Maintain Console agents

NetApp Console setup and administration

NetApp
January 27, 2026

Table of Contents

Maintain Console agents

Maintain a VCenter or ESXi host for the Console agent

You can make changes to your existing VCenter or ESXi host after you deploy the Console agent. For example, you can increase the CPU or RAM of the VM instance that hosts the Console agent.

Perform these maintenance tasks using the VM web console:

- Increase disk size
- Restart the agent
- Update static routes
- Update search domains

Limitations

Upgrading the agent through the console is not yet supported. In addition, you can only view information about the IP address, DNS, and gateways.

Access the VM maintenance console

You can access the maintenance Console from the VSphere client.

Steps

1. Open the VSphere client and log in to your VCenter.
2. Select the VM instance that hosts the Console agent.
3. Select **Launch Web Console**.
4. Log in to the VM instance using the user name and password that you specified when you created the VM instance. The username is `maint` and the password is the one that you specified when you created the VM instance.

Change the maint user password

You can change the password for the `maint` user.

Steps

1. Open the VSphere client and log in to your VCenter.
2. Select the VM instance that hosts the Console agent.
3. Select **Launch Web Console**.
4. Log in to the VM instance using the user name and password that you specified when you created the VM instance. The username is `maint` and the password is the one that you specified when you created the VM instance.
5. Enter `1` to view the `System Configuration` menu.
6. Enter `1` to change the maintenance user password and follow the on-screen prompts.

Increase the CPU or RAM of the VM instance

You can increase the CPU or RAM of the VM instance that hosts the Console agent.

Edit the VM instance settings in your VCenter or ESXi host, then use the maintenance Console to apply the changes.

Steps in the VSphere client

1. Open the VSphere client and log in to your VCenter.
2. Select the VM instance that hosts the Console agent.
3. Right-click the VM instance and select **Edit Settings**.
4. Increase the hard drive space used for /opt or the /var partition.
    a. Select **Hard Disk 2** to increase the hard drive space used for /opt.
    b. Select **Hard Disk 3** to increase the hard drive space used for /var.
5. Save your changes.

Steps in the maintenance console

1. Open the VSphere client and log in to your VCenter.
2. Select the VM instance that hosts the Console agent.
3. Select **Launch Web Console**.
4. Log in to the VM instance using the user name and password that you specified when you created the VM instance. The username is `maint` and the password is the one that you specified when you created the VM instance.
5. Enter `1 to view the `System Configuration` menu.
6. Enter `2` and follow the on-screen prompts. The console scans for new settings and increases the size of the partitions.

View network settings for the agent VM

View the network settings for the agent VM in the VSphere client to confirm or troubleshoot network issues. You can only view (not update) the following network settings: IP address and DNS details.

Steps

1. Open the VSphere client and log in to your VCenter.
2. Select the VM instance that hosts the Console agent.
3. Select **Launch Web Console**.
4. Log in to the VM instance using the user name and password that you specified when you created the VM instance. The username is `maint` and the password is the one that you specified when you created the VM instance.
5. Enter `2` to view the `Network Configuration` menu.
6. Enter a number between 1 and 6 to view the corresponding network settings.

Update the static routes for the agent VM

Add, update, or remove static routes for the agent VM as needed.

Steps

1. Open the VSphere client and log in to your VCenter.
2. Select the VM instance that hosts the Console agent.
3. Select **Launch Web Console**.
4. Log in to the VM instance using the user name and password that you specified when you created the VM instance. The username is `maint` and the password is the one that you specified when you created the VM instance.
5. Enter `2` to view the `Network Configuration` menu.
6. Enter `7` to update static routes and follow the on-screen prompts.
7. Press Enter.
8. Optionally, make additional changes.
9. Enter `9` to commit your changes.

Update domain search settings for the agent VM

You can update the search domain settings for the agent VM.

Steps

1. Open the VSphere client and log in to your VCenter.
2. Select the VM instance that hosts the Console agent.
3. Select **Launch Web Console**.
4. Log in to the VM instance using the user name and password that you specified when you created the VM instance. The username is `maint` and the password is the one that you specified when you created the VM instance.
5. Enter `2`` to view the `Network Configuration` menu.
6. Enter `8` to update the domain search settings and follow the on-screen prompts.
7. Press Enter.
8. Optionally, make additional changes.
9. Enter `9` to commit your changes.

Access the agent diagnostic tools

Access diagnostic tools to troubleshoot issues with the Console agent. NetApp Support may ask you to do this when troubleshooting issues.

