Manage AutoSupport with the CLI

ONTAP 9

NetApp
June 04, 2024

Table of Contents

Manage AutoSupport with the CLI

Manage AutoSupport overview

AutoSupport is a mechanism that proactively monitors the health of your system and automatically sends messages to NetApp technical support, your internal support organization, and a support partner. Although AutoSupport messages to technical support are enabled by default, you must set the correct options and have a valid mail host to have messages sent to your internal support organization.

Only the cluster administrator can perform AutoSupport management. The storage virtual machine (SVM) administrator has no access to AutoSupport.

AutoSupport is enabled by default when you configure your storage system for the first time. AutoSupport begins sending messages to technical support 24 hours after AutoSupport is enabled. You can shorten the 24-hour period by upgrading or reverting the system, modifying the AutoSupport configuration, or changing the system time to be something other than a 24-hour period.

You can disable AutoSupport at any time, but you should leave it enabled. Enabling AutoSupport can significantly help speed problem determination and resolution should a problem occur on your storage system. By default, the system collects AutoSupport information and stores it locally, even if you disable AutoSupport.

For more information about AutoSupport, see the NetApp Support Site.

Related information

- NetApp Support
- Learn more about the AutoSupport commands in the ONTAP CLI

Use AutoSupport and Active IQ Digital Advisor

The AutoSupport component of ONTAP collects telemetry and sends it for analysis. Active IQ Digital Advisor analyzes the data from AutoSupport and provides proactive care and optimization. Using artificial intelligence, Active IQ can identify potential problems and help you resolve them before they impact your business.

Active IQ enables you to optimize your data infrastructure across your global hybrid cloud by delivering actionable predictive analytics and proactive support through a cloud-based portal and mobile app. Data-driven insights and recommendations from Active IQ are available to all NetApp customers with an active SupportEdge contract (features vary by product and support tier).

Here are some things you can do with Active IQ:

- Plan upgrades. Active IQ identifies issues in your environment that can be resolved by upgrading to a newer version of ONTAP and the Upgrade Advisor component helps you plan for a successful upgrade.
- View system wellness. Your Active IQ dashboard reports any issues with wellness and helps you correct those issues. Monitor system capacity to make sure you never run out of storage space. View support cases for your system.

- Manage performance. Active IQ shows system performance over a longer period than you can see in System Manager. Identify configuration and system issues that are impacting your performance.
- Maximize efficiency. View storage efficiency metrics and identify ways to store more data in less space.
- View inventory and configuration. Active IQ displays complete inventory and software and hardware configuration information. See when service contracts are expiring and renew them to ensure you remain supported.

Related information

NetApp Documentation: Active IQ Digital Advisor

Launch Active IQ

SupportEdge Services

When and where AutoSupport messages are sent

AutoSupport sends messages to different recipients, depending on the type of message. Learning when and where AutoSupport sends messages can help you understand messages that you receive through email or view on the Active IQ (formerly known as My AutoSupport) web site.

Unless specified otherwise, settings in the following tables are parameters of the `system node autosupport modify` command.

Event-triggered messages

When events occur on the system that require corrective action, AutoSupport automatically sends an event-triggered message.

When the message is sent	Where the message is sent
AutoSupport responds to a trigger event in the EMS	Addresses specified in `-to` and `-noteto`. (Only critical, service-affecting events are sent.) Addresses specified in `-partner-address` Technical support, if `-support` is set to `enable`

Scheduled messages

AutoSupport automatically sends several messages on a regular schedule.

When the message is sent	Where the message is sent
Daily (by default, sent between 12:00 a.m. and 1:00 a.m. as a log message)	Addresses specified in `-partner-address` Technical support, if `-support` is set to `enable`

When the message is sent	Where the message is sent
Daily (by default, sent between 12:00 a.m. and 1:00 a.m. as a performance message), if the `-perf` parameter is set to `true`	Addresses specified in -partner-address`  Technical support, if `-support` is set to `enable`
Weekly (by default, sent Sunday between 12:00 a.m. and 1:00 a.m.)	Addresses specified in `-partner-address` Technical support, if `-support` is set to `enable`

Manually triggered messages

You can manually initiate or resend an AutoSupport message.

When the message is sent	Where the message is sent
You manually initiate a message using the `system node autosupport invoke` command	If a URI is specified using the `-uri` parameter in the `system node autosupport invoke` command, the message is sent to that URI. If `-uri` is omitted, the message is sent to the addresses specified in `-to` and `-partner-address`. The message is also sent to technical support if `-support` is set to `enable`.
You manually initiate a message using the `system node autosupport invoke-core-upload` command	If a URI is specified using the `-uri` parameter in the `system node autosupport invoke-core-upload` command, the message is sent to that URI, and the core dump file is uploaded to the URI. If `-uri` is omitted in the `system node autosupport invoke-core-upload` command, the message is sent to technical support, and the core dump file is uploaded to the technical support site. Both scenarios require that `-support` is set to `enable` and `-transport` is set to `https` or `http`. Due to the large size of core dump files, the message is not sent to the addresses specified in the `-to` and `-partner-addresses` parameters.

