



# **Converged Systems Advisor**

## Converged Systems Advisor

NetApp  
June 20, 2025

This PDF was generated from <https://docs.netapp.com/us-en/converged-systems-advisor/index.html> on June 20, 2025. Always check docs.netapp.com for the latest.

# Table of Contents

Converged Systems Advisor .....	1
Discover what's new .....	1
Get started .....	1
Learn about Converged Systems Advisor .....	1
Get help and connect with peers .....	1
Release notes .....	2
What's new in Converged Systems Advisor .....	2
31 July 2020 .....	2
New functionality for storage change detection (diffs) .....	2
Expanded configuration assurance for cluster interconnect switches .....	2
Initial coverage of NVMe designs .....	2
Archive of "What's new in Converged Systems Advisor" .....	2
Contents .....	3
30 April 2020 .....	3
3 February 2020 .....	4
7 November 2019 .....	5
24 July 2019 .....	5
25 April 2019 .....	6
28 March 2019 .....	6
17 January 2019 .....	7
13 September 2018 .....	8
Known issues .....	8
Concepts .....	10
Converged Systems Advisor overview .....	10
How Converged Systems Advisor works .....	10
Licensing .....	11
Security .....	12
How the data is collected .....	12
How the data is transferred .....	13
How the data is kept secure and private .....	13
User roles .....	14
Getting started .....	15
Quick start for Converged Systems Advisor .....	15
1 Prepare your environment .....	15
2 Create accounts on FlexPod devices .....	15
3 Grant CSA user privileges using a TACACS+ server .....	15
4 Set up and deploy the agent .....	15

 5	Add/share infrastructure in the portal .....	15
 6	Configure notifications .....	15
 7	Set a static IP address .....	16
	Prepare your environment .....	16
	Create accounts for FlexPod devices .....	16
	Create a read-only account for Cisco UCS Manager .....	17
	Create a read-only account for Nexus switches .....	17
	Create an admin account for ONTAP .....	17
	Create a read-only account for VMware .....	18
	Create a read-only account on the APIC .....	18
	Grant CSA user privileges using a TACACS+ server .....	18
	Setup and deploy the agent .....	21
	Download and install the agent .....	21
	Set up networking for the agent .....	21
	Install an SSL certificate on the agent .....	23
	Configure the agent to discover your FlexPod infrastructure .....	23
	Add infrastructure to the portal .....	24
	Sharing an infrastructure with other users .....	25
	Configure notifications .....	25
	Set a static IP address on the agent .....	26
	Monitoring your infrastructure .....	28
	Review the history for an infrastructure .....	28
	Monitor rules in your infrastructure .....	29
	Review alerts for failed rules and warnings .....	29
	Remediate failed rules .....	29
	Suppress failed rules .....	30
	Display suppressed rules .....	31
	Generate reports .....	32
	Track support contracts .....	32
	Troubleshoot Converged Systems Advisor .....	34
	You cannot connect to the agent through a web browser .....	34
	The agent cannot discover devices .....	34
	Unable to connect to agent VM using SSH .....	34
	Where to get help and find more information .....	36
	Legal notices .....	37
	Copyright .....	37
	Trademarks .....	37
	Patents .....	37
	Privacy policy .....	37
	Open source .....	37

# Converged Systems Advisor

NetApp Converged Systems Advisor validates, monitors, and optimizes the deployment of your FlexPod converged infrastructure to ensure the best performance and availability for your business applications.

## Discover what's new

[What's new in Converged Systems Advisor](#)

## Get started

[Quick start](#)

## Learn about Converged Systems Advisor

- [Overview](#)
- [Architecture](#)
- [Licensing](#)

## Get help and connect with peers

[NetApp Community: Converged Infrastructure](#)

# Release notes

## What's new in Converged Systems Advisor

NetApp periodically updates Converged Systems Advisor to bring you new features, enhancements, and bug fixes.

To confirm FlexPod components are supported by the CSA agent, reference the [NetApp Interoperability Matrix Tool](#) (IMT).

### 31 July 2020

The release includes the following enhancements:

- [New functionality for storage change detection \(diffs\)](#)
- [Expanded configuration assurance for cluster interconnect switches](#)
- [Initial coverage of NVMe designs](#)

#### New functionality for storage change detection (diffs)

Now you can detect changes that have occurred on the storage system. To check for change, from the **Storage Inventory** pages, click **View Configuration Difference**. Then, select a previous configuration data and time, which will be compared to the most recent storage configuration. Any changes that have occurred will be highlighted for quick review.

