



Technical Report

# AutoSupport and AutoSupport On Demand Configuration

Brett Albertson, NetApp  
August 2023 | TR-4444

## Abstract

This guide is intended to assist customers, partners, and NetApp in configuring AutoSupport™ and AutoSupport On Demand™ on NetApp® storage systems.

For feedback or questions please email [ng-activeiq-feedback@netapp.com](mailto:ng-activeiq-feedback@netapp.com)

## TABLE OF CONTENTS

<b>Introduction .....</b>	<b>3</b>
AutoSupport .....	3
Benefits of AutoSupport .....	3
Managing AutoSupport in Data ONTAP .....	4
<b>Active IQ Digital Advisor .....</b>	<b>6</b>
<b>AutoSupport On Demand .....</b>	<b>7</b>
AutoSupport On Demand Benefits .....	7
AutoSupport On Demand Security .....	7
<b>Configuring AutoSupport in Data ONTAP .....</b>	<b>9</b>
Setting up AutoSupport in Data ONTAP .....	10
Testing the AutoSupport Configuration .....	14
<b>Configuring AutoSupport in E-Series .....</b>	<b>15</b>
<b>Configuring AutoSupport in StorageGRID .....</b>	<b>15</b>
<b>Configuring AutoSupport in SolidFire and HCI .....</b>	<b>15</b>
<b>Troubleshooting AutoSupport in Data ONTAP .....</b>	<b>16</b>
Troubleshooting AutoSupport When Messages Are Not Received .....	16
Troubleshooting AutoSupport over HTTPS .....	16
Troubleshooting AutoSupport over SMTP .....	17
Truncated Content in AutoSupport (AutoSupport Budgets) .....	19
NetApp does not receive AutoSupport messages sent through HTTPS with certificate validation enabled .....	22
<b>Additional Information .....</b>	<b>24</b>
<b>Version History .....</b>	<b>24</b>

## LIST OF TABLES

Table 1) AutoSupport messages. ....	5
-------------------------------------	---

## LIST OF FIGURES

Figure 1) Active IQ Digital Advisor main dashboard .....	6
Figure 2) AutoSupport On Demand data flow .....	8
Figure 3) HTTPS encrypted communication diagram .....	23

# Introduction

AutoSupport™ (ASUP™) is a mechanism that sends messages containing telemetry data to NetApp. This data enables many tools, support use-cases, and other data workflows including support case automation. Enabling AutoSupport on your system provides foundational data for support tools designed to expedite support case resolution and maximize your system's uptime.

Although AutoSupport messages to technical support are enabled by default, you always have the choice to disable it. You can set the options such as transport method and copying the messages to your internal support organization or a partner support organization.

This document covers the steps required to configure AutoSupport and AutoSupport On Demand on ONTAP-based storage systems. It also contains links for other NetApp storage system types.

## AutoSupport

AutoSupport is a feature of NetApp® storage operation systems such as the Data ONTAP® operating system software, providing the data for an integrated, efficient monitoring and reporting capability and supporting data collection. AutoSupport provides the capability to send system health status messages directly to NetApp, partners, and your own company. In the event of a support incident, information is automatically sent to NetApp and other designated destinations for quick incident resolution. AutoSupport also sends periodic diagnostic data back to NetApp where it is automatically analyzed for known issues or risks that may affect future system stability and performance. One of the main tools for customers to access this data is Active IQ Digital Advisor which includes predictive and proactive recommendations using AI and Machine Learning techniques. Active IQ Digital Advisor is NetApp's main AIOps platform and all of it works via analyzing AutoSupport data.

## Benefits of AutoSupport

Unless otherwise prohibited by data security policy, AutoSupport should be enabled as a NetApp best practice. In fact, enabling AutoSupport enhances security by auditing your existing security risks and warning you about potential attack vectors. There are many specific benefits for enabling and maintaining consistent AutoSupport functionality.

Some of those benefits are:

- Automated call home function regarding critical events — support cases for critical events are opened automatically, such as a request for hardware replacement
- Nonintrusive alerting to notify you of a problem and provide information so that NetApp can take corrective action
- Message monitoring by analysis tools such as Active IQ Digital Advisor and BlueXP for known configuration issues
- Ongoing health check analyses of hundreds of system parameters and intelligent linking of detected issues to solution information
- Handling of Return Merchandise Authorization (RMA) requests without customer action
- Sending of system alerts to NetApp and customer contacts
- Powering tools such as Active IQ, BlueXP, and System Manager
- Enabling workflows such as support renewals, add-ons, and tech refresh activities

It is important to remember that even if you cannot send the AutoSupport data to NetApp, it is still a key element for any support issue. In the event a support case is opened, NetApp support will request that an AutoSupport message be manually retransmitted or forwarded to expedite troubleshooting.

## Managing AutoSupport in Data ONTAP

In ONTAP, only the cluster administrator can perform AutoSupport management. The storage virtual machine (SVM) administrator has no access to AutoSupport.

AutoSupport can be disabled at any time, but it is recommended to leave it enabled. Enabling AutoSupport can significantly expedite problem determination and resolution should a problem occur on the storage system. By default, the system collects AutoSupport information and stores it locally, even if you disable AutoSupport.

While configuring the storage for the first time, AutoSupport is enabled by default. AutoSupport begins to send messages to NetApp support 24 hours after the system is first turned on. You can decrease the 24-hour period by upgrading or reverting the system, modifying the AutoSupport configuration, or changing the system time to something other than a 24-hour period.