When the message is sent	Where the message is sent
You manually initiate a message using the `system node autosupport invoke-performance-archive` command	If a URI is specified using the `-uri` parameter in the `system node autosupport invoke-performance-archive` command, the message is sent to that URI, and the performance archive file is uploaded to the URI. If `-uri` is omitted in the `system node autosupport invoke-performance-archive`, the message is sent to technical support, and the performance archive file is uploaded to the technical support site. Both scenarios require that `-support` is set to `enable` and `-transport` is set to `https` or `http`. Due to the large size of performance archive files, the message is not sent to the addresses specified in the `-to` and `-partner-addresses` parameters.
You manually resend a past message using the `system node autosupport history retransmit` command	Only to the URI that you specify in the `-uri` parameter of the `system node autosupport history retransmit` command

Messages triggered by technical support

Technical support can request messages from AutoSupport using the AutoSupport OnDemand feature.

When the message is sent	Where the message is sent
When AutoSupport obtains delivery instructions to generate new AutoSupport messages	Addresses specified in `-partner-address` Technical support, if `-support` is set to `enable` and `-transport` is set to `https`
When AutoSupport obtains delivery instructions to resend past AutoSupport messages	Technical support, if `-support` is set to `enable` and `-transport` is set to `https`
When AutoSupport obtains delivery instructions to generate new AutoSupport messages that upload core dump or performance archive files	Technical support, if `-support` is set to `enable` and `-transport` is set to `https`. The core dump or performance archive file is uploaded to the technical support site.

How AutoSupport creates and sends event-triggered messages

AutoSupport creates event-triggered AutoSupport messages when the EMS processes a

trigger event. An event-triggered AutoSupport message alerts recipients to problems that require corrective action and contains only information that is relevant to the problem. You can customize what content to include and who receives the messages.

AutoSupport uses the following process to create and send event-triggered AutoSupport messages:

1. When the EMS processes a trigger event, EMS sends AutoSupport a request.

   A trigger event is an EMS event with an AutoSupport destination and a name that begins with a `callhome.` prefix.

2. AutoSupport creates an event-triggered AutoSupport message.

   AutoSupport collects basic and troubleshooting information from subsystems that are associated with the trigger to create a message that includes only information that is relevant to the trigger event.

   A default set of subsystems is associated with each trigger. However, you can choose to associate additional subsystems with a trigger by using the `system node autosupport trigger modify` command.

3. AutoSupport sends the event-triggered AutoSupport message to the recipients defined by the `system node autosupport modify` command with the `-to`, `-noteto`, `-partner-address`, and `-support` parameters.

   You can enable and disable delivery of AutoSupport messages for specific triggers by using the `system node autosupport trigger modify` command with the `-to` and `-noteto` parameters.

Example of data sent for a specific event

The `storage shelf PSU failed` EMS event triggers a message that contains basic data from the Mandatory, Log Files, Storage, RAID, HA, Platform, and Networking subsystems and troubleshooting data from the Mandatory, Log Files, and Storage subsystems.

You decide that you want to include data about NFS in any AutoSupport messages sent in response to a future `storage shelf PSU failed` event. You enter the following command to enable troubleshooting-level data for NFS for the `callhome.shlf.ps.fault` event:

```
        cluster1::\>
        system node autosupport trigger modify -node node1 -autosupport
-message shlf.ps.fault -troubleshooting-additional nfs
```

Note that the `callhome.` prefix is dropped from the `callhome.shlf.ps.fault` event when you use the `system node autosupport trigger` commands, or when referenced by AutoSupport and EMS events in the CLI.

Types of AutoSupport messages and their content

AutoSupport messages contain status information about supported subsystems. Learning what AutoSupport messages contain can help you interpret or respond to messages that you receive in email or view on the Active IQ (formerly known as My AutoSupport) web

site.