Steps

1. Open the VSphere client and log in to your VCenter.
2. Select the VM instance that hosts the Console agent.
3. Select **Launch Web Console**.
4. Log in to the VM instance using the user name and password that you specified when you created the VM instance. The username is `maint` and the password is the one that you specified when you created the VM instance.
5. Enter `3` to view the Support and Diagnostics menu.

6. Enter `1` to access the diagnostic tools and follow the on-screen prompts.
   + For example, you can verify that all agent services are running. Check the Console agent status.

Access the agent diagnostic tools remotely

You can access diagnostic tools remotely with a tool such as Putty. Enable SSH access to the agent VM by assigning a one-time password.

SSH access enables advanced terminal features like copy and paste.

Steps

1. Open the VSphere client and log in to your VCenter.
2. Select the VM instance that hosts the Console agent.
3. Select **Launch Web Console**.
4. Log in to the VM instance using the user name and password that you specified when you created the VM instance. The username is `maint` and the password is the one that you specified when you created the VM instance.
5. Enter `3` to view the `Support and Diagnostics` menu.
6. Enter `2` to access the diagnostic tools and follow the on-screen prompts to configure a one-time password that expires in 24 hours.
7. Use an SSH tool such as Putty to connect to the agent VM using the user name `diag` and the one-time password that you configured.

Install a CA-signed certificate for web-based console access

When you use the NetApp Console in restricted mode, the user interface is accessible from the Console agent virtual machine that's deployed in your cloud region or on-premises. By default, the Console uses a self-signed SSL certificate to provide secure HTTPS access to the web-based console running on the Console agent.

If required by your business, you can install a certificate signed by a certificate authority (CA), which provides better security protection than a self-signed certificate. After you install the certificate, the Console uses the CA-signed certificate when users access the web-based console.

Install an HTTPS certificate

Install a certificate signed by a CA for secure access to the web-based console running on the Console agent.

About this task

You can install the certificate using one of the following options:

- Generate a certificate signing request (CSR) from the Console, submit the certificate request to a CA, and then install the CA-signed certificate on the Console agent.

  The key pair that the Console uses to generate the CSR is stored internally on the Console agent. The Console automatically retrieves the same key pair (private key) when you install the certificate on the Console agent.

- Install a CA-signed certificate that you already have.

  With this option, the CSR is not generated through the Console. You generate the CSR separately and store the private key externally. You provide the Console with the private key when you install the certificate.

Steps

1. Select **Administration > Agents**.
2. On the **Overview** page, select the action menu for a Console agent and select **HTTPS Setup**.

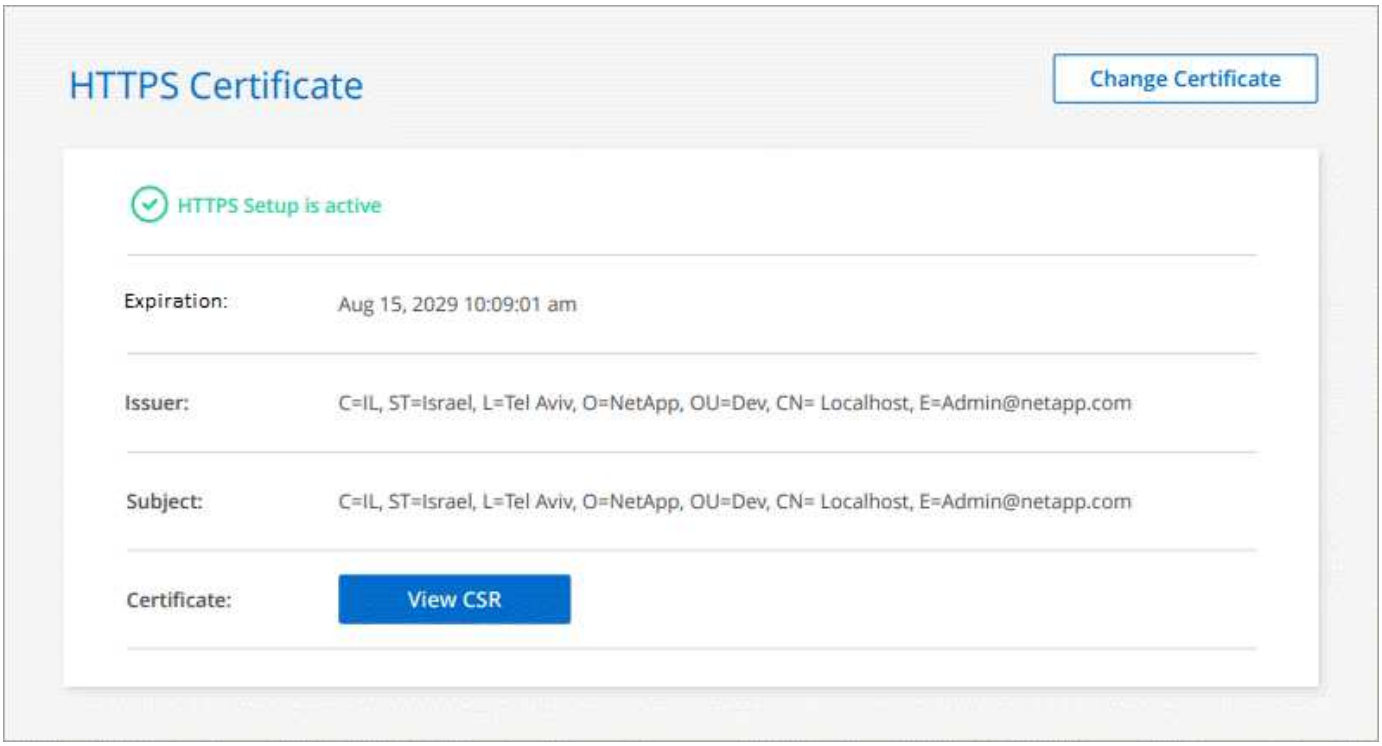
   The Console agent must be connected to edit it.