#### Expanded configuration assurance for cluster interconnect switches

In the Converged Systems Advisor portal, the configuration assurance checks have been expanded to monitor the supportability of ONTAP cluster interconnect switching for the following models:

- Cisco Nexus 3132Q-V
- Cisco Nexus 3232C
- Cisco Nexus 92300YC

#### Initial coverage of NVMe designs

Initial configuration assurance checks have been added to monitor supportability of NVMe ONTAP storage designs in FlexPod.

## Archive of "What's new in Converged Systems Advisor"

NetApp periodically updates Converged Systems Advisor to bring you new features, enhancements, and bug fixes.

To confirm FlexPod components are supported by the CSA agent, reference the [NetApp Interoperability Matrix Tool](#) (IMT).

## Contents

This archive contains information from the following releases:

- [30 April 2020](#)
- [3 February 2020](#)
- [7 November 2019](#)
- [24 July 2019](#)
- [25 April 2019](#)
- [28 March 2019](#)
- [17 January 2019](#)
- [13 September 2018](#)

## 30 April 2020

This release includes the following enhancements:

- [Upgrade Advisor](#)
- [Cluster interconnect switch](#)
- [Capacity card enhancements](#)
- [System diagram alerts](#)

### Upgrade Advisor

Now you can check compatibility for your VMware vCenter and ONTAP versions with your Nexus and UCS components. To check compatibility, use Upgrade Advisor in the dashboard under Firmware Interoperability. All versions you see are supported.



### Cluster interconnect switch

**Cluster Interconnect Switch** was added under **Firmware Interoperability** in the Dashboard view. Now you can monitor the supportability of ONTAP cluster interconnect switches for the following models:

- Cisco Nexus 3132Q-V
- Cisco Nexus 3232C
- Cisco Nexus 92300YC



In the agent, you can now add a cluster interconnect switch as a device in the **Add Device Information** drop-down menu.

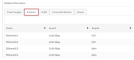


Capacity card enhancements

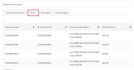
Links to network port utilization and UCS Blade Server utilization were also added to help you monitor and expand your FlexPod infrastructure. In the Dashboard view, when you go to Capacity, you'll see two new links.



Port Utilization links to detailed information for interfaces in the Network tier.



UCS Blade Server Utilization links to detailed information for blades in the Compute tier.



System diagram alerts

You'll now see alerts in the diagram views of your system so you can monitor your infrastructure better.



Fixed issues

The following known issues have been fixed in this release:

Bug ID	Description
<a href="#">1253405</a>	Nexus switch port status might be displayed incorrectly in Converged Systems Advisor.

- Return to [Contents](#)

3 February 2020

This release includes the following enhancements:

- [Navigation enhancements](#)
- [Aggregate details](#)

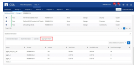
Navigation enhancements

- This release makes it possible for you to see all of your systems in **View All Systems**.
- It's easier for you to see and navigate through the structure of your component tiers. You can use the drop-down menu and arrows to view your devices.
- It's also easier to navigate to and from the Dashboard (home) view using a breadcrumb trail.



Aggregate details

In the Dashboard view, when you go to Capacity, you can now see a link to **Aggregate Details**. You can use the link provided to see detailed information about your aggregates in the Storage tier.



## Fixed issues

The following known issues have been fixed in this release:

Bug ID	Description
<a href="#">1279956</a>	Single node MetroCluster does not show the IOXM expansion module in the Overview and Rule summary on the cluster detail page.

- Return to [Contents](#)

## 7 November 2019



All of the new features and enhancements in this release are automatically included after you add your Flexpod into Converged Systems Advisor. Follow the instructions in [Getting Started](#) to add your FlexPod as a Converged Infrastructure into Converged Systems Advisor.

This release includes the following new features and enhancements:

- [MetroCluster awareness](#)
- [NVMe awareness](#)
- [Improved interoperability functionality](#)

### MetroCluster awareness

Converged Systems Advisor now supports adding a single site of a MetroCluster FlexPod as a converged infrastructure. Analytics will now be able to determine the health of both sides of the MetroCluster.

### NVMe awareness

Converged Systems Advisor will now run analytics to check the configuration of the NVMe protocol which is supported on ONTAP 9.4 and above.

### Improved interoperability functionality

Converged Systems Advisor has an updated interoperability card that will link to a pop up that shows the current, nearest, and latest versions supported for each component. A new report has been added in the pop up to show an individualized Interoperability report per component tier.

- Return to [Contents](#)

## 24 July 2019

This release includes the following new features and enhancements:

- [Support for Cisco ACI in FlexPod](#)



- [Support for multiple clusters in a single FlexPod](#)

## Support for Cisco ACI in FlexPod

Converged Systems Advisor now supports FlexPod designs with Cisco ACI Networking. The support and configuration of all devices in your FlexPod will be evaluated, even the two dynamically determined leaf switches connected to your other FlexPod devices.