Type of message	Type of data the message contains
Event-triggered	Files containing context-sensitive data about the specific subsystem where the event occurred
Daily	Log files
Performance	Performance data sampled during the previous 24 hours
Weekly	Configuration and status data
Triggered by the `system node autosupport invoke` command	Depends on the value specified in the `-type` parameter: • `test` sends a user-triggered message with some basic data. This message also triggers an automated email response from technical support to any specified email addresses, using the `-to` option, so that you can confirm that AutoSupport messages are being received. • `performance` sends performance data. • `all` sends a user-triggered message with a complete set of data similar to the weekly message, including troubleshooting data from each subsystem. Technical support typically requests this message.
Triggered by the `system node autosupport invoke-core-upload` command	Core dump files for a node
Triggered by the `system node autosupport invoke-performance-archive` command	Performance archive files for a specified period of time

Type of message	Type of data the message contains
Triggered by AutoSupport OnDemand	AutoSupport OnDemand can request new messages or past messages: • New messages, depending on the type of AutoSupport collection, can be `test`, `all`, or `performance`. • Past messages depend on the type of message that is resent. AutoSupport OnDemand can request new messages that upload the following files to the NetApp Support Site at mysupport.netapp.com: • Core dump • Performance archive

What AutoSupport subsystems are

Each subsystem provides basic and troubleshooting information that AutoSupport uses for its messages. Each subsystem is also associated with trigger events that allow AutoSupport to collect from subsystems only information that is relevant to the trigger event.

AutoSupport collects context-sensitive content. You can view information about subsystems and trigger events by using the `system node autosupport trigger show` command.

AutoSupport size and time budgets

AutoSupport collects information, organized by subsystem, and enforces a size and time budget on content for each subsystem. As storage systems grow, AutoSupport budgets provide control over the AutoSupport payload, which in turn provides scalable delivery of AutoSupport data.

AutoSupport stops collecting information and truncates the AutoSupport content if the subsystem content exceeds its size or time budget. If the content cannot be truncated easily (for example, binary files), AutoSupport omits the content.

You should modify the default size and time budgets only if asked to do so by NetApp Support. You can also review the default size and time budgets of the subsystems by using the `autosupport manifest show` command.

Files sent in event-triggered AutoSupport messages

Event-triggered AutoSupport messages only contain basic and troubleshooting information from subsystems that are associated with the event that caused AutoSupport to generate the message. The specific data helps NetApp support and support partners

troubleshoot the problem.

AutoSupport uses the following criteria to control content in event-triggered AutoSupport messages:

- Which subsystems are included

  Data is grouped into subsystems, including common subsystems, such as Log Files, and specific subsystems, such as RAID. Each event triggers a message that contains only the data from specific subsystems.

- The detail level of each included subsystem

  Data for each included subsystem is provided at a basic or troubleshooting level.

You can view all possible events and determine which subsystems are included in messages about each event using the `system node autosupport trigger show` command with the `-instance` parameter.

In addition to the subsystems that are included by default for each event, you can add additional subsystems at either a basic or a troubleshooting level using the `system node autosupport trigger modify` command.

Log files sent in AutoSupport messages

AutoSupport messages can contain several key log files that enable technical support staff to review recent system activity.

All types of AutoSupport messages might include the following log files when the Log Files subsystem is enabled:

Log file	Amount of data included from the file
• Log files from the `/mroot/etc/log/mlog/` directory • The MESSAGES log file	Only new lines added to the logs since the last AutoSupport message up to a specified maximum. This ensures that AutoSupport messages have unique, relevant—not overlapping—data. (Log files from partners are the exception; for partners, the maximum allowed data is included.)
• Log files from the `/mroot/etc/log/shelflog/` directory • Log files from the `/mroot/etc/log/acp/` directory • Event Management System (EMS) log data	The most recent lines of data up to a specified maximum.

The content of AutoSupport messages can change between releases of ONTAP.

Files sent in weekly AutoSupport messages

Weekly AutoSupport messages contain additional configuration and status data that is

useful to track changes in your system over time.

The following information is sent in weekly AutoSupport messages:

- Basic information about every subsystem
- Contents of selected `/mroot/etc` directory files
- Log files
- Output of commands that provide system information
- Additional information, including replicated database (RDB) information, service statistics, and more

How AutoSupport OnDemand obtains delivery instructions from technical support

AutoSupport OnDemand periodically communicates with technical support to obtain delivery instructions for sending, resending, and declining AutoSupport messages as well as uploading large files to the NetApp support site. AutoSupport OnDemand enables AutoSupport messages to be sent on-demand instead of waiting for the weekly AutoSupport job to run.

AutoSupport OnDemand consists of the following components:

- AutoSupport OnDemand client that runs on each node
- AutoSupport OnDemand service that resides in technical support

The AutoSupport OnDemand client periodically polls the AutoSupport OnDemand service to obtain delivery instructions from technical support. For example, technical support can use the AutoSupport OnDemand service to request that a new AutoSupport message be generated. When the AutoSupport OnDemand client polls the AutoSupport OnDemand service, the client obtains the delivery instructions and sends the new AutoSupport message on-demand as requested.