3. In the HTTPS Setup page, install a certificate by generating a certificate signing request (CSR) or by installing your own CA-signed certificate:

Option	Description
Generate a CSR	a. Enter the host name or DNS of the Console agent host (its Common Name), and then select **Generate CSR**. The Console displays a certificate signing request. b. Use the CSR to submit an SSL certificate request to a CA. The certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format. c. Upload the certificate file and then select **Install**.
Install your own CA-signed certificate	a. Select **Install CA-signed certificate**. b. Load both the certificate file and the private key and then select **Install**. The certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format.

Result

The Console agent now uses the CA-signed certificate to provide secure HTTPS access. The following image shows an agent that is configured for secure access:



Renew the Console HTTPS certificate

You should renew the agent's HTTPS certificate before it expires to ensure secure access. If you don't renew the certificate before it expires, a warning appears when users access the web console using HTTPS.

Steps

1. Select **Administration > Agents**.
2. On the **Overview** page, select the action menu for a Console agent and select **HTTPS Setup**.

   Details about the certificate displays, including the expiration date.

3. Select **Change Certificate** and follow the steps to generate a CSR or install your own CA-signed certificate.

Configure a Console agent to use a proxy server

If your corporate policies require you to use a proxy server for all communication to the internet, then you need to configure your agents to use that proxy server. If you didn't configure a Console agent to use a proxy server during installation, then you can configure the Console agent to use that proxy server at any time.

The agent's proxy server enables outbound internet access without a public IP or NAT gateway. The proxy server provides outbound connectivity only for the Console agent, not for Cloud Volumes ONTAP systems.

If Cloud Volumes ONTAP systems lack outbound internet access, the Console configures them to use the Console agent's proxy server. You must ensure that the Console agent's security group allows inbound connections over port 3128. Open this port after deploying the Console agent.

If the Console agent itself doesn't have an outbound internet connection, Cloud Volumes ONTAP systems cannot use the configured proxy server.

Supported configurations

- Transparent proxy servers are supported for agents that serve Cloud Volumes ONTAP systems. If you use NetApp data services with Cloud Volumes ONTAP, create a dedicated agent for Cloud Volumes ONTAP where you can use a transparent proxy server.
- Explicit proxy servers are supported with all agents, including those that manage Cloud Volumes ONTAP systems and those that manage NetApp data services.
- HTTP and HTTPS.
- The proxy server can reside in the cloud or in your network.

Once you have configured a proxy, you cannot change the proxy type. If you need to change the proxy type, you remove the Console agent and add a new agent with the new proxy type.

Enable an explicit proxy on a Console agent

When you configure a Console agent to use a proxy server, that agent and the Cloud Volumes ONTAP systems that it manages (including any HA mediators), all use the proxy server.

This operation restarts the Console agent. Verify the Console agent is idle before proceeding.

Steps

1. Select **Administration > Agents**.
2. On the **Overview** page, select the action menu for a Console agent and select **Edit agent**.

   The Console agent must be active to edit it.

