Plan

ONTAP 9

NetApp
February 06, 2026

Table of Contents

Plan

Prepare to use ONTAP AutoSupport

You can configure an ONTAP cluster to deliver AutoSupport messages to NetApp. As part of this, you can also send a copy of the messages to local email addresses, typically within your organization. You should prepare to configure AutoSupport by reviewing the available options.

Deliver AutoSupport messages to NetApp

AutoSupport messages can be delivered to NetApp using either HTTPS or SMTP protocols. Beginning with ONTAP 9.15.1, you can also use TLS with SMTP.

Use HTTPS whenever possible for communication with AutoSupport OnDemand and uploads of large files.

Also note the following:

- Only one delivery channel to NetApp can be configured for the AutoSupport messages. You cannot use two protocols to deliver AutoSupport messages to NetApp.
- AutoSupport limits the maximum file size for each protocol. If the size of an AutoSupport message exceeds the configured limit, AutoSupport delivers as much of the message as possible but truncation will occur.
- You can change the maximum file size if needed. Learn more about `system node autosupport modify` in the ONTAP command reference.
- Both protocols can be transported over IPv4 or IPv6 based on the address family to which the name resolves.
- The TCP connection established by ONTAP to send AutoSupport messages is temporary and short-lived.

HTTPS

This provides the most robust features. Note the following:

- AutoSupport OnDemand and the transfer of large files are supported.
- An HTTPS PUT request is attempted first. If the request fails during transmission, the request restarts where it stopped.
- If the server does not support PUT, the HTTPS POST method is used instead.
- The default limit for HTTPS transfers is 50 MB.
- The HTTPS protocol uses port 443.

SMTP

As a general rule, you should use SMTP only if HTTPS is not allowed or is unsupported. Note the following:

- AutoSupport OnDemand and transfers of large files are not supported.
- If SMTP sign-in credentials are configured, they are sent unencrypted and in the clear.

- The default limit for transfers is 5 MB.
- The unsecured SMTP protocol uses port 25.

Improve SMTP security with TLS

When using SMTP, all traffic is unencrypted and can be easily intercepted and read. Beginning with ONTAP 9.15.1 you can also use TLS with SMTP (SMTPS). In this case, *explicit TLS* is used which activates the secure channel after the TCP connection is established.

The following port is typically used for SMTPS: Port 587

Additional configuration considerations

There are a few additional considerations when configuring AutoSupport.

For more information about the commands relevant to these considerations, refer to Set up AutoSupport.

Send a local copy using email

Regardless of the protocol used to deliver AutoSupport messages to NetApp, you can also send a copy of each message to one or more local email addresses. For example, you might send messages to your internal support organization or a partner organization.

> If you deliver messages to NetApp using SMTP (or SMTPS) and you also send local email copies of those messages, the same email server configuration is used.

HTTP proxy

Depending on your network configuration, the HTTPS protocol might require additional configuration of a proxy URL. If HTTPS is used to send AutoSupport messages to technical support and you have a proxy, you must identify the URL for the proxy. If the proxy uses a port other than the default (port 3128), you can specify the port for that proxy. You can also optionally specify a user name and password for proxy authentication.

Install the server certificate

With TLS (HTTPS or SMTPS), the certificate downloaded from the server is validated by ONTAP based on the root CA certificate. Before using HTTPS or SMTPS, you need to make sure the root certificate is installed in ONTAP and that ONTAP can validate the server certificate. This validation is performed based on the CA that signed the server certificate.

ONTAP includes a large number of pre-installed root CA certificates. In many cases, the certificate for your server will be immediately recognized by ONTAP without additional configuration. Depending on how the server certificate was signed, you might need to install a root CA certificate and any intermediate certificates.

Use the following procedure to install the certificate, if needed. You should install all required certificates at the cluster level.

Example 1. Steps

System Manager

1. In System Manager, select **Cluster** > **Settings**.
2. Scroll down to the **Security** section.
3. Select → next to **Certificates**.
4. Under the **Trusted certificate authorities** tab click **Add**.
5. Click **Import** and select the certificate file.
6. Complete the configuration parameters for your environment.
7. Click **Add**.

CLI

1. Begin the installation:

   ```
   security certificate install -type server-ca
   ```

   Learn more about `security certificate install` in the ONTAP command reference.