AutoSupport sends messages to recipients depending on the type of message. Learning when and where AutoSupport sends messages can help understand messages that are received through e-mail or viewed on Active IQ Digital Advisor.

Active IQ Digital Advisor is a web-based application that is part of the NetApp support site. It aggregates AutoSupport messages received from systems and provides recommendations and views to help improve system availability and efficiency. For more information, see the [Active IQ Digital Advisor documentation](#).

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

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

1. When the Event Management System (EMS) of a node processes a trigger event, EMS sends a request to the AutoSupport module.  
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 with the `system node autosupport modify` command, using 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.

AutoSupport also sends several messages on a regular schedule. You can manually initiate or resend an AutoSupport message. NetApp technical support can request messages from AutoSupport using the AutoSupport On Demand feature.

Table 1 shows types of AutoSupport messages and their content.

**Table 1) AutoSupport messages.**

Type of Message	Type of Data the Message Contains
Event-triggered	Files containing context-sensitive data about the specific subsystems related to the event.
Daily	Log files.
Performance	Performance data sampled during the previous 24 hours.
Weekly	Configuration and status data.
Triggered by the <code>system node autosupport invoke</code> command	<p>Depends on the value specified by the <code>-type</code> parameter:</p> <ul style="list-style-type: none"> <li><code>test</code> sends a user-triggered message with some basic data. This message also triggers an automated e-mail response from technical support to any specified e-mail addresses, using the <code>-to</code> option, so that you can confirm that AutoSupport messages are being received.</li> <li><code>performance</code> sends performance data.</li> <li><code>all</code> sends a user-triggered message with a complete set of data, including troubleshooting data from each subsystem. Technical support typically requests this message.</li> </ul>
Triggered by the <code>system node autosupport invoke-core-upload</code> command	<p>Core dump file for a node.</p> <p>There is an option to invoke this command with a NetApp Support case number. By providing the case number, the uploaded core dump file is associated with the correct technical case and expedites problem resolution.</p> <p><b>Example:</b></p> <pre>cluster1::&gt; system node autosupport invoke-coredump -core-filename core.4070309011.2014-12-20.17_06_03.nz -message "Latest core of problem" -case-number 2006123456</pre>
Triggered by the <code>system node autosupport invoke-performance-archive</code> command	<p>Performance archive files for a specified period.</p> <p>There is an option to invoke this command with a case number. By providing the case number, the uploaded performance archive is associated with the correct technical case and expedites problem resolution.</p> <pre>cluster1::&gt; system node autosupport invoke-performance-archive -start-date 12/20/2014 19:19:47 -end-date 12/20/2014 25:00:00 -message "Some perf date for 12/20" -case-number 2006123456</pre>
Triggered by NetApp Support using AutoSupport On Demand	<p>AutoSupport On Demand can retransmit failed messages and relay remote instructions that are equivalent to AutoSupport invoke commands offered through CLI:</p> <ul style="list-style-type: none"> <li><code>system node autosupport invoke</code></li> <li><code>system node invoke-performance-archive</code></li> <li><code>system node autosupport invoke-core-upload</code></li> <li><code>system node invoke-diagnostic</code> (in diag mode)</li> </ul>

# Active IQ Digital Advisor

Active IQ Digital Advisor is a web-based application that uses information from AutoSupport and other data sources to provide predictive and proactive insights to help improve availability, efficiency, and performance.

It is important to continually monitor the Active IQ Digital Advisor portal and check for systems that do not send support information, because this is critical information for expediting support issue resolution. The proactive and predictive nature of AutoSupport provides the capability to avoid or minimize risks and issues before they occur.

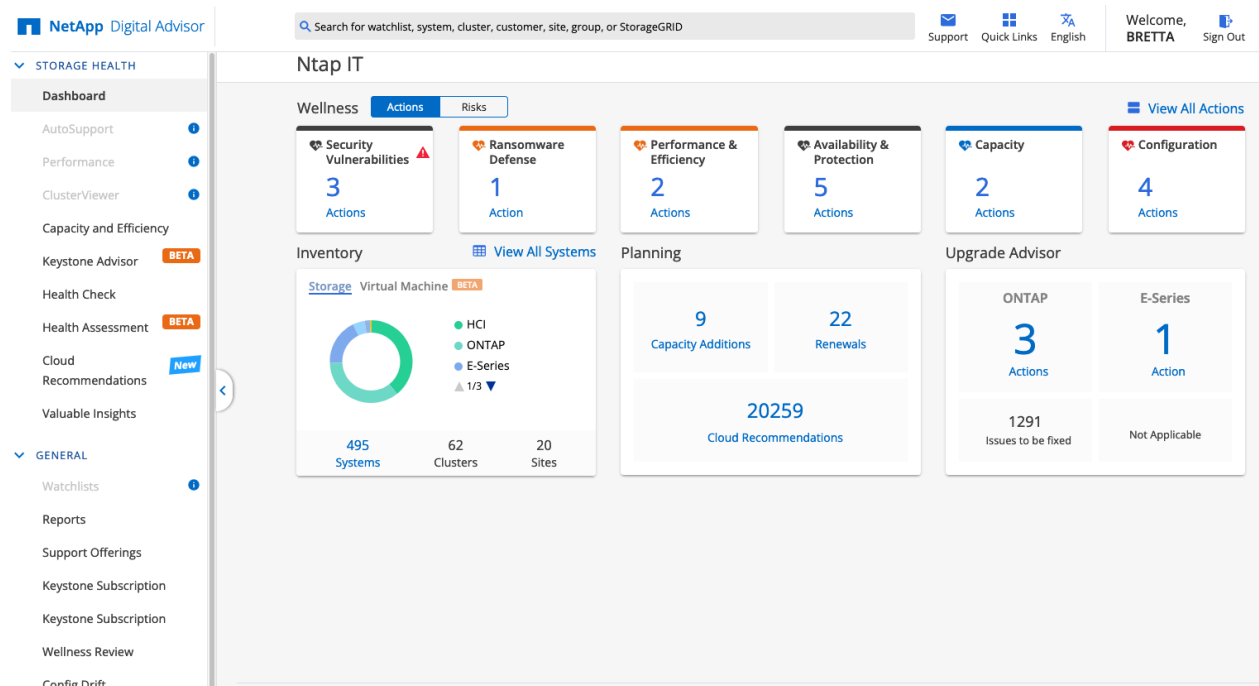
Your system must have AutoSupport enabled and configured so that it can send data back to NetApp.