## Support for multiple clusters in a single FlexPod

Converged Systems Advisor now supports multiple clusters in a single FlexPod. Storage ONTAP rules are processed on all clusters and all clusters are reflected on the system diagram.

- [Return to Contents](#)

## 25 April 2019

This release includes the following new features and enhancements:

- [Automatically resolving failed rules](#)
- [Displaying suppressed rules](#)

### Automatically resolving failed rules

Converged Systems Advisor can now automatically resolve issues that cause certain rules to fail. This functionality is automatically enabled by restarting your agent.

### Displaying suppressed rules

You can now display a global list of suppressed rules within Converged Systems Advisor and reenable alerts for suppressed rules from the list.

### Fixed issues

The following known issues have been fixed in this release:

Bug ID	Description
<a href="#">1211321</a>	System diagram images might not display for a converged infrastructure
<a href="#">1211987</a>	Storage Cluster Efficiency value is displayed incorrectly
<a href="#">1211995</a>	Nexus switch port status might be displayed incorrectly
<a href="#">1211999</a>	Space reservation status is displayed incorrectly

- [Return to Contents](#)

## 28 March 2019

The following known issues have been fixed in this release:

Bug ID	Description
<a href="#">1211993</a>	Thin Provisioned status is displayed incorrectly in CSA

Bug ID	Description
<a href="#">1211998</a>	Disk Space Utilization percentage is displayed incorrectly in CSA
<a href="#">1211990</a>	Interfaces mapped to the VLAN in Nexus switch might be mismatched with the actual device output in CSA
<a href="#">1212001</a>	Power Supply information for a rack mounted server might be displayed incorrectly in CSA

- [Return to Contents](#)

## 17 January 2019

This release includes the following new features and enhancements:

- [Support for new FlexPod devices](#)
- [Detailed information about hosts and virtual machines](#)
- [Simplified experience when adding an infrastructure](#)
- [Device import using a file](#)
- [Integration with NetApp Active IQ](#)

### Support for new FlexPod devices

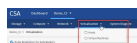
Converged Systems Advisor now supports the following FlexPod devices:

- Cisco UCS C-Series Rack Servers
- Nexus 3000 series switches
- Cisco UCS switches directly attached to NetApp controllers

For a complete list of supported devices, see the [NetApp Interoperability Matrix Tool](#).

### Detailed information about hosts and virtual machines

Converged Systems Advisor now provides more information about your virtualization environment. You can drill down to view information about individual hosts and virtual machines, including diagrams, an inventory list, and a rules summary.



### Simplified experience when adding an infrastructure

It's now easier to add an infrastructure to Converged Systems Advisor. The portal enables you to enter the information step by step:

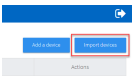


[Learn how to add an infrastructure to Converged Systems Advisor.](#)

### Device import using a file

You can now configure the Converged Systems Advisor agent to discover your FlexPod infrastructure by importing a file that includes information about each device. Importing the devices is an alternative to manually

adding each device, one by one.



[Learn how to configure the agent to discover your FlexPod infrastructure.](#)

**Integration with NetApp Active IQ**

You can now launch Active IQ from Converged Systems Advisor. The following example shows an Active IQ link available in the Storage page:



**Fixed issues**

The following known issues have been fixed in this release:

Bug ID	Description
4671	Firefox might stop responding when browsing the Converged Systems Advisor portal.
4500	The Converged Systems Advisor portal does not log you out after the timeout interval has expired. You remain logged in, but cannot see your FlexPod systems.
2794	Converged Systems Advisor displays "Pass" for the rule titled "VMware tools check" even though VMware tools was not installed on the virtual machine.

- Return to [Contents](#)

**13 September 2018**

This release of Converged Systems Advisor includes the following new features:

- A new user interface and user experience to simplify customers' FlexPod operations
- Health and best practices validation for VMware virtualization
- Support for Cisco MDS switches with expanded Fibre Channel support

**Known issues**

Known issues identify problems that might prevent you from using the service successfully. If a Bugs Online report is available, the bug ID contains a hyperlink to the report.

Bug ID	Description
<a href="#">1234597</a>	Converged Systems Advisor does not remediate the DNS configuration for more than four SVMs.

Bug ID	Description
<a href="#">1234603</a>	After creating multiple remediation jobs with collection enabled, collection is triggered only for the first remediation job.
<a href="#">1335590</a>	The "Storage failover state" CA rule was removed from Converged Systems Advisor.
<a href="#">1335593</a>	The version numbers of the Nexus and MDS switches are shown incorrectly under "Upgrade Advisor".

# Concepts

## Converged Systems Advisor overview

Converged Systems Advisor validates the deployment of your FlexPod infrastructure and provides continuous monitoring and notifications to ensure business continuity.