2. Look for the following console message:

   ```
   Please enter Certificate: Press <Enter> when done
   ```

3. Open the certificate file with a text editor.
4. Copy the entire certificate including the following lines:

   ```
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

5. Paste the certificate into the terminal after the command prompt.
6. Press **Enter** to complete the installation.
7. Confirm the certificate is installed by running one of the following commands:

   ```
   security certificate show-user-installed
   ```

   ```
   security certificate show
   ```

   Learn more about `security certificate show` in the ONTAP command reference.

Related information

- Set up AutoSupport
- ONTAP command reference

Set up ONTAP AutoSupport

You can configure an ONTAP cluster to deliver AutoSupport messages to NetApp technical support and send email copies to your internal support organization. As part of this, you can also test the configuration before using it in a production environment.

About this task

Beginning with ONTAP 9.5, you enable and configure AutoSupport for all nodes of a cluster simultaneously. When a new node joins the cluster, the node automatically inherits the same AutoSupport configuration. To support this, the scope of the CLI command `system node autosupport modify` is cluster-level. The `-node` command option is retained for backward compatibility, but it is ignored.

> In ONTAP 9.4 and earlier releases, the command `system node autosupport modify` is specific to each node. If your cluster is running ONTAP 9.4 or earlier, you need to enable and configure AutoSupport on each node in the cluster.

Before you begin

The recommended transport configuration for delivering AutoSupport messages to NetApp is HTTPS (HTTP with TLS). This option provides the most robust features and best security.

Review Prepare to use AutoSupport for more information before configuring your ONTAP cluster.

Steps

1. Ensure that AutoSupport is enabled:

   ```
   system node autosupport modify -state enable
   ```

2. If you want NetApp technical support to receive AutoSupport messages, use the following command:

   ```
   system node autosupport modify -support enable
   ```

   You must enable this option if you want to enable AutoSupport to work with AutoSupport OnDemand or if you want to upload large files, such as core dump and performance archive files, to technical support or a specified URL.

   > AutoSupport OnDemand is enabled by default and functional when configured to send messages to technical support using HTTPS transport protocol.

3. If you enabled NetApp technical support to receive AutoSupport messages, specify which transport protocol to use for these messages.

   You can choose from the following options:

If you want to…	Then set the following parameters of the `system node autosupport modify` command…
Use the default HTTPS protocol	a. Set `-transport` to `https`. b. If you use a proxy, set `-proxy-url` to the URL of your proxy. This configuration supports communication with AutoSupport OnDemand and uploads of large files.
Use SMTP	Set `-transport` to `smtp`. This configuration does not support AutoSupport OnDemand or uploads of large files.

4. If you want your internal support organization or a support partner to receive AutoSupport messages, perform the following actions:
   a. Identify the recipients in your organization by setting the following parameters of the `system node autosupport modify` command:

Set this parameter…	To this…
`-to`	Up to five comma-separated individual email addresses or distribution lists in your internal support organization that will receive key AutoSupport messages
`-noteto`	Up to five comma-separated individual email addresses or distribution lists in your internal support organization that will receive a shortened version of key AutoSupport messages designed for cell phones and other mobile devices
`-partner-address`	Up to five comma-separated individual email addresses or distribution lists in your support partner organization that will receive all AutoSupport messages

   b. Check that addresses are correctly configured by listing the destinations using the `system node autosupport destinations show` command.
5. If you configured the recipient addresses for your internal support organization in the previous step or you chose SMTP transport for messages to technical support, configure SMTP by setting the following parameters of the `system node autosupport modify` command:
   - Set `-mail-hosts` to one or more mail hosts, separated by commas.

     You can set a maximum of five.

     You can configure a port value for each mail host by specifying a colon and port number after the mail host name: for example, `mymailhost.example.com:5678`, where 5678 is the port for the mail host.

- Set `-from` to the email address that sends the AutoSupport message.

6. Configure DNS.
7. Optionally, add command options if you want to change specific settings:

If you want to do this…	Then set the following parameters of the `system node autosupport modify` command…
Hide private data by removing, masking, or encoding sensitive data in the messages	Set `-remove-private-data` to `true`. If you change from `false` to `true`, all AutoSupport history and all associated files are deleted.
Stop sending performance data in periodic AutoSupport messages	Set `-perf` to `false`.

8. If you are using SMTP to deliver AutoSupport messages to NetApp, you can optionally enable TLS for improved security.
   a. Display the values available for the new parameter:

```
cluster1::> system node autosupport modify -smtp-encryption ?
```

   b. Enable TLS for SMTP message delivery:

```
cluster1::> system node autosupport modify -smtp-encryption start_tls
```

   c. Display the current configuration:

```
cluster1::> system node autosupport show -fields smtp-encryption
```

9. Check the overall configuration by using the `system node autosupport show` command with the `-node` parameter.
10. Verify the AutoSupport operation by using the `system node autosupport check show` command.

    If any problems are reported, use the `system node autosupport check show-details` command to view more information.

11. Test that AutoSupport messages are being sent and received:
    a. Use the `system node autosupport invoke` command with the `-type` parameter set to `test`:

```
cluster1::> system node autosupport invoke -type test -node node1
```

    b. Confirm that NetApp is receiving your AutoSupport messages:

```
system node autosupport history show -node local
```

The status of the latest outgoing AutoSupport message should eventually change to `sent-successful` for all appropriate protocol destinations.

c. Optionally, confirm that AutoSupport messages are being sent to your internal support organization or to your support partner by checking the email of any address that you configured for the `-to`, `-noteto`, or `-partner-address` parameters of the `system node autosupport modify` command.

Related information

- Prepare to use AutoSupport
- ONTAP command reference

Copyright information

Trademark information