Benefits of Active IQ Digital Advisor:

- Can view a node, a cluster, a site, a customer, or a grouping of those called a watchlist
- Predicts storage capacity growth to identify capacity addition needs
- Recommends upgrade needs for ONTAP systems and provides upgrade plans
- Proactively identifies system risks related to a configuration issue or known bugs
- Provides configuration, capacity, efficiency, and performance views and reports for better management of your NetApp systems
- Generates reports

You can access Active IQ Digital Advisor by going to <https://activeiq.netapp.com/>

Figure 1) Active IQ Digital Advisor main dashboard



Provide a NetApp storage serial number/system ID or site name in the search box. It opens the dashboard with latest the AutoVirtual information received by NetApp.

# AutoSupport On Demand

AutoSupport On Demand (AOD) is a capability that allows NetApp to collect AutoSupport information to troubleshoot cases without the need for customer intervention. AutoSupport On Demand enables AutoSupport messages to be sent on-demand, instead of waiting for a periodic AutoSupport message.

The AutoSupport On Demand solution is an integral part of the Data ONTAP AutoSupport capability. Data ONTAP storage systems configured for HTTPS AutoSupport delivery periodically communicate with technical support to obtain AutoSupport On Demand delivery instructions for sending, resending, and declining AutoSupport messages.

## AutoSupport On Demand Benefits

Improves customer support experience

- Reduces customer time and overhead while gathering diagnostics for troubleshooting
- Requires minimal customer configuration

Expedites NetApp case resolution

- Ensures availability of up-to-date diagnostic and configuration information
- NetApp Support and Support Partners can obtain all the information needed, even during customer off-hours, without customer involvement
- Enhances AutoSupport reliability by allowing retransmission of ASUPs lost due to transient network or delivery issues

## AutoSupport On Demand Security

AutoSupport On Demand is seamlessly and securely integrated into the NetApp AutoSupport capability:

- All On Demand instructions are transferred through encrypted HTTPS in response to queries from the storage system (outbound communication only).
- On Demand enables a limited set of predefined AutoSupport instructions:
  - Request collection of new AutoSupport data to determine current system state.
  - Request more in-depth AutoSupport data when needed to resolve complex cases (diagnostic ASUP messages, core files, and performance archives).
- On Demand is restricted to users with valid NetApp Support site credentials and appropriate business roles (technical support engineers, support account managers, and support partners authorized to work on a given storage system).
- On Demand usage transparency:
  - Customers can review and execute all predefined delivery instructions using Data ONTAP CLI.
  - If configured, customers and partners receive a copy of the AutoSupport message
  - On Demand usage is tracked and displayed:
    - On Demand requests are logged in daily management log AutoSupport messages.
    - Resulting AutoSupport messages contain On Demand in the title and can be viewed through Active IQ.

## AutoSupport On Demand Operation

AutoSupport On Demand consists of the following components:

- AutoSupport On Demand client that runs on each node

- AutoSupport On Demand service that resides at NetApp technical support

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

AutoSupport On Demand is enabled by default on systems that meet the minimal product configuration requirements, which include:

- AutoSupport is enabled.
- AutoSupport is configured to send messages to technical support using the HTTPS transport protocol.
- Storage controller is running ONTAP 8.2 or later.

