlexPod devices:

- Create a read-only account for Cisco UCS Manager
- Create a read-only account for Nexus switches
- Create an admin account for ONTAP
- Create a read-only account for VMware
- Create a read-only account on the APIC
- Grant CSA user privileges using a TACACS+ server

The agent uses these accounts to collect configuration information from each device.

Create a read-only account for Cisco UCS Manager

Steps

1. Log in to Cisco UCS Manager.
2. Create a locally authenticated user named *csa-readonly*.

All new users are read-only by default.

Create a read-only account for Nexus switches

Steps

1. Log in to each Nexus switch using SSH or Telnet.
2. Enter global configuration mode:

```
 configure terminal
.. Create a new user:
```

```
 username [name] password [password] role network-operator
.. Save the configuration:
```

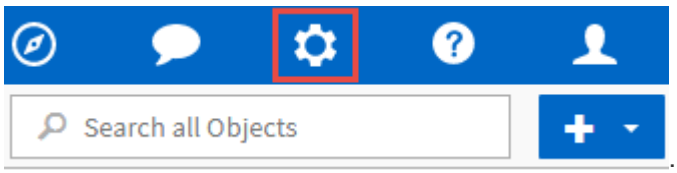
```
copy running configuration startup configuration
```

If you are using a TACACS+ server and you need to grant CSA user privileges, go to Granting CSA user privileges using a TACACS+ server.

Create an admin account for ONTAP

Steps

1. Log in to OnCommand System Manager and click the settings icon:



2. On the Users page, click **Add**.
3. Enter a user name and password and add **ssh**, **ontapi** and **console** as user login methods with admin access.

Create a read-only account for VMware

Steps

1. Log in to vCenter.
2. In the vCenter menu, choose **Administration**.
3. Under roles, choose **Read-only**.
4. Click the icon for **Clone role action** and change the name to **CSA**.
5. Select the newly created **CSA** role.
6. Click the **Edit role** icon.
7. Under **Edit role**, choose **Global** and then check **Licenses**.
8. On the sidebar, select **Single sign on→Users and groups→Create a new user**.
9. Name the new user **CSARO** under DOMAIN vpshere.local.
10. On the sidebar, select **Global Permissions** under **Access Control**.
11. Choose the user **CSARO** and assign ROLE **CSA**.
12. Log in to the Web Client.

    Use user ID: **CSARO@vsphere.local** and previously created password.

Create a read-only account on the APIC

Steps

1. Click **Admin**.
2. Click **Create new local users**.
3. Under **User Identity**, enter the user information.
4. Under **Security** select all security domain options.
5. Click **+** to add user certificates and SSH keys if needed.
6. Click **Next**.
7. Click **+** to add roles for your domain.
8. Select the **Role Name** from the dropdown menu.
9. Select **Read** for the **Role Privilege Type**.
10. Click **Finish**.

Grant CSA user privileges using a TACACS+ server

If you are using a TACACS+ server and you need to grant CSA user privileges for your switches, you should create a user privilege group and grant the group access to the specific setup commands needed by CSA.

The following commands should be written into the configuration file for your TACACS+ server.

Steps

1. Enter the following to create a user privilege group with read-only access:

```
group=group_name {
  default service=deny
  service=exec{
    priv-lvl=0
  }
}
```

1. Enter the following to grant access to commands needed by CSA:

```
cmd=show {
  permit "environment"
  permit "version"
  permit "feature"
  permit "feature-set"
  permit hardware.*
  permit "interface"
  permit "interface"
  permit "interface transceiver"
  permit "inventory"
  permit "license"
  permit "module"
  permit "port-channel database"
  permit "ntp peers"
  permit "license usage"
  permit "port-channel summary"
  permit "running-config"
  permit "startup-config"
  permit "running-config diff"
  permit "switchname"
  permit "int mgmt0"
  permit "cdp neighbors detail"
  permit "vlan"
  permit "vpc"
  permit "vpc peer-keepalive"
  permit "mac address-table"
  permit "lacp port-channel"
  permit "policy-map"
  permit "policy-map system type qos"
  permit "policy-map system type queuing"
  permit "policy-map system type network-qos"
  permit "zoneset active"
  permit "san-port-channel summary"
  permit "flogi database"
  permit "fcns database detail"
  permit "fcns database detail"
  permit "zoneset active"
  permit "vsan"
  permit "vsan usage"
  permit "vsan membership"
  }
```