AutoSupport OnDemand is enabled by default. However, AutoSupport OnDemand relies on some AutoSupport settings to continue communicating with technical support. AutoSupport OnDemand automatically communicates with technical support when the following requirements are met:

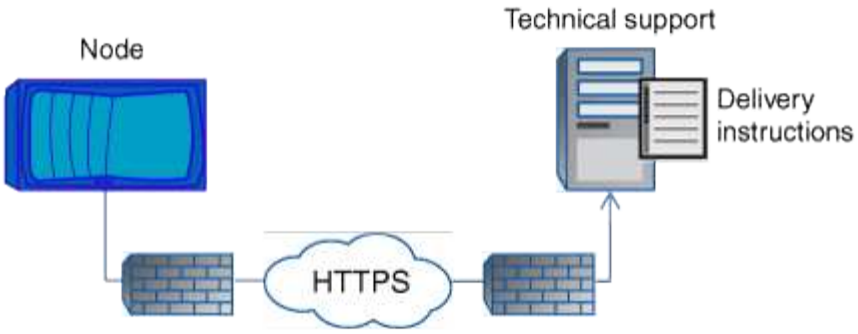
- AutoSupport is enabled.
- AutoSupport is configured to send messages to technical support.
- AutoSupport is configured to use the HTTPS transport protocol.

The AutoSupport OnDemand client sends HTTPS requests to the same technical support location to which AutoSupport messages are sent. The AutoSupport OnDemand client does not accept incoming connections.

AutoSupport OnDemand uses the “autosupport” user account to communicate with technical support. ONTAP prevents you from deleting this account.

If you want to disable AutoSupport OnDemand, but keep AutoSupport enabled, use the command: `system node autosupport modify -ondemand-state disable`.

The following illustration shows how AutoSupport OnDemand sends HTTPS requests to technical support to obtain delivery instructions.



The delivery instructions can include requests for AutoSupport to do the following:

- Generate new AutoSupport messages.

  Technical support might request new AutoSupport messages to help triage issues.

- Generate new AutoSupport messages that upload core dump files or performance archive files to the NetApp support site.

  Technical support might request core dump or performance archive files to help triage issues.

- Retransmit previously generated AutoSupport messages.

  This request automatically happens if a message was not received due to a delivery failure.

- Disable delivery of AutoSupport messages for specific trigger events.

  Technical support might disable delivery of data that is not used.

Structure of AutoSupport messages sent by email

When an AutoSupport message is sent by email, the message has a standard subject, a brief body, and a large attachment in 7z file format that contains the data.

If AutoSupport is configured to hide private data, certain information, such as the hostname, is omitted or masked in the header, subject, body, and attachments.

Subject

The subject line of messages sent by the AutoSupport mechanism contains a text string that identifies the reason for the notification. The format of the subject line is as follows:

HA Group Notification from *System_Name* (*Message*) *Severity*

- *System_Name* is either the hostname or the system ID, depending on the AutoSupport configuration

Body

The body of the AutoSupport message contains the following information:

- Date and timestamp of the message

- Version of ONTAP on the node that generated the message
- System ID, serial number, and hostname of the node that generated the message
- AutoSupport sequence number
- SNMP contact name and location, if specified
- System ID and hostname of the HA partnernode

Attached files

The key information in an AutoSupport message is contained in files that are compressed into a 7z file called `body.7z` and attached to the message.

The files contained in the attachment are specific to the type of AutoSupport message.

AutoSupport severity types

AutoSupport messages have severity types that help you understand the purpose of each message—for example, to draw immediate attention to an emergency problem, or only to provide information.

Messages have one of the following severities:

- **Alert**: Alert messages indicate that a next-higher level event might occur if you do not take some action.

  You must take an action against alert messages within 24 hours.

- **Emergency**: Emergency messages are displayed when a disruption has occurred.

  You must take an action against emergency messages immediately.

- **Error**: Error conditions indicate what might happen if you ignore.
- **Notice**: Normal but significant condition.
- **Info**: Informational message provides details about the issue, which you can ignore.
- **Debug**: Debug-level messages provide instructions you should perform.

If your internal support organization receives AutoSupport messages through email, the severity appears in the subject line of the email message.

Prepare to use 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 the HTTP or SMTP protocol. To improve security you can use TLS with HTTP. Beginning with ONTAP 9.15.1, you can also use TLS with SMTP.

Use HTTP with TLS (HTTPS) whenever possible.

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. See the command `system node autosupport modify` for more information.
- 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.

HTTP

This provides the most robust features. Note the following:

- AutoSupport OnDemand and the transfer of large files are supported.
- An HTTP 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 HTTP POST method is used instead.
- The default limit for HTTP transfers is 25 MB.
- The unsecured HTTP protocol uses port 80.