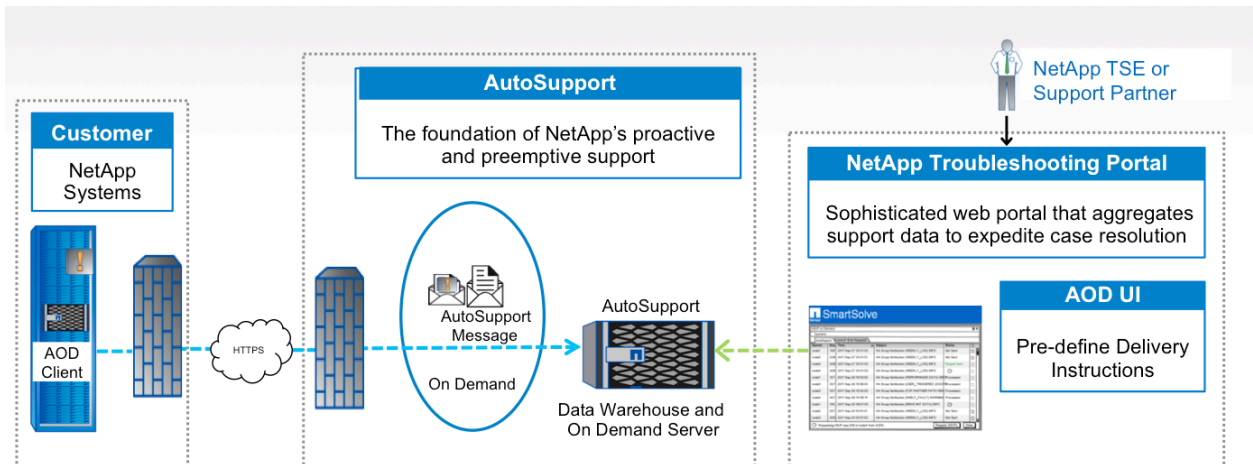
The AutoSupport On Demand client sends HTTPS requests to the same technical support location to which AutoSupport messages are sent. The AutoSupport On Demand client does not accept incoming connections.

**Note:** AutoSupport On Demand uses a pre-defined "autosupport" local user account to facilitate administration of AutoSupport on Demand features. ONTAP prevents you from deleting this account.

If you want to disable AutoSupport On Demand but keep AutoSupport enabled and configured to send messages to technical support by using the HTTPS transport protocol, contact technical support for assistance.

Figure 3 shows how AutoSupport On Demand sends HTTPS requests to technical support to obtain delivery instructions.

**Figure 2) AutoSupport On Demand data flow**



AutoSupport On Demand available for Data ONTAP® 8.2 + systems and HTTPS only

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 (Retransmits can be requested manually or automatically if a message was not received due to a delivery failure or On Demand deferral).
- Defer delivery of AutoSupport messages for specific trigger events (Technical support might disable delivery of certain types of AutoSupport data that is rarely needed or redundant).

## Configuring AutoSupport in Data ONTAP

This chapter details how to set up AutoSupport on a Data ONTAP system and covers basic system requirements.

### AutoSupport Requirements

Use HTTPS for delivery of AutoSupport messages to provide the best security and to support all the latest AutoSupport features. Although AutoSupport supports SMTP for delivery of AutoSupport messages, HTTPS is recommended.

**Note:** The use of HTTP has been deprecated.

### Supported Protocols

#### HTTPS

HTTPS uses TCP port 443. This protocol is the default transport protocol. This protocol supports AutoSupport On Demand and uploads of large files.

When AutoSupport messages are sent using HTTPS, the X.509 certificate of the NetApp AutoSupport server is validated, and the message content is encrypted.

NetApp strongly recommends using HTTPS transport for AutoSupport delivery for the following reasons:

- HTTPS transport is significantly more secure and reliable than SMTP
- HTTPS is not restricted by SMTP e-mail size constraints
- HTTPS is easy to configure and manage
- HTTPS transport can be used along with SMTP delivery to internal customer personnel or systems
- HTTPS enables integrated AutoSupport On Demand capability to expedite case resolution

#### SMTP

- SMTP uses TCP port 25. You can configure AutoSupport to use a different port.
- This protocol should be used only if network connection does not allow HTTPS.
- This protocol does not support uploads of large files and AutoSupport On Demand.
- Although SMTP data is not encrypted by the node, most modern mail servers do encrypt SMTP messages going outside of the company. NetApp supports receiving encrypted SMTP.
- SMTP infrastructure imposes greater limitations on message size.

### External Mail Server

If you use SMTP to send AutoSupport messages either to your internal support organization or to technical support, you must configure an external mail server. The storage system does not function as a mail server; it requires an external mail server at your site to send mail. The mail server must be a host that listens on the SMTP port (25) or another port, and it must be configured to send and receive 8-bit

Multipurpose Internet Mail Extensions (MIME) encoding. Example mail hosts include a UNIX host running an SMTP server such as the sendmail program and a Windows server running the Microsoft Exchange server. You can have one or more mail hosts.

If AutoSupport is configured with specific e-mail addresses for an internal support organization or a support partner organization, those messages are always sent by SMTP. For example, if you use the recommended HTTPS protocol to send messages to technical support and you also want to send messages to your internal support organization, your messages are transported using both HTTPS and SMTP, respectively.

## AutoSupport Payload

AutoSupport limits the maximum file size for each protocol. The default setting for HTTPS transfers is 50MB (ONTAP 9 and later) or 10MB (Data ONTAP 8.3 and earlier). The default setting for SMTP transfers is 5MB. If the size of the AutoSupport message exceeds the configured limit, AutoSupport delivers as much of the message as possible. AutoSupport automatically overrides the maximum size limit for the HTTPS protocol when you generate and send AutoSupport messages that upload core dump or performance archive files to the NetApp Support site or a specified URL.

## Setting up AutoSupport in Data ONTAP

This section provides the steps to set up AutoSupport on NetApp AFF, FAS, ASA, CVO, FlexArray, and V-Series storage controllers.

### Configuring DNS

DNS must be configured to resolve NetApp's AutoSupport HTTP/S destination URLs and if you use host names instead of IP addresses.