1. Enter the following to add your CSA user account to the newly created group:

```
user=user_account{
  member=group_name
  login=file/etc/passwd
}
```

Setup and deploy the agent

You must deploy the Converged Systems Advisor agent on a VMware ESXi server. The agent collects configuration data about each device in your FlexPod converged infrastructure and sends that data to the Converged Systems Advisor portal.

Steps

1. Download and install the agent
2. Set up networking for the agent
3. Install an SSL certificate on the agent
4. Configure the agent to discover your FlexPod infrastructure

Download and install the agent

You must deploy the Converged Systems Advisor agent on a VMware ESXi server.

About this task

To minimize bandwidth usage, you should install the agent on a VMware ESXi server that is in the same data center as the FlexPod configuration. The agent must have connectivity to each FlexPod component and to the internet so it can send configuration data to the Converged Systems Advisor portal using HTTPS port 443.

The agent is deployed as a VMware vSphere virtual machine from an Open Virtualization Format (OVF) template. The template is Debian-based with 1 vCPU and 2 GB of RAM (more may be needed for multiple or larger FlexPod systems).

Steps

1. Download the agent:
   a. Log in to the Converged Systems Advisor portal.
   b. Click **Download Agent**.
2. Install the agent by deploying the OVF template on the VMware ESXi server.

   On some versions of VMware, you might receive a warning when deploying the OVF template. The virtual machine was developed on the latest version of VCenter with hardware compatibility for older versions, which might result in the warning. You should review the configuration options prior to acknowledging the warning and then proceed with installation.

Set up networking for the agent

You must ensure that networking is set up correctly on the agent virtual machine to enable communication between the agent and FlexPod devices and between the agent and several internet endpoints. Note that the networking stack is disabled on the virtual machine until the system initializes.

Steps

1. Ensure that an outbound internet connection enables access to the following endpoints:
   - csa.netapp.com
   - docker.com
   - docker.io
2. Log in to the agent's virtual machine console using the VMware vSphere client.

   The default user name is `csa` and the default password is `netapp`.

   For security purposes, SSHD is disabled by default.
3. When prompted, change the default password and make note of the password, because it cannot be recovered.

   After you change the password, the system reboots and starts the agent software.
4. If DHCP is not available in the subnet, configure a static IP address and DNS settings using standard Debian tools, and then reboot the agent.

   Click here for detailed instructions.

   The network configuration for the Debian virtual machine defaults to DHCP. NetworkManager is installed and provides a text user interface that you can start from the command nmtui (see the man page for more details).

   For additional help with networking, see the network configuration page on the Debian wiki.
5. If your security policies dictate that the agent must be on one network to communicate with FlexPod devices and another network to communicate with the internet, add a second network interface in VCenter and configure the correct VLANs and IP addresses.
6. If a proxy server is required for internet access, run the following command:

   `sudo csa_set_proxy`

   The command generates two prompts and shows the required format for the proxy entry. The first prompt enables you to specify an HTTP proxy, while the second enables you to specify an HTTPS proxy.

   Enter the HTTP proxy below using the format:
   `http://user:password@proxy-server:proxy-port`

   Leave blank if no HTTP proxy is required for internet access.
7. Once the network is up, wait approximately 5 minutes for the system to update and start.

   A broadcast message appears on the console when the agent is operational.
8. Verify connectivity by running the following CLI command from the agent:

   ```
   curl -k https://www.netapp.com/us/index.aspx
   ```

If the command fails, verify DNS settings. The agent virtual machine must have a valid DNS configuration and the ability to reach csa.netapp.com.