Watch the following video for an overview of Converged Systems Advisor:

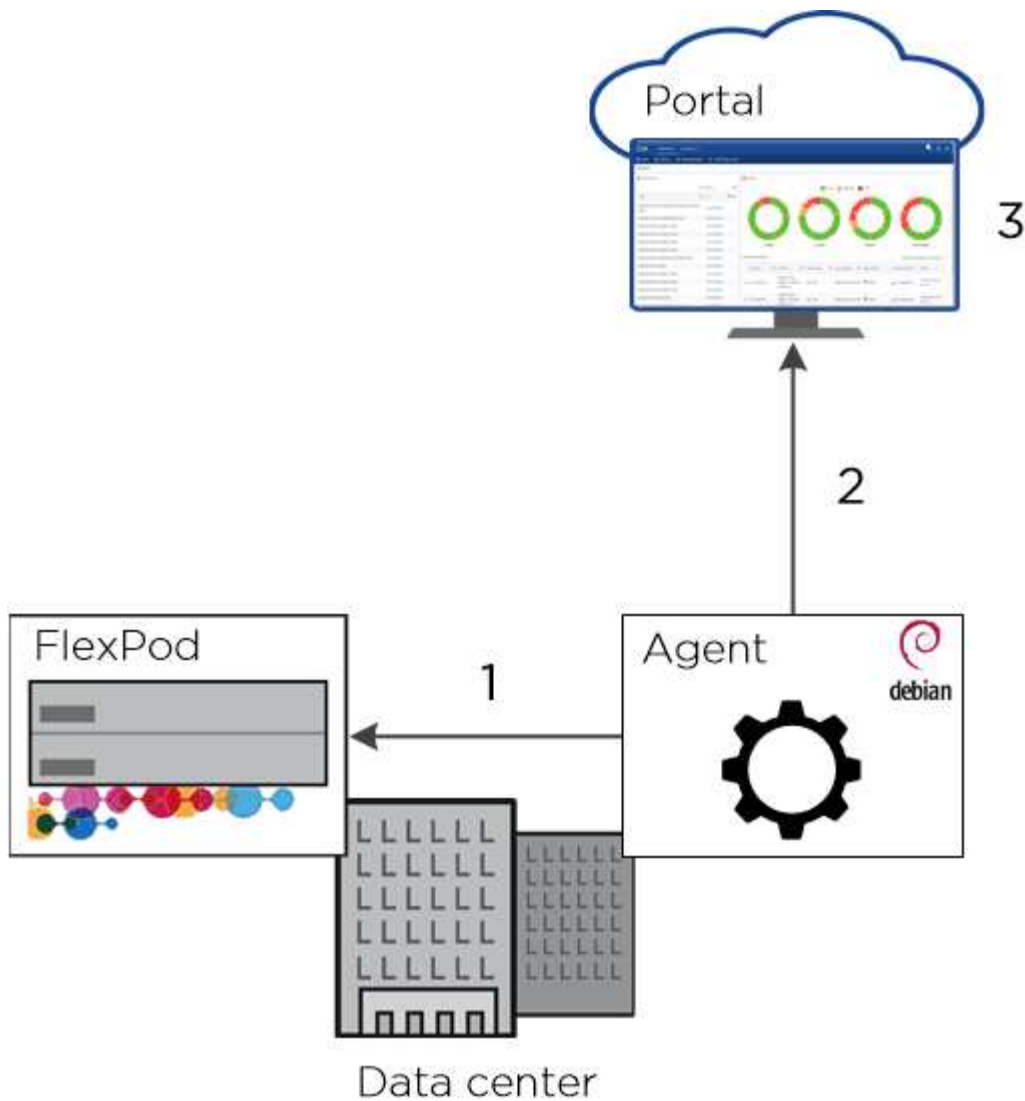
 | <https://img.youtube.com/vi/CZHu0Xp33BY/maxresdefault.jpg>

For more details about the value that Converged Systems Advisor provides, [read the datasheet](#).

## How Converged Systems Advisor works

Converged Systems Advisor is a software-as-a-service (SaaS) platform that consists of an on-premises agent and a cloud-based portal.

The following image shows the relationship between Converged Systems Advisor components:



1. The Converged Systems Advisor agent, which resides on your premises, collects configuration data from a FlexPod converged infrastructure using credentials that you provide.
2. The agent sends the data to the Converged Systems Advisor portal.
3. Users log in to the Converged Systems Advisor portal using a web browser to validate, monitor, and optimize their FlexPod converged infrastructure.

[Read how Converged Systems Advisor keeps the data secure.](#)

## Licensing

A license is required to unlock features in Converged Systems Advisor. You can choose from a few licensing options for each FlexPod converged infrastructure.