#### On ONTAP

1. Enable DNS on the cluster.

```
vserver services name-service dns create -vserver cluster_name -domains domainname -
name-servers ip_address -state enabled
```

### Allowing ONTAP IP Addresses through your Firewall (if applicable)

1. For ONTAP AutoSupport messages to NetApp via HTTPS, allow all node-mgmt and cluster-mgmt Logical Interfaces (LIFs) on ONTAP clusters.
2. Service Processor AutoSupport messages are sent via SMTP only.
3. For ONTAP AutoSupport messages via SMTP, they need to reach your local SMTP gateway and be allowed to send e-mail to [autosupport@netapp.com](mailto:autosupport@netapp.com).

## Making Sure AutoSupport Is Enabled

Enable AutoSupport to receive AutoSupport messages.

#### On ONTAP

1. Set the `-state` parameter of the `system node autosupport modify` command to `enable`.

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

2. If you want technical support to receive AutoSupport messages, set the `-support` parameter of the `system node autosupport modify` command to `enable`.

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

You must enable this option if you want to enable AutoSupport to work with AutoSupport On Demand or if you want to upload large files, such as core dump and performance archive files, to technical support or a specified URL. These commands need to be repeated on all nodes of the cluster. As new nodes join the cluster, it is important that their AutoSupport configuration match the existing nodes.

## Specifying Transport Protocol for Messages

Specify the transport protocol to be used by AutoSupport to send AutoSupport messages.

### On ONTAP

1. HTTPS is the default protocol. Use SMTP only if the network connection does not allow HTTPS. Set the transport protocol using the `-transport` parameter.

```
system node autosupport modify -node nodename -transport protocol
```

2. If you choose HTTPS as the transport protocol and you use a proxy, set `-proxy-url` to the URL of the proxy.

```
system node autosupport modify -node nodename -proxy-url proxyurl
```

These commands need to be repeated on all nodes of the cluster. As new nodes join the cluster, it is important that their AutoSupport configuration match the existing nodes.

## Specifying Proxy Configuration details for HTTPS Systems

If the `-transport` parameter is set to HTTPS and your organization uses a proxy.

Use the `-proxy-url` parameter to specify an HTTP or HTTPS proxy

Format: `[-proxy-url <text>]` - Support Proxy URL:Port

Example:

```
system node autosupport modify -node nodename -proxy-url proxyurl:8080
```

### Note:

- Enter the URL without an `http://` or `https://` prefix
  - HTTP uses TCP port 80
  - NetApp recommends that customers use a **HTTP/1.1** compliant proxy. Customers that use an older HTTP/1.0 proxy might require additional configuration to enable the AutoSupport On Demand capability to overcome incompatibilities related to transfer encoding headers.
- If proxy authentication is also required, include the username and password in the URL:  
Format: `"[username]:[password]@[host]:[port]"`

```
system node autosupport modify -node nodename -proxy-url user1:mypass@proxyurl:8080
```

- If unspecified, the default password is an empty string. To specify a proxy that contains a question mark, press ESC followed by the `"?"`.
- In Data ONTAP 8.3 and earlier, password in both "autosupport show" and "options autosupport" output is in plaintext.
- In ONTAP 9.0 and later, password entry uses the secure (enter it twice) interactive method. In addition, "\*\*\*\*\*" password in the URL text is displayed in various cluster shell CLI commands (autosupport show, autosupport check show).
- In ONTAP 9.0 and later, AutoSupport options are entirely removed from "options" output in nodeshell/dBlade CLI.

For example:

```
Support URL for HTTP/S PUT: support.netapp.com/put/AsupPut
Support Proxy URL: andris:*****@proxy.netapp.com:8080
Support Address: autosupport@netapp.com
```

## Configuring Mail Server for SMTP Transport

Configure an e-mail server name or IP address that can route e-mail-based messages from the storage node. This configuration is required for internal support organization or support partners to receive AutoSupport messages or if you use SMTP as the transport protocol to NetApp.

### On ONTAP

1. Configure a mail host using the following command. You can configure a port value for each mail host by specifying a colon and port number after the mail host name. You can set up to five mail hosts.

```
system node autosupport modify -node nodename -mail-hosts mailhost:port
```

2. Set the `-from` e-mail address that sends the AutoSupport message.
3. Set `-to`, `-noteto`, and `-partner-address` parameters to set e-mail addresses that receive AutoSupport messages. `-noteto` recipients receive a shortened version of key AutoSupport messages designated for cell phones and other mobile devices. Up to five e-mail addresses can be provided for each parameter.
4. Check the addresses are correctly configured by listing destinations with the following command.

```
system node autosupport destinations show
```

## Configuring Additional AutoSupport Options

### On ONTAP

1. To hide private data by removing, masking, or encoding sensitive data in the messages, set `-remove-private-data` to `true`. If you change it from `false` to `true`, all AutoSupport history and all associated files are deleted.
2. To stop sending periodic performance AutoSupport messages, set `-perf` to `false`.

#### Note:

- Limiting AutoSupport content and disabling Performance data is not recommended as all the AutoSupport content is used for monitoring and troubleshooting by various NetApp tools.
- If "minimal/remove-private-data" is enabled, hourly performance data is NOT sent in Performance Data/Snapshot AutoSupports.
- If "minimal/remove-private-data" is enabled, this setting cannot be overridden by manual AutoSupport or AutoSupport On Demand invocations.

## Performance Archives: Performance first failure data collection for ONTAP 8.3 and later

Beginning with ONTAP 8.3, performance content is collected and stored ('archived') on every system by default. This content is built on top of a new functionality in Data ONTAP, which automatically stores Quality of Service performance statistics on a per-volume basis for diagnostic purposes for up to 28 days

on each Data ONTAP node.