Install an SSL certificate on the agent

Optional: If needed, install an SSL certificate on the agent.

The agent creates a self-signed certificate when the virtual machine boots for the first time. If required, you can delete that certificate and use your own SSL certificate.

About this task

Converged Systems Advisor supports the following:
* Any cipher compatible with OpenSSL version 1.0.1 or greater
* TLS 1.1 and TLS 1.2

Steps

1. Log in to the agent's virtual machine console.
2. Navigate to `/opt/csa/certs`
3. Delete the self-signed certificate that the agent created.
4. Paste your SSL certificate.
5. Restart the virtual machine.

Configure the agent to discover your FlexPod infrastructure

You must configure the agent to collect configuration data from each device in your FlexPod converged infrastructure.
The agent requires credentials to collect configuration data. You must provide the credentials when you configure the agent.

Steps

1. Open a web browser and enter the IP address of the agent virtual machine.
2. Log in to the agent with the customer's NetApp Support Site account user name and password.

For any partners deploying a licensed version of CSA on behalf of their customer, it's important for the customer's account to be used in this step (for NetApp Support and records management).

3. Add the FlexPod devices that you want the agent to discover.

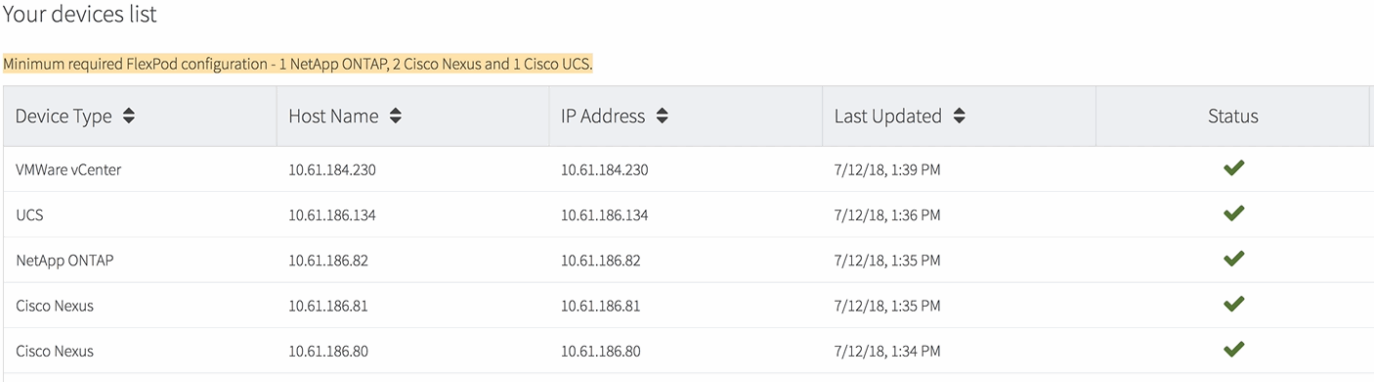
   You have two options:

   a. Click **Add a device** to enter details about your FlexPod devices, one by one.
   b. Click **Import devices** to fill out and upload a CSV template that includes details about all devices.

      Note the following:
      * The user name and password should be for the account that you previously created for the device.
      * If your UCS environment has LDAP user management configured, then you must add the user's domain before the user name. For example: local\csa-readonly

Result

Each device in the FlexPod infrastructure should display in the table with a checkmark.



Add infrastructure to the portal

After you configure the agent, it sends information about each FlexPod device to the Converged Systems Advisor portal. You must now select each of those components in the portal to create an entire infrastructure that you can monitor.

Steps

1. In the Converged Systems Advisor portal, click **Add Infrastructure**.
2. Complete the steps to add the infrastructure:
   a. Enter basic details about the infrastructure.

      If you are adding a Cisco ACI Infrastructure, enter **yes** when asked if your FlexPod uses Cisco UCS Manager; and enter **Nexus switch in ACI mode** when asked the type of Network Configuration your FlexPod contains.

   b. Select each device that is part of the FlexPod configuration.