3. Select **HTTP Proxy Configuration**.
4. Select **Explicit proxy** in the Configuration type field.
5. Select **Enable Proxy**.
6. Specify the server using the syntax http://*address:port* or https://*address:port*
7. Specify a user name and password if basic authentication is required for the server.

   Note the following:

   - The user can be a local user or domain user.
   - For a domain user, you must enter the ASCII code for the \ as follows: domain-name%92user-name

     For example: netapp%92proxy

   - The Console doesn't support passwords that include the @ character.
8. Select **Save**.

Enable a transparent proxy for a Console agent

Only Cloud Volumes ONTAP supports using a transparent proxy on the Console agent. If you use NetApp data services in addition to Cloud Volumes ONTAP, you should create a separate agent to use for data services or to use for Cloud Volumes ONTAP.

Before enabling a transparent proxy, ensure that the following requirements are met:

- The agent is installed on the same network as the transparent proxy server.
- TLS inspection is enabled on the proxy server.
- You have a certificate in PEM format that matches the one used on the transparent proxy server.
- You do not use the Console agent for any NetApp data services other than Cloud Volumes ONTAP.

To configure an existing agent to use a transparent proxy server, you use the Console agent maintenance tool that is available through the command line on the Console agent host.

When you configure a proxy server, the Console agent restarts. Verify the Console agent is idle before proceeding.

Steps

Ensure that you have a certificate file in PEM format for the proxy server. If you do not have a certificate, contact your network administrator to obtain one.

1. Open a command-line interface on the Console agent host.
2. Navigate to the Console agent maintenance tool directory: `/opt/application/netapp/service-manager-2/agent-maint-console`
3. Run the following command to enable the transparent proxy, where `/home/ubuntu/<certificate-file>.pem` is the directory and name certificate file that you have for the proxy server:

   ```
   ./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
   ```

   Ensure that the certificate file is in PEM format and resides in the same directory as the command or specify the full path to the certificate file.

   ```
   ./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
   ```

Modify the transparent proxy for the Console agent

You can update a Console agent's existing transparent proxy server by using the `proxy update` command or remove the transparent proxy server by using the `proxy remove` command. For more information, review the documentation for Agent maintenance console.

Once you have configured a proxy, you cannot change the proxy type. If you need to change the proxy type, you remove the Console agent and add a new agent with the new proxy type.

Update the Console agent proxy if it loses access to the internet

If the proxy configuration for your network changes, your agent might lose access to the internet. For example, if someone changes the password for the proxy server or updates the certificate. In this case, you'll need to access the UI from the Console agent host directly and update the settings. Ensure you have network access to the Console agent host and that you can log into the Console.

Enable direct API traffic

If you configured a Console agent to use a proxy server, you can enable direct API traffic on the Console agent in order to send API calls directly to cloud provider services without going through the proxy. Agents running in AWS, Azure, or Google Cloud support this option.

If you disable Azure Private Links with Cloud Volumes ONTAP and use service endpoints, enable direct API traffic. Otherwise, the traffic won't be routed properly.

Learn more about using an Azure Private Link or service endpoints with Cloud Volumes ONTAP

Steps

1. Select **Administration > Agents**.
2. On the **Overview** page, select the action menu for a Console agent and select **Edit agent**.

   The Console agent must be active to edit it.

3. Select **Support Direct API Traffic**.
4. Select the checkbox to enable the option and then select **Save**.

Troubleshoot the Console agent

To troubleshoot issues with a Console agent, you can verify issues yourself or work with NetApp Support who might ask for your system ID, agent version, or the latest AutoSupport messages.

If you have a NetApp Support Site account, you can also view the NetApp Knowledge Base.

Common error messages and resolutions

This table lists common error messages and shows how to fix them:

Error message	Explanation	What to do
Unable to load the Console agent UI	Agent installation has failed	• Verify that the Service Manager service is active. • Verify that all containers are running. • Ensure your firewall allows access to the service at port 8888. • If you still have problems, contact support.

Error message	Explanation	What to do
Cannot access the NetApp agent UI	This message appears when trying to access the IP address of an agent. The agent can fail to initialize if it doesn't have the correct network access or if it is unstable.	• Connect to the Console agent. • Verify that the Service Manager service • Verify that the agent has the network access it needs. Learn more about required network access endpoints.
Unable to load agent settings	The Console displays this message when you try to access the Agent settings page..	• Check if the OCCM container is running and working. • If the issue persists, contact support.
Unable to load support information for the agent.	This message displays if the agent cannot access your support account.	• Verify that the agent has outbound access to the required endpoints. Learn more about required network access endpoints.