License	Features	Terms
No license	Limited version to demonstrate product capabilities: <ul style="list-style-type: none"> <li>• Monitoring of FlexPod configurations for a 24-hour trial period</li> <li>• Health dashboards to view FlexPod best practice compliance</li> <li>• Limited inventory and remediation (available in licensed versions)</li> </ul>	<ul style="list-style-type: none"> <li>• Free</li> <li>• Single use (24 hours)</li> </ul>
Standard	<ul style="list-style-type: none"> <li>• Continuous monitoring of FlexPod configurations</li> <li>• Health dashboards to view FlexPod best practice compliance</li> <li>• Firmware interoperability for compute, network, storage, and hypervisor</li> <li>• Lifecycle management tools to identify changes and prevent configuration drift</li> <li>• Detailed inventory and system diagrams for advanced troubleshooting</li> <li>• Support provided directly by NetApp</li> </ul>	Subscription-based license: <ul style="list-style-type: none"> <li>• 12 months minimum</li> <li>• 60 months maximum</li> </ul>
Premium	All functionality included in the Standard license, plus: <ul style="list-style-type: none"> <li>• Reporting               <p>Comprehensive, real-time reporting of FlexPod health, interoperability, and inventory</p> </li> <li>• Notification and alerting               <p>Regular notifications of configuration health and changes in status</p> </li> </ul>	Subscription-based license: <ul style="list-style-type: none"> <li>• 12 months minimum</li> <li>• 60 months maximum</li> </ul>

## Security

Converged Systems Advisor collects configuration data about your FlexPod converged infrastructure to help you validate and monitor the system. You might want to understand how the data is collected, how it is transferred to NetApp, and how it is kept secure and private.

### How the data is collected

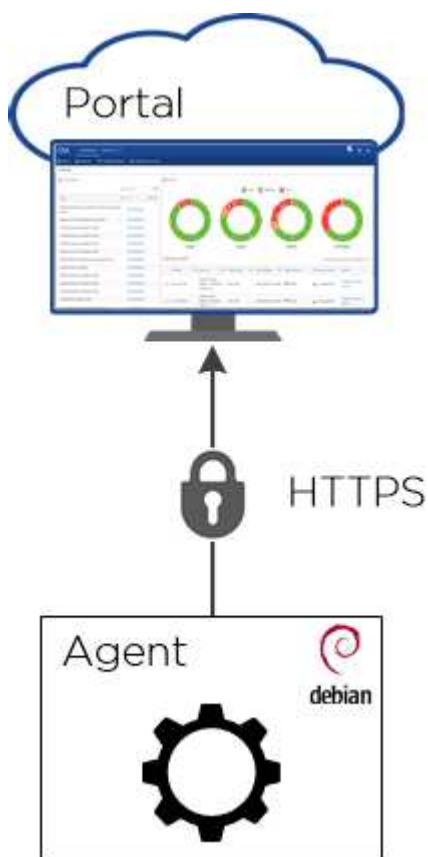
The Converged Systems Advisor agent requires credentials to access the devices in your FlexPod converged infrastructure. Read-only credentials are required for Cisco UCS and Nexus switches, while admin credentials are required for ONTAP. The credentials are encrypted and stored locally on the agent—they are not sent to the cloud-based portal.

After you provide the credentials, the agent collects *configuration* data from the devices. *Customer* data that resides on the devices is never accessed or transferred. A representative sample of the configuration data that the agent collects includes the following:

- Capacity
- CPU and memory
- Device connectivity
- Device names and IDs
- Device state
- Firmware versions
- IP addresses
- iSCSI targets
- Licenses
- MAC addresses
- Model numbers
- Serial numbers

## How the data is transferred

After the agent discovers configuration data from your FlexPod converged infrastructure, it sends the data to the Converged Systems Advisor portal using HTTPS. The communication is encrypted using NetApp's TLS 1.2 certificate.



## How the data is kept secure and private

The configuration data resides within the NetApp network and is managed by NetApp IT. The data is secured by a data access layer that requires positive identification of each user who requests access.



The user who deployed the agent can access the data from the Converged Systems Advisor portal by logging in with a NetApp Support Site account. This user has *owner* privileges to the converged infrastructure. The owner can share the converged infrastructure with other users by granting read-only, write, or owner privileges. Those users must also have a registered NetApp Support Site account to log in to the portal.

[Review the differences between read-only, write, and owner privileges.](#)

## User roles

When you share a converged infrastructure with another user, you must provide read-only, write, or owner privileges.

The following table identifies the tasks that each user role can perform.