SMTP

As a general rule, you should use SMTP only if HTTPS/HTTP is not allowed or unsupported for some reason. 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 HTTP transfers is 5 MB.
- The unsecured SMTP protocol uses port 25.

Improve security with TLS

When using either HTTP or SMTP, all traffic is unencrypted and can be easily intercepted and read. When using HTTP, you should always configure the protocol to also use TLS (HTTPS).

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.

Ports for secure protocols

The following ports are typically used for the secure versions of these protocols:

- HTTPS - port 443

- SMTPS - port 587

Certificate validation

With TLS, 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. See Install the server certificate for more information.

Additional configuration considerations

There are a few additional considerations when configuring AutoSupport.

Sending 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 may 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

If you use TLS (HTTPS or SMTPS), you need to make sure 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. So in many cases, the certificate for your server will be immediately recognized by ONTAP without additional configuration. But depending on how the server certificate was signed, you may need to install a root CA certificate and any intermediate certificates.

Follow the instructions provided below to install the certificate if needed. You should install all the 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
   ```

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-----

   -----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 using one of the following:

   ```
   security certificate show-user-installed

   security certificate show
   ```

Set up 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.

3. If NetApp technical support is enabled to receive AutoSupport messages, specify which transport protocol to use for the 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 are sending messages to your internal support organization 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.

Upload core dump files

When a core dump file is saved, an event message is generated. If the AutoSupport service is enabled and configured to send messages to NetApp support, an AutoSupport message is transmitted, and an automated email acknowledgement is sent to you.

What you'll need

- You must have set up AutoSupport with the following settings:

- AutoSupport is enabled on the node.
- AutoSupport is configured to send messages to technical support.
- AutoSupport is configured to use the HTTP or HTTPS transport protocol.

  The SMTP transport protocol is not supported when sending messages that include large files, such as core dump files.

About this task

You can also upload the core dump file through the AutoSupport service over HTTPS by using the `system node autosupport invoke-core-upload` command, if requested by NetApp support.

How to upload a file to NetApp

Steps

1. View the core dump files for a node by using the `system node coredump show` command.

   In the following example, core dump files are displayed for the local node:

   ```
   cluster1::> system node coredump show -node local
   Node:Type Core Name Saved Panic Time
   --------- ------------------------------------------ -----
   -----------------
   node:kernel
   core.4073000068.2013-09-11.15_05_01.nz true 9/11/2013 15:05:01
   ```

2. Generate an AutoSupport message and upload a core dump file by using the `system node autosupport invoke-core-upload` command.

   In the following example, an AutoSupport message is generated and sent to the default location, which is technical support, and the core dump file is uploaded to the default location, which is the NetApp support site:

   ```
   cluster1::> system node autosupport invoke-core-upload -core-filename
   core.4073000068.2013-09-11.15_05_01.nz -node local
   ```

   In the following example, an AutoSupport message is generated and sent to the location specified in the URI, and the core dump file is uploaded to the URI:

   ```
   cluster1::> system node autosupport invoke-core-upload -uri
   https//files.company.com -core-filename
   core.4073000068.2013-09-11.15_05_01.nz -node local
   ```

Upload performance archive files

You can generate and send an AutoSupport message that contains a performance archive. By default, NetApp technical support receives the AutoSupport message, and the performance archive is uploaded to the NetApp support site. You can specify an alternate destination for the message and upload.

What you'll need

- You must have set up AutoSupport with the following settings:
  - AutoSupport is enabled on the node.
  - AutoSupport is configured to send messages to technical support.
  - AutoSupport is configured to use the HTTP or HTTPS transport protocol.

    The SMTP transport protocol is not supported when sending messages that include large files, such as performance archive files.

About this task

You must specify a start date for the performance archive data that you want to upload. Most storage systems retain performance archives for two weeks, enabling you to specify a start date up to two weeks ago. For example, if today is January 15, you can specify a start date of January 2.

Step

1. Generate an AutoSupport message and upload the performance archive file by using the `system node autosupport invoke-performance-archive` command.

   In the following example, 4 hours of performance archive files from January 12, 2015 are added to an AutoSupport message and uploaded to the default location, which is the NetApp support site:

   ```
   cluster1::> system node autosupport invoke-performance-archive -node
   local -start-date 1/12/2015 13:42:09 -duration 4h
   ```

   In the following example, 4 hours of performance archive files from January 12, 2015 are added to an AutoSupport message and uploaded to the location specified by the URI:

   ```
   cluster1::> system node autosupport invoke-performance-archive -node
   local -start-date 1/12/2015 13:42:09 -duration 4h -uri
   https://files.company.com
   ```

Get AutoSupport message descriptions

The descriptions of the AutoSupport messages that you receive are available through the ONTAP Syslog Translator.

Steps

1. Go to the Syslog Translator.
2. In the **Release** field, enter the the version of ONTAP you are using. In the **Search String** field, enter "callhome". Select **Translate**.
3. The Syslog Translator will alphabetically list all events that match the message string you entered.

Commands for managing AutoSupport