Using the AutoSupport infrastructure, a Performance Archive can be created and uploaded to NetApp.

EMS events will report the following message if the Performance Archive is disabled.

To enable Performance Archive, contact technical support for assistance.

```
::*> event log show -event perf*
Time                Node                Severity      Event
-----
INFORMATIONAL perf.ccma.off: Performance archiver is not enabled.
```

### Uploading Performance Archive

Run the 'system node autosupport invoke-performance-archive' sub-command with the following options:

```
-start-date <"MM/DD/YYYY HH:MM:SS">
-duration <[<integer>h][<integer>m][<integer>s]> (or -end-date)
-node *
-case-number <text>
```

Note that the maximum duration for any single collection is 6 hours and the recommended sample period is 4 hours. Performance Archives can only be uploaded via HTTP/HTTPS. SMTP is not currently supported as an upload method for Performance Archives. Performance Archives can also be requested for support troubleshooting using AutoSupport On Demand.

## Checking Overall AutoSupport Configuration

### In ONTAP

Run the following command to check the overall configuration. The command should report the same values for all nodes in the cluster.

```
cluster1::> system node autosupport show -node nodename -instance
Node: node1
State: enable
SMTP Mail Hosts: mailhost
From Address: Postmaster
List of To Addresses: me@itsupport.com
List of Noteto Addresses: alerts@itsupport.com
List of Partner Addresses: -
Send AutoSupport Messages to Vendor Support: enable
Protocol to Contact Support: https
Support URL for HTTP/HTTPS: support.netapp.com/asupprod/post/1.0/postAsup
Support URL for HTTP/S PUT: support.netapp.com/put/AsupPut
Support Proxy URL:
Support Address: autosupport@netapp.com
Hostname Subject: false
NHT Enable: true
Performance Data Enable: true
Retry Interval: 4m
Retry Count: 15
Reminder Enable: true
Last Subject Sent: MANAGEMENT_LOG
Last Time Sent: 9/17/2017 00:25:09
Maximum HTTP Size: 50MB
Maximum SMTP Size: 5MB
Remove Sensitive Data: false
```

## Testing the AutoSupport Configuration

Once configured, test AutoSupport to make sure everything is working properly. If a test AutoSupport message is sent to NetApp, an e-mail is sent back to the destination addresses specified in the `autosupport.to/-to` parameter to verify that the message is received. If you do not receive the confirmation e-mail from NetApp or NetApp did not receive the message, perform the troubleshooting task for blocked network ports or access policies relative to the transport protocol (HTTPS or SMTP) in use to resolve the problem.

### In ONTAP

1. If you are running ONTAP 8.3 or later, run `system node autosupport check show` to check the AutoSupport configuration.
2. Use the `system node autosupport invoke` command with the `-type` parameter set to `test`.

```
system node autosupport invoke -type test -node nodename -message Test
```

3. Confirm that NetApp is receiving your AutoSupport messages by checking the e-mail address that are specified in the `-to` parameter, who should have received an automated response from the NetApp mail handler. Additionally, log into Active IQ to confirm reception.

```
system node autosupport history -node nodename
```

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

4. **Optional:** Confirm that the AutoSupport message is being sent to your internal support organization or to your support partner by checking the e-mail of any address that you configured for the `-to`, `-noteto`, or `-partner-address` parameters of the `system node autosupport modify` command.

### Sample Test AutoSupport Email Message

```
+++++
Dear NetApp Customer,

This email is sent to acknowledge the receipt of the AutoSupport email from:

System ID: ##SYSID
Hostname: ##HOSTNAME
The AutoSupport had the following subject line:
##ASUPSUBJECT
```

## AutoSupport configuration recommendation through Active IQ

HTTPS is the recommended protocol for using AutoSupport. If AutoSupport on the storage controller is set up with another protocol, Active IQ shows the best practice and corrective action steps under Health Check.

Users can view this information at the single system level, cluster level, or at aggregated levels (customer, site, and group) through the Health Check in Active IQ.

## Decommission/Decline AutoSupport

The following process describes the steps necessary to decline and decommission systems that are no longer in use.

- Identify the storage system serial number for the system you are decommissioning or declining AutoSupport. For a large list of serial numbers, open a nontechnical case on the NetApp Support site and attach the list of serial numbers.
- Log in to the NetApp Support site.
- Select the My Support tab.
- Click Systems => then View Installed Products.
- Enter the serial number of the system.

**To decline AutoSupport:**

- Leave the selection on Manage Product Location & Details and click Go.
- In the Configuration Details section, select Update Configuration Details.
- Choose the reason you are declining AutoSupport from the drop-down menu.
- Click Confirm Data Submit Changes.

**To decommission:**

- From the Manage Product Location & Details drop-down menu, select Decommission this system and click Go.
- Complete the information on the Decommission Form and click Submit.