Task	Read-only	Write	Owner
View a system	Yes	Yes	Yes
Update a system's name	No	Yes	Yes
Update support contract details	No	Yes	Yes
Edit the data collection interval	No	Yes	Yes
Request a new data collection	No	Yes	Yes
Share a system	No	Yes, with read-only or write access	Yes, with read-only, write, or owner access
Modify the components of a system	No	No	Yes
Delete a system	No	No	Yes

# Getting started

## Quick start for Converged Systems Advisor

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

### **1 Prepare your environment**

Verify support for your configuration. [Prepare your environment](#).

### **2 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](#).

### **3 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](#)

### **4 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](#).

### **5 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](#).

### **6 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:
```

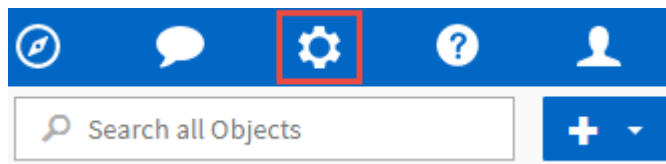
```
copy running configuration startup configuration
```

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 vpsphere.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@vpsphere.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.

Your devices list

Minimum required FlexPod configuration - 1 NetApp ONTAP, 2 Cisco Nexus and 1 Cisco UCS.

Device Type ▾	Host Name ▾	IP Address ▾	Last Updated ▾	Status
VMWare vCenter	10.61.184.230	10.61.184.230	7/12/18, 1:39 PM	✓
UCS	10.61.186.134	10.61.186.134	7/12/18, 1:36 PM	✓
NetApp ONTAP	10.61.186.82	10.61.186.82	7/12/18, 1:35 PM	✓
Cisco Nexus	10.61.186.81	10.61.186.81	7/12/18, 1:35 PM	✓
Cisco Nexus	10.61.186.80	10.61.186.80	7/12/18, 1:34 PM	✓

## 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:

<b>Collection Failures</b>	Alerts you when Converged Systems Advisor cannot collect data from a converged infrastructure.
<b>Offline Agent</b>	Alerts you when a Converged Systems Advisor agent is not online.
<b>Daily Alert Digest</b>	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.

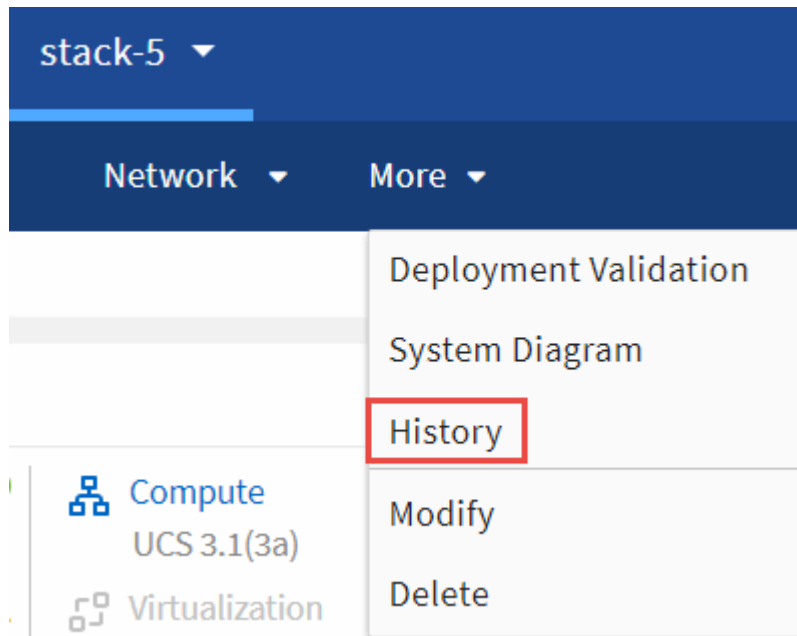
# Monitoring your infrastructure

## Review the history for an infrastructure

When you receive an alert about a failed rule, you can view a history of what changed in the configuration to help you resolve the issue.

### Steps

1. Select a converged infrastructure.
2. Click **More > History**.

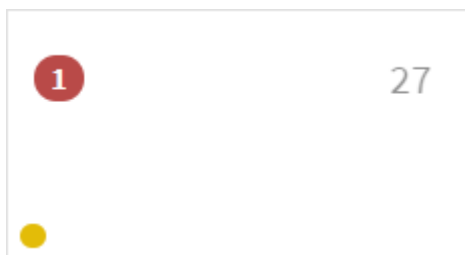


3. Click a day on the calendar to view the number of warnings and failures that were identified during each data collection.



The number that appears for each day corresponds to the number of times that the agent collected data. For example, if you keep the default collection interval of 24 hours, you should see one collection per day.

The following image shows a single collection on the 27th of the month.



4. To view more details about the data that was collected, click **Go to CI Dashboard** for a collection.
5. If needed, view the history for the last time that no warnings or failures were identified.

Comparing the data between the two collection periods can help you identify what changed.

## Monitor rules in your infrastructure

To monitor your infrastructure, you can remediate failed rules, suppress rules, view the list of rules that have been suppressed and, if desired, select to end the suppression.

### Review alerts for failed rules and warnings

Converged Systems Advisor continuously monitors your infrastructure and generates warnings and failures to ensure that the system is configured and performing to best practices.

#### Steps

1. Log in to the [Converged Systems Advisor portal](#) and click **Rules**.

The Rules page displays a summary of all rules. The status for each rule is either **Pass**, **Warning**, or **Fail**.

2. Click the filter icon in the Status column and select **Fail**, **Warning**, or both.
3. Review details about individual rules by clicking the arrow next to the Status column.
4. Follow the instructions in the resolution to fix the issue.

If needed, [review the configuration history](#) for the infrastructure to help you resolve the issue.

#### After you finish

The status for the rules that you addressed should display as Pass after the agent's next collection period.

### Remediate failed rules

Converged Systems Advisor can resolve some failed rules for you by correcting the underlying issue with the converged infrastructure.

#### About this task


- You must have the Premium license.
- You must be assigned as an owner of the converged infrastructure.

#### Steps

1. Log in to the [Converged Systems Advisor portal](#) and click **Rules**.

The Rules page displays a summary of all rules. The status for each rule is either **Pass**, **Warning**, or **Fail**.

2. Select **Filter rules that can be remediated**.
3. Expand the rule that you want to resolve.
- 4.

Click  in the top right corner of the expanded rule.

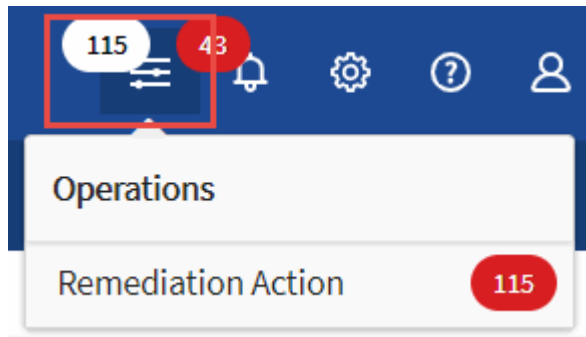


If the icon is disabled, it's either because the agent is offline, you don't have Owner privileges, or because you don't have a Premium license.