You use the `system node autosupport` commands to change or view AutoSupport configuration, display information about previous AutoSupport messages, and send, resend or cancel an AutoSupport message.

Configure AutoSupport

If you want to…	Use this command…
Control whether any AutoSupport messages are sent	`system node autosupport modify` with the `-state` parameter
Control whether AutoSupport messages are sent to technical support	`system node autosupport modify` with the `-support` parameter
Set up AutoSupport or modify the configuration of AutoSupport	`system node autosupport modify`
Enable and disable AutoSupport messages to your internal support organization for individual trigger events, and specify additional subsystem reports to include in messages sent in response to individual trigger events	`system node autosupport trigger modify`

Display information about the AutoSupport configuration

If you want to…	Use this command…
Display the AutoSupport configuration	`system node autosupport show` with the `-node` parameter
View a summary of all addresses and URLs that receive AutoSupport messages	`system node autosupport destinations show`
Display which AutoSupport messages are sent to your internal support organization for individual trigger events	`system node autosupport trigger show`
Display status of AutoSupport configuration as well as delivery to various destinations	`system node autosupport check show`

If you want to…	Use this command…
Display detailed status of AutoSupport configuration as well as delivery to various destinations	`system node autosupport check show-details`

Display information about past AutoSupport messages

If you want to…	Use this command…
Display information about one or more of the 50 most recent AutoSupport messages	`system node autosupport history show`
Display information about recent AutoSupport messages generated to upload core dump or performance archive files to the technical support site or a specified URI	`system node autosupport history show-upload-details`
View the information in the AutoSupport messages including the name and size of each file collected for the message along with any errors	`system node autosupport manifest show`

Send, resend, or cancel AutoSupport messages

If you want to…	Use this command…
Retransmit a locally stored AutoSupport message, identified by its AutoSupport sequence number If you retransmit an AutoSupport message, and if support already received that message, the support system will not create a duplicate case. If, on the other hand, support did not receive that message, then the AutoSupport system will analyze the message and create a case, if necessary.	`system node autosupport history retransmit`
Generate and send an AutoSupport message—for example, for testing purposes	`system node autosupport invoke` Use the `-force` parameter to send a message even if AutoSupport is disabled. Use the `-uri` parameter to send the message to the destination you specify instead of the configured destination.
Cancel an AutoSupport message	`system node autosupport history cancel`

Related information

ONTAP 9 Commands

Information included in the AutoSupport manifest

The AutoSupport manifest provides you with a detailed view of the files collected for each AutoSupport message. The AutoSupport manifest also includes information about collection errors when AutoSupport cannot collect the files it needs.

The AutoSupport manifest includes the following information:

- Sequence number of the AutoSupport message
- Which files AutoSupport included in the AutoSupport message
- Size of each file, in bytes
- Status of the AutoSupport manifest collection
- Error description, if AutoSupport failed to collect one or more files

You can view the AutoSupport manifest by using the `system node autosupport manifest show` command.

The AutoSupport manifest is included with every AutoSupport message and presented in XML format, which means that you can either use a generic XML viewer to read it or view it using the Active IQ (formerly known as My AutoSupport) portal.

AutoSupport case suppression during scheduled maintenance windows

AutoSupport case suppression enables you to stop unnecessary cases from being created by AutoSupport messages that are triggered during scheduled maintenance windows.

To suppress AutoSupport cases, you must manually invoke an AutoSupport message with a specially formatted text string: `MAINT=xh`. `x` is the duration of the maintenance window in units of hours.

Related information

How to suppress automatic case creation during scheduled maintenance windows

Troubleshoot AutoSupport when messages are not received

If the system does not send the AutoSupport message, you can determine whether that is because AutoSupport cannot generate the message or cannot deliver the message.

Steps

1. Check delivery status of the messages by using the `system node autosupport history show` command.
2. Read the status.

This status	Means
initializing	The collection process is starting. If this state is temporary, all is well. However, if this state persists, there is an issue.
collection-failed	AutoSupport cannot create the AutoSupport content in the spool directory. You can view what AutoSupport is trying to collect by entering the `system node autosupport history show -detail` command.
collection-in-progress	AutoSupport is collecting AutoSupport content. You can view what AutoSupport is collecting by entering the `system node autosupport manifest show` command.
queued	AutoSupport messages are queued for delivery, but not yet delivered.
transmitting	AutoSupport is currently delivering messages.
sent-successful	AutoSupport successfully delivered the message. You can find out where AutoSupport delivered the message by entering the `system node autosupport history show -delivery` command.
ignore	AutoSupport has no destinations for the message. You can view the delivery details by entering the `system node autosupport history show -delivery` command.
re-queued	AutoSupport tried to deliver messages, but the attempt failed. As a result, AutoSupport placed the messages back in the delivery queue for another attempt. You can view the error by entering the `system node autosupport history show` command.
transmission-failed	AutoSupport failed to deliver the message the specified number of times and stopped trying to deliver the message. You can view the error by entering the `system node autosupport history show` command.
ondemand-ignore	The AutoSupport message was processed successfully, but the AutoSupport OnDemand service chose to ignore it.

3. Perform one of the following actions:

For this status	Do this
initializing or collection-failed	Contact NetApp Support, because AutoSupport cannot generate the message. Mention the following Knowledge Base article: AutoSupport is failing to deliver: status is stuck in initializing