## Configuring AutoSupport in E-Series

For a complete guide to AutoSupport on E-Series, please see the following document:

[https://kb.netapp.com/onprem/E-Series/Management\\_Apps/How\\_to\\_enable\\_AutoSupport\\_on\\_E-Series\\_SANtricity\\_System\\_Manager](https://kb.netapp.com/onprem/E-Series/Management_Apps/How_to_enable_AutoSupport_on_E-Series_SANtricity_System_Manager)

## Configuring AutoSupport in StorageGRID

For a guide to configuring AutoSupport on StorageGRID see this documentation:

<https://docs.netapp.com/us-en/storagegrid-117/admin/configure-autosupport-grid-manager.html>

There is also a nice blog post describing AutoSupport on StorageGRID:

<https://www.netapp.com/blog/enable-autosupport-to-get-more-insights-analytics-for-storagegrid-system/>

There are also instructions posted to our communities site: <https://community.netapp.com/t5/Tech-ONTAP-Blogs/Enabling-StorageGRID-AutoSupport-and-integrating-with-Active-IQ/ba-p/171339>

## Configuring AutoSupport in SolidFire and HCI

For documentation on configuration, see this link to our documentation: [https://docs.netapp.com/us-en/hci/docs/task\\_mnode\\_enable\\_activeIQ.html](https://docs.netapp.com/us-en/hci/docs/task_mnode_enable_activeIQ.html)

# Troubleshooting AutoSupport in Data ONTAP

This section provides the steps to troubleshoot AutoSupport when messages are not received, or certain content is missing.

## Troubleshooting 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 because it cannot deliver the message.

1. Check delivery status of the messages by using the `system node autosupport history show` command.
2. Read the status.
  - **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 additional information about the error 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 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 On Demand service chose to ignore it. Perform one of the following actions:
    - **Initializing or collection-failed. Contact technical support because AutoSupport cannot generate the message.**
    - **Ignore, re-queued, or transmission failed.** Check the destinations are correctly configured for SMTP, HTTP, or HTTPS because AutoSupport cannot deliver the message.

## Troubleshooting AutoSupport over HTTPS

If the system does not send the expected AutoSupport message and you are using HTTPS, you can check several settings to resolve the problem.



## On ONTAP

1. Confirm basic network connectivity and DNS lookup. If you are running Data ONTAP 8.3 or later, run `system node autosupport check show` to check the AutoSupport configuration and connectivity.
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 the value `up`.

3. Record the node names, the LIF name, and the LIF IP address for later use.
4. Make sure 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
```

If the error refers to a problem with the digital certificate, contact technical support.

6. Confirm that the cluster can access NetApp's AutoSupport servers successfully:

```
network traceroute -node local -destination default_router
network traceroute -node local -destination support.netapp.com
system node autosupport show -fields proxy-url
network traceroute -node local -destination proxy_url
```

If any of these destinations are not reachable, 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 approach 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, make sure that HTTPS traffic can exit your internal network:
  - a. Configure a web client on the same subnet as the cluster management LIF. Make sure that all configuration parameters are the same values as for the AutoSupport configuration, including using the same proxy server, username, password, and port.
  - b. Access **<https://support.netapp.com>** with the web client.

The access should be successful. If not, make sure that all firewalls are configured correctly to allow HTTPS and DNS traffic and that the proxy server is configured correctly.

## Troubleshooting AutoSupport over SMTP

If the system does not send the AutoSupport message and you are using SMTP, you can check several settings to resolve the problem.

## On ONTAP

1. Confirm basic network connectivity and DNS lookup. If you are running Data ONTAP 8.3 or later, run `system node autosupport check show` to check the AutoSupport configuration and connectivity.
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 the value `up`.

3. Record the node names, the LIF name, and the LIF IP address for later use.

4. If you are using hostnames for mail host destinations, make sure that DNS is enabled and configured correctly:

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

5. Display all the mail hosts configured to be used by AutoSupport:

```
system node autosupport show -fields mail-hosts
```

Record all mail hosts displayed.

6. For each mail host displayed by the previous step, make sure that the host can be reached by the node:

```
network traceroute -node local -destination mailhost
```

If any of these destinations are not reachable, 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 approach assists you in determining whether the issue is in your network configuration or your cluster configuration.

7. Log in to the host designated as the mail host and make sure that it can serve SMTP requests:

```
netstat -aAn|grep 25
```

25 is the listener SMTP port number. A message like the following text is displayed:

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

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

```
telnet mailhost 25
```

A message like the following text is displayed:

```
220 smtp.yourco.com Sendmail 4.1/SMI-4.1 ready at Thu, 30 Nov 2015 10:49:04 PST
```

9. At the Telnet prompt, make sure 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.

10. At the Telnet prompt, send a test message:

```
SUBJECT: TESTING
```

```
THIS IS A TEST
```

```
.
```

**Note:**

- Make sure 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.
11. From the Data ONTAP CLI, send an AutoSupport test message to a trusted e-mail address to which you have access:

```
system node autosupport invoke -node local -type test
```

12. 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 time stamp. It is probably the most recent attempt.

13. 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 node or cluster management LIF or the specified "from" e-mail address. 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, make sure that SMTP relay is enabled for the `autosupport@netapp.com` destination on all your SMTP mail hosts or use HTTPS as a transport protocol.

If the message to the locally administered e-mail account fails, confirm that your SMTP servers are configured to forward attachments with both characteristics:

- The "7z" suffix
- The "application/x-7x-compressed" MIME type

## Truncated Content in AutoSupport (AutoSupport Budgets)

As the Data ONTAP storage operating system grows in functionality, so does the amount of content collected and delivered in AutoSupport messages. Certain mail servers drop e-mail messages that have exceedingly large attachments (5MB or greater), and some web servers have file upload size limitations, as well.

ONTAP has AutoSupport collection and delivery budgets to be able to generate AutoSupport data quickly, with minimal impact to the data serving workflows and with minimal bandwidth requirements.

In the AutoSupport collection framework, all the content is owned by subsystems. AutoSupport enforces subsystem time and size limits during collection to provide the opportunity for all subsystems to collect their fair share of information. If a subsystem exceeds its allotted budget in terms of time or size limit, AutoSupport halts the collection for that subsystem and moves on the next one.

AutoSupport delivery budgets control the maximum size of an AutoSupport compressed payload archive. There are two delivery size limits: one for SMTP and the other for HTTPS. If the size of an AutoSupport archive exceeds the size limit, some content is dropped. During delivery, the content gets added to the archive in the order of priority recorded in the manifest, until the limit is reached.

Steps to determine if certain content is missing due to budget constraints:

1. Check the `manifest.xml` file included in the AutoSupport message. The status of the item in question is one of the following:

```
collection-truncated-size-limit  
collection-skipped-size-limit  
collection-truncated-time-limit  
collection-skipped-time-limit  
delivery-skipped-size-limit
```

Alternatively, run either of the following commands and check the output:

```
system node autosupport manifest show  
system node autosupport manifest show -seq-num SequenceNumber
```

(The latter command shows only those entries for a particular message.)

The item in question should have one of the preceding status values.

2. The collection size limit covers an entire subsystem of the node, not just individual files. For example, if a subsystem is responsible for six different entries (or files) in the manifest and

the fourth entry could not be collected due to the overall size constraints on the subsystem, the fifth and sixth items are also not collected.

The order in which these entries are collected is given by the **prio-num** field in the manifest. To display the collection order for each entry within a particular manifest, run the following command:

```
system node autosupport manifest show -node local -seq-num SequenceNumber -fields
prio-num,body-file,subsys,status,error,size-collected
system node autosupport manifest show -status *-limit -fields subsys,status,error
```

To reveal only the entries for a certain subsystem, add the flag **-subsys**, followed by the subsystem name (for example, **log\_files**).

**Note:** Some files (e.g., log files) have individual size budgets for AutoSupport collection. If a file collection is truncated because of a file-specific limit, the manifest status for this condition is **collection-truncated-file-size-limit**. This truncation is expected behavior and can be ignored. Budgets for specific files are not configurable.

If the collection size limit for a subsystem has in fact been reached for a particular AutoSupport message, the first manifest entry in error might be displayed as having the **collection-truncated-size-limit** status, while all succeeding entries in the subsystem will have the **collection-skipped-size-limit** status.

Consider the following example output:

```
Cluster1::system node autosupport*> manifest show -node local -seq-num 14 -fields
prio-num,body-file,subsys,status,error,size-collected -subsys mhost
node      seq-num prio-num subsys body-file      size-collected
status                                         error
-----
node-01 14      39      mhost  rdb_dump.txt 1KB  collection-truncated-size-limit ""
node-01 14      40      mhost  cluster_ha.xml
                                         730B collection-truncated-size-limit ""
node-01 14      41      mhost  cluster_ring.xml
                                         - collection-skipped-size-limit ""
node-01 14      42      mhost  dns.xml      - collection-skipped-size-limit ""
node-01 14      43      mhost  hosts.xml    - collection-skipped-size-limit ""
node-01 14      44      mhost  jm_sched.xml - collection-skipped-size-limit ""
node-01 14      45      mhost  jm_history_table_errors.xml
                                         - collection-skipped-size-limit ""
node-01 14      46      mhost  contact_info_view.xml
                                         - collection-skipped-size-limit ""
node-01 14      47      mhost  clusterPeer_itable.xml
                                         - collection-skipped-size-limit ""
node-01 14      48      mhost  foreign_cluster_addrs.xml
                                         - collection-skipped-size-limit ""
node-01 14      49      mhost  foreign_cluster_authority.xml
                                         - collection-skipped-size-limit ""
node-01 14      50      mhost  health_monitor_cache.xml
                                         - collection-skipped-size-limit ""
node-01 14      51      mhost  smdb_smf_metrics.xml
                                         - collection-skipped-size-limit ""
node-01 14      52      mhost  node_root_mounts.xml
                                         - collection-skipped-size-limit ""
```

In the preceding example, the attempt to collect the second item in the mhost subsystem, **cluster\_ha.xml**, is related to the failure. (For this output, the subsystem size limit was set to 1KB, which is a very low value.)

Note that not all the files are truncated if the subsystem size limit is breached. Binary files that exceed the subsystem limits are not truncated but are omitted from the AutoSupport message entirely. Only ASCII (text) files can be gracefully truncated.

If AutoSupport data is being truncated, perform the following steps to change the AutoSupport configuration to mitigate truncation:

1. Ensure that HTTPS is the AutoSupport transport in use. If AutoSupport is currently configured to use SMTP (email), modify the `-transport` parameter (Protocol to Contact Support) to use HTTPS instead of SMTP. With the HTTPS transport protocol, the overall AutoSupport message size can be much larger and the connection with NetApp is encrypted and secure. Ensure that outbound communication from the node-mgmt LIFS of each node can connect to TCP port 443 for host support.netapp.com. If your environment uses an HTTP proxy, confirm that the proxy is reachable, instead.

#### Notes:

- Enabling HTTPS for the AutoSupport transport is mandatory to resolve AutoSupport truncation. If SMTP must be used, do not continue with these steps as they might increase truncation.
- Changing the AutoSupport transport protocol does not affect SMTP-based