5. If necessary, fill in the input values.

Depending on the failed rule, some input values are necessary to resolve the issue.

6. If you want a data collection to be taken after the successful completion of the remediation, then select the option **Collect When Remediation Job Completes**.
7. Click **Run remediation**.
8. Click **Confirm**.
9. To view actions being taken to resolve failed rules, click the **Operations** icon and selection **Remediation Action**.



## Suppress failed rules

Converged Systems Advisor allows you to suppress rules so that do not show up in dashboard and no longer send email notifications on rule failure.






For example, enabling telnet is not recommended, but if you prefer to enable it, you can suppress the rule.

### About this task

You must have the Premium license to configure notifications.

### Steps

1. From the Dashboard, click **Rules**.
2. Find the rules that you are looking for by filtering the contents of the table.
3. Select one or more rows for rules that have a status of Warning or Fail and then click the **Alerts** icon.

4 items selected ▼		Global Filter		
Component 	Sub-category 	Resource 		
Storage	Discovery	Cluster		
Storage	Discovery	Cluster		
Storage	Discovery	Cluster		

4. Select a duration and then click **Submit**.



If you want to enable the alerts, follow these same steps and select **End Suppression**.

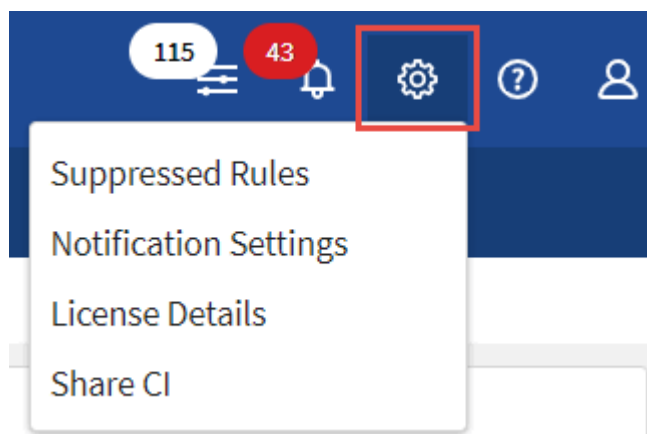
### Result

Converged Systems Advisor no longer notifies you about the rule for the specified duration and the rule will no longer be visible in the dashboard.

## Display suppressed rules







### Steps

1. Click the **Settings** icon and select **Suppressed Rules**.



2. Select the suppressed rules that you want to begin displaying.

3. Click the **Alerts** icon.

4 items selected ▼		Global Filter 		
Component 	Sub-category 	Resource 		
Storage	Discovery	Cluster		
Storage	Discovery	Cluster		
Storage	Discovery	Cluster		

4. Select **End Suppression** and then click **Submit**.

### Result

Alerts are enabled for the selected rule and the rule is displayed in the Rules table and dashboard.

## Generate reports

If you have a Premium license, you can generate several types of reports that provide details about the current status of your converged infrastructure: an inventory report, a health report, an assessment report, a deployment validation report for partners, and more.

### Steps

1. Click **Reports**.
2. Select a report and click **Generate**.
3. Choose your options for the report:
  - a. Select a converged infrastructure.
  - b. Optionally change from the most recent data collection to a previous one.
  - c. Choose how you want to view the report: in your browser, as a downloaded PDF, or via email.

### Result

Converged Systems Advisor generates the report.

## Track support contracts









You can add details about support contracts for each device in a configuration: the start date, end date, and contract ID. This enables you to easily track the details in a central location so you know when to renew support contracts for each device.

### Steps

1. Click **Select a CI** and select the converged infrastructure.
2. In the Support Contract widget, click the **Edit contract** icon.
3. Select the **Start Date** and **End Date** and enter the **Contract ID**.
4. Click **Submit**.
5. Repeat the steps for each device in the configuration.

### Result

Converged Systems Advisor now displays the support contract details for each device. You can easily see which devices have active and expired support contracts.

<input checked="" type="checkbox"/> Support Contract		<a href="#">View Details</a>
 backup	Expired	
 stack5-9k-1	Active 2019-04-10	
 stack5-9k-2	Active 2019-04-23	
 stack5-ucs	Active 2019-04-23	

# Troubleshoot Converged Systems Advisor

If you encounter a problem while using Converged Systems Advisor, the following information might help you resolve the issue.

## You cannot connect to the agent through a web browser

You need to connect to the agent through a web browser to configure discovery of your FlexPod devices. If you cannot connect through a web browser, ensure that the agent has an outbound internet connection to `csa.netapp.com`. The agent application cannot start without an internet connection, which prevents you from accessing its web interface.

If a proxy server is required for internet access, [configure the agent virtual machine to use it](#).

## The agent cannot discover devices

If the agent cannot discover a FlexPod device, verify the following:

- Ensure that the agent has an open connection to each FlexPod device.

To verify, ping each device from the agent.

- Verify whether a local network is using the 172.17.x.x subnet.

The agent uses the 172.17.x.x subnet internally. If a local network is using that same subnet, then you must change the subnet on the agent:

1. Log in to the agent's virtual machine console.

The default user name is `csa` and the default password is `netapp`. You should change the default password after you log in.

2. Add the file `/etc/docker/daemon.json` with the following contents:

```
{ "bip": "172.44.x.x" }
```

The bip address can be any non-conflicting IP address. It does not need to be in the 172 range.

3. Reboot the virtual machine.

## Unable to connect to agent VM using SSH

SSH for the agent VM is disabled by default.

- To start SSH, log in to the agent VM via the console in vCenter and run the following commands:

```
sudo su
systemctl start ssh
```

- To check if SSH is enabled, run the following command:

```
systemctl is-enabled ssh
```

- To check the status of SSH on the agent VM, run the following command:

```
systemctl status ssh
```

- To enable SSH to persist across reboots, run the following commands:

```
sudo su  
systemctl enable ssh
```

# Where to get help and find more information

You can get help and find more information about Converged Systems Advisor through various resources.

- [Converged Systems Advisor datasheet](#)

For more details about the value that Converged Systems Advisor provides.

- [NetApp Technical Report 4036: FlexPod Datacenter Technical Specifications](#)

Review the best practices and firmware requirements that Converged Systems Advisor compares your configurations against.

- [NetApp Interoperability Matrix Tool](#)

Verify support for your configuration.

- [NetApp Community](#)

Connect with peers, ask questions, exchange ideas, find resources, and share best practices.

- [NetApp Product Documentation](#)

Search NetApp product documentation for instructions, resources, and answers.

- [Open a Support Case](#)

Open a support case for additional assistance. Support cases should be opened under **Cat1 → Remote Diagnostic Tools** and **Cat2 → Converged System Advisor**.

# Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

## Copyright

<https://www.netapp.com/company/legal/copyright/>

## Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

<https://www.netapp.com/company/legal/trademarks/>

## Patents

A current list of NetApp owned patents can be found at:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

## Privacy policy

<https://www.netapp.com/company/legal/privacy-policy/>

## Open source

Notice files provide information about third-party copyright and licenses used in NetApp software.

[Notice for Converged Systems Advisor](#)



## Copyright information

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.