For this status	Do this
ignore, re-queued, or transmission failed	Check that destinations are correctly configured for SMTP, HTTP, or HTTPS because AutoSupport cannot deliver the message.

Troubleshoot AutoSupport message delivery over HTTP or HTTPS

If the system does not send the expected AutoSupport message and you are using HTTP or HTTPS, or the Automatic Update feature is not working, you can check a number of settings to resolve the problem.

What you'll need

You should have confirmed basic network connectivity and DNS lookup:

- Your node management LIF must be up for operational and administrative status.
- You must be able to ping a functioning host on the same subnet from the cluster management LIF (not a LIF on any of the nodes).
- You must be able to ping a functioning host outside the subnet from the cluster management LIF.
- You must be able to ping a functioning host outside the subnet from the cluster management LIF using the name of the host (not the IP address).

About this task

These steps are for cases when you have determined that AutoSupport can generate the message, but cannot deliver the message over HTTP or HTTPS.

If you encounter errors or cannot complete a step in this procedure, determine and address the problem before proceeding to the next step.

Steps

1. Display the detailed status of the AutoSupport subsystem:

   ```
   system node autosupport check show-details
   ```

   This includes verifying connectivity to AutoSupport destinations by sending test messages and providing a list of possible errors in your AutoSupport configuration settings.

2. Verify the status of the node management LIF:

   ```
   network interface show -home-node local -role node-mgmt -fields
   vserver,lif,status-oper,status-admin,address,role
   ```

   The `status-oper` and `status-admin` fields should return "up".

3. Record the SVM name, the LIF name, and the LIF IP address for later use.
4. Ensure that DNS is enabled and configured correctly:

   ```
   vserver services name-service dns show
   ```

5. Address any errors returned by the AutoSupport message:

   `system node autosupport history show -node * -fields node,seq-num,destination,last-update,status,error`

   For assistance troubleshooting any returned errors, see the ONTAP AutoSupport (Transport HTTPS and HTTP) Resolution Guide.

6. Confirm that the cluster can access both the servers it needs and the Internet successfully:

   a. `network traceroute -lif node-management_LIF -destination DNS server`

   b. `network traceroute -lif node_management_LIF -destination support.netapp.com`

      The address `support.netapp.com` itself does not respond to ping/traceroute, but the per-hop information is valuable.

   c. `system node autosupport show -fields proxy-url`

   d. `network traceroute -node node_management_LIF -destination proxy_url`

   If any of these routes are not functioning, try the same route from a functioning host on the same subnet as the cluster, using the “traceroute” or “tracert” utility found on most third-party network clients. This assists you in determining whether the issue is in your network configuration or your cluster configuration.

7. If you are using HTTPS for your AutoSupport transport protocol, ensure that HTTPS traffic can exit your network:

   a. Configure a web client on the same subnet as the cluster management LIF.

      Ensure that all configuration parameters are the same values as for the AutoSupport configuration, including using the same proxy server, user name, password, and port.

   b. Access `https://support.netapp.com` with the web client.

      The access should be successful. If not, ensure that all firewalls are configured correctly to allow HTTPS and DNS traffic, and that the proxy server is configured correctly. For more information on configuring static name resolution for support.netapp.com, see the Knowledge Base article How would a HOST entry be added in ONTAP for support.netapp.com?

8. Beginning with ONTAP 9.10.1, if you enabled the Automatic Update feature, ensure you have HTTPS connectivity to the following additional URLs:
   - https://support-sg-emea.netapp.com
   - https://support-sg-naeast.netapp.com
   - https://support-sg-nawest.netapp.com

Troubleshoot AutoSupport message delivery over SMTP

If the system cannot deliver AutoSupport messages over SMTP, you can check a number of settings to resolve the problem.

What you’ll need

You should have confirmed basic network connectivity and DNS lookup:

- Your node management LIF must be up for operational and administrative status.
- You must be able to ping a functioning host on the same subnet from the cluster management LIF (not a LIF on any of the nodes).
- You must be able to ping a functioning host outside the subnet from the cluster management LIF.
- You must be able to ping a functioning host outside the subnet from the cluster management LIF using the name of the host (not the IP address).

About this task

These steps are for cases when you have determined that AutoSupport can generate the message, but cannot deliver the message over SMTP.

If you encounter errors or cannot complete a step in this procedure, determine and address the problem before proceeding to the next step.

All commands are entered at the ONTAP command-line interface, unless otherwise specified.

Steps

1. Verify the status of the node management LIF:

   network interface show -home-node local -role node-mgmt -fields vserver,lif,status-oper,status-admin,address,role

   The `status-oper` and `status-admin` fields should return `up`.

2. Record the SVM name, the LIF name, and the LIF IP address for later use.
3. Ensure that DNS is enabled and configured correctly:

   vserver services name-service dns show

4. Display all of the servers configured to be used by AutoSupport:

   system node autosupport show -fields mail-hosts

   Record all server names displayed.

5. For each server displayed by the previous step, and `support.netapp.com`, ensure that the server or URL can be reached by the node:

   network traceroute -node local -destination *server_name*

   If any of these routes is not functioning, try the same route from a functioning host on the same subnet as the cluster, using the “traceroute” or “tracert” utility found on most third-party network clients. This assists you in determining whether the issue is in your network configuration or your cluster configuration.

6. Log in to the host designated as the mail host, and ensure that it can serve SMTP requests:

   netstat -aAn|grep 25

   `25` is the listener SMTP port number.

   A message similar to the following text is displayed:

```
ff64878c tcp        0      0  *.25    *.*    LISTEN.
```

7. From some other host, open a Telnet session with the SMTP port of the mail host:

   telnet *mailhost* 25

   A message similar to the following text is displayed:

```
220 filer.yourco.com Sendmail 4.1/SMI-4.1 ready at Thu, 30 Nov 2014
10:49:04 PST
```

8. At the telnet prompt, ensure that a message can be relayed from your mail host:

   HELO *domain_name*

   MAIL FROM: *your_email_address*

   RCPT TO: autosupport@netapp.com

   `domain_name` is the domain name of your network.

   If an error is returned saying that relaying is denied, relaying is not enabled on the mail host. Contact your system administrator.

9. At the telnet prompt, send a test message:

   DATA

   SUBJECT: TESTING THIS IS A TEST

   .

   Ensure that you enter the last period (.) on a line by itself. The period indicates to the mail host that the message is complete.

   If an error is returned, your mail host is not configured correctly. Contact your system administrator.

10. From the ONTAP command-line interface, send an AutoSupport test message to a trusted email address that you have access to:

    system node autosupport invoke -node local -type test

11. Find the sequence number of the attempt:

    system node autosupport history show -node local -destination smtp

    Find the sequence number for your attempt based on the timestamp. It is probably the most recent attempt.

12. Display the error for your test message attempt:

system node autosupport history show -node local -seq-num seq_num -fields error

If the error displayed is `Login denied`, your SMTP server is not accepting send requests from the cluster management LIF. If you do not want to change to using HTTPS as your transport protocol, contact your site network administrator to configure the SMTP gateways to address this issue.

If this test succeeds but the same message sent to mailto:autosupport@netapp.com does not, ensure that SMTP relay is enabled on all of your SMTP mail hosts, or use HTTPS as a transport protocol.

If even the message to the locally administered email account does not succeed, confirm that your SMTP servers are configured to forward attachments with both of these characteristics:

- The “7z” suffix
- The “application/x-7x-compressed” MIME type.

Troubleshoot the AutoSupport subsystem

The `system node check show` commands can be used to verify and troubleshoot any issues related to the AutoSupport configuration and delivery.

Step

1. Use the following commands to display the status of the AutoSupport subsystem.

Use this command…	To do this…
system node autosupport check show	Display overall status of the AutoSupport subsystem, such as the status of AutoSupport HTTP or HTTPS destination, AutoSupport SMTP destinations, AutoSupport OnDemand Server, and AutoSupport configuration
system node autosupport check show-details	Display detailed status of the AutoSupport subsystem, such as detailed descriptions of errors and the corrective actions

Copyright information

Trademark information