Check the Console agent status

Use one of the following commands to verify your Console agent. All services should have a status of *Running*. If this isn't the case, contact NetApp support.

For more detailed information about accessing the Console agent diagnostics, see the following topics:

- Check the Console agent status (for Linux host deployments)
- Check the Console agent status (for VCenter deployments)

Docker (for Ubuntu and VCenter deployments)

```
docker ps -a
```

Podman (for RedHat Enterprise Linux deployments)

```
podman ps -a
```

View the Console agent version

View the Console agent version to confirm the upgrade or share it with your NetApp representative.

Steps

1. Select **Administration > Support > Agents**.

   The Console displays the version at the top of the page.

Verify network access

Ensure that the Console agent has the network access it needs. Learn more about required network access points.

Run configuration checks on the Console agent

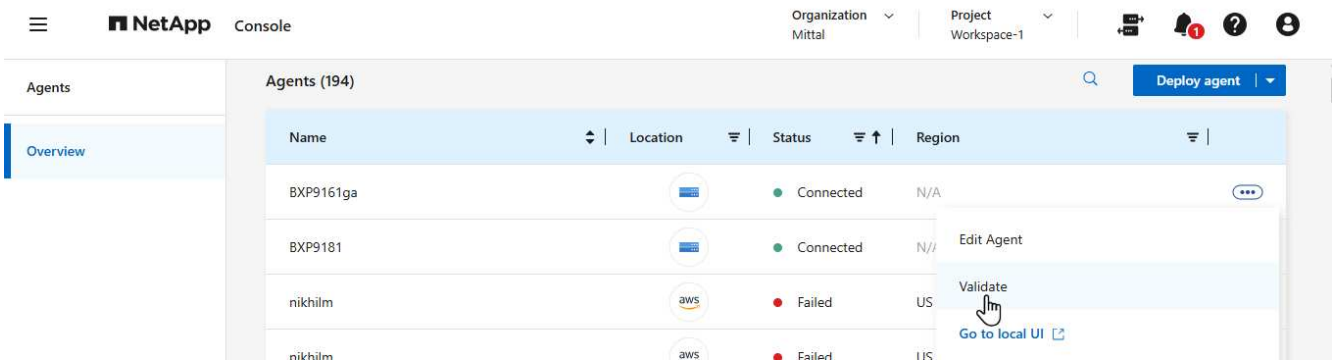
Run configuration checks on Console agents from the Console or or the Agent maintenance console to make sure they are connected.

You can also run configuration checks using the agent maintenance console. Learn more about using the config-checker validate command.

You can only validate agents that have a status of **Connected**.

Steps from the Console

1. Select **Administration > Agents**.
2. Select the action menu for a Console agent that you want to check and choose **Validate**.



Validation can take up to 15 minutes. Results show when it is done.

Console agent installation issues

If the installation fails, view the report and logs to resolve the issues.

You can also access the validation report in JSON format and the configuration logs directly from the Console agent host in the following directories:

```
/tmp/netapp-console-agents/logs

/tmp/netapp-console-agents/results.json
```

- For new agent deployments, NetApp checks for the following endpoints: listed here. This configuration check fails with an error if you are using the previous endpoints used for upgrades, listed here. NetApp recommends updating your firewall rules to allow access to the current endpoints and block access to the previous endpoints at your earliest convenience Learn how to update your networking.
- If you update the endpoints in your firewall, your existing agents will continue to work.

Disable configuration checks for manual installations

There may be times when you need to disable the configuration checks that verify outbound connectivity during installation. For example, when manually installing an agent in your Government Cloud environment, you need to disable the configuration checks or the installation will fail.

Steps

You disable the configuration check by setting the *skipConfigCheck* flag in the *com/opt/application/netapp/service-manager-2/config.json* file. By default, this flag is set to false and the configuration check verifies outbound access for the agent. Set this flag to true to disable the check. Be familiar with JSON syntax before completing this step.

To re-enable the configuration check, use these steps and set the *skipConfigCheck* flag to false.

Steps

1. Access the Console agent host as root or with sudo privileges.
2. Create a backup copy of the */opt/application/netapp/service-manager-2/config.json* file to ensure you can revert your changes.
3. Stop the service manager 2 service by running the following command:

```
systemctl stop netapp-service-manager.service
```

1. Edit the */opt/application/netapp/service-manager-2/config.json* file and change the value of the *skipConfigCheck* flag to true.

```
  "skipConfigCheck": true
```

2. Save your file.
3. Restart the service manager 2 service by running the following command:

```
systemctl restart netapp-service-manager.service
```

Work with NetApp Support

If you haven't been able to resolve the issues with your Console agent, you may want to contact NetApp Support. NetApp support may ask for the Console agent ID or for you to send the Console agent logs to them if they don't have them already.