      When you select a device, the Eligibility column displays either **Eligible** or **Not Eligible**. A device is not eligible if it was discovered by a different agent.

3. After you have selected all of the required components, you should see a green checkmark next to each device type.

   a. Add your Converged Systems Advisor serial number to unlock key functionality.
   b. Review the summary, accept the terms of the license agreement, and click **Add Infrastructure**.

      If you are a partner or reseller, you can skip the steps about adding a license or serial number and just click **Add Infrastructure**.

Result

Converged Systems Advisor adds the infrastructure to the portal and starts collecting configuration data about each device. Wait a few minutes for the agent to collect information from the devices.

Sharing an infrastructure with other users

Sharing a converged infrastructure enables another person to log in to the Converged Systems Advisor portal so they can view and monitor the configuration. The person who you share the infrastructure with must have a NetApp Support Site account.

Steps

1. In the Converged Systems Advisor portal, click the **Settings icon**, and then click **Users**.
2. Select the configuration from the User table.
3. Click the  icon.
4. Enter one or more email addresses next to the user role that you want to provide.

   View the differences between each role.

   You can enter multiple email addresses in a single field by pressing **Enter** after the first email address.

5. Click **Send**.

Result

The user should receive an email that contains instructions for accessing Converged Systems Advisor.

Configure notifications

If you have a Premium license, Converged Systems Advisor can alert you about changes to your FlexPod infrastructure through email notifications.

Steps

1. In the Converged Systems Advisor portal, click the **Settings icon**, and then click **Alert Settings**.
2. Check the notification that you would like to receive for each converged infrastructure that has a Premium license.

   Each notification includes the following information:

Collection Failures	Alerts you when Converged Systems Advisor cannot collect data from a converged infrastructure.
Offline Agent	Alerts you when a Converged Systems Advisor agent is not online.
Daily Alert Digest	Alerts you about failed rules that occurred on the previous day.

3. Click **Save**.

Result

Converged Systems Advisor will now send email notifications to the users associated with the converged

infrastructure.

Set a static IP address on the agent

If your environment does not have a DHCP server, you can set a static IP address on the Converged Systems Advisor agent.

Steps

1. Log in to the agent's virtual machine console using the VMware vSphere client.

   The default user name is **csa** and the default password is **netapp**. Change the password, if prompted.

2. Enter `sudo su -` at the csa prompt to become root.
3. Enter `# systemctl stop csa.service` to stop the CSA service.
4. Enter the following to determine your correct interface file name.

   In this example, the interface file name is `eth0`.

   ```
   # ls /etc/network/interfaces.d/
   ```

5. Enter `# /sbin/ifdown eth0` to stop the active interface.
6. Edit the /etc/network/interfaces.d/eth0 file with the editor of your choice.

   ```
   # nano /etc/network/interfaces.d/eth0
   ```
   or
   ```
   # vi /etc/network/interfaces.d/eth0
   ```

   The file contains the following:

   ```
   allow-hotplug eth0
   iface eth0 inet dhcp
   ```

7. Remove `iface eth0 inet dhcp` and add the following.
   NOTE: You must substitute the correct values for all the entries that follow the field names in the example below. For instance, `192.168.11.1` is the value for the gateway in the example. However, instead of `192.168.11.1`, you should enter the correct address for your gateway.

   ```
   iface eth0 inet static
   address 192.168.11.100
   netmask 255.255.255.0
   gateway 192.168.11.1
   dns-domain example.com
   dns-nameservers 192.168.11.1
   ```

8. Save the file.

   In nano, you enter **ctrl + o** followed by **ctrl + x** to save.

9. Enter `vi/etc/resolv.conf` to open the configuration file.
10. Add `nameserver <ip_address>` to the top of the file.

11. Enter `# ifup eth0` to start the network interface.
12. Enter `systemctl start csa.service` to restart Converged Systems Advisor.