Find the Console agent ID

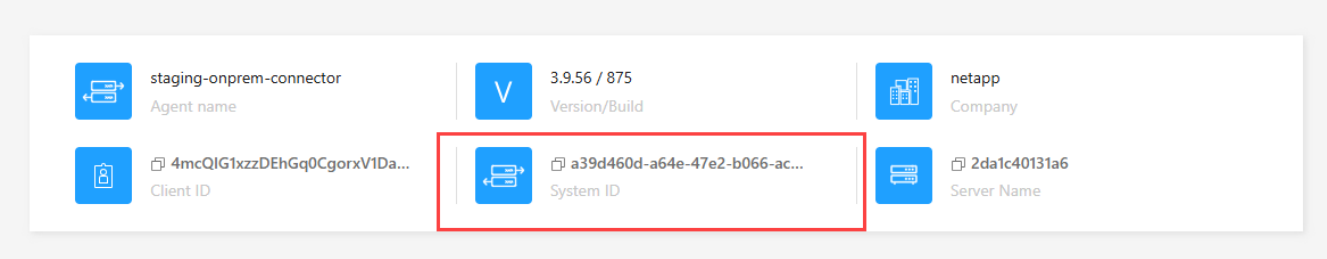
To help you get started, you may need the system ID of your Console agent. The ID is typically used for licensing and troubleshooting purposes.

Steps

1. Select **Administration > Support > Agents**.

   You can find the system ID at the top of the page.

Example



2. Hover and click on the ID to copy it.

Download or send an AutoSupport message

If you're having problems, NetApp might ask you to send an AutoSupport message to NetApp support for troubleshooting purposes.

The NetApp Console takes up to five hours to send AutoSupport messages due to load balancing. For urgent communication, download the file and send it manually.

Steps

1. Select **Administration > Support > Agents**.
2. Depending on how you need to send the information to NetApp support, choose one of the following options:
   a. Select the option to download the AutoSupport message to your local machine. You can then send it to NetApp Support using a preferred method.
   b. Select **Send AutoSupport** to directly send the message to NetApp Support.

Fix download failures when using a Google Cloud NAT gateway

The Console agent automatically downloads software updates for Cloud Volumes ONTAP. Your configuration can cause the download to fail if it uses a Google Cloud NAT gateway. You can correct this issue by limiting the number of parts that the software image is divided into. This step must be completed by using the API.

Step

1. Submit a PUT request to /occm/config with the following JSON as body:

```
{
  "maxDownloadSessions": 32
}
```

The value for *maxDownloadSessions* can be 1 or any integer greater than 1. If the value is 1, then the downloaded image will not be divided.

Note that 32 is an example value. The value depends on your NAT configuration and the number of simultaneous sessions.

Learn more about the /occm/config API call

Get help from the NetApp Knowledge Base

View troubleshooting information created by the NetApp Support team.

Uninstall and remove a Console agent

Uninstall the a Console agent to troubleshoot issues or to permanently remove it from the host. The steps that you need to use depends on the deployment mode that you're using. Once you have removed a Console agent from your environment, you can remove it from the Console.

Learn about NetApp Console deployment modes.

Uninstall the agent when using standard or restricted mode

If you're using standard mode or restricted mode (in other words, the agent host has outbound connectivity), then you should follow the steps below to uninstall the agent.

Steps

1. Connect to the Linux VM for the agent.
2. From the Linux host, run the uninstallation script:

   ```
   /opt/application/netapp/service-manager-2/uninstall.sh [silent]
   ```

   silent runs the script without prompting you for confirmation.

Remove Console agents from the Console

If you have deleted an agent VM or uninstalled the agent, you should remove it from the list of agents in the Console. After you delete an agent VM or uninstall the agent software, the agent shows a status of **Disconnected** in the Console.

Note the following about removing a Console agent:

- This action doesn't delete the virtual machine.
- This action can't be reverted—once you remove a Console agent, you can't add it back.

Steps

1. Select **Administration > Agents**.
2. On the **Overview** page , select the action menu for a disconnected agent and select **Remove agent**.
3. Enter the name of the agent to confirm and then select **Remove**.

Copyright information

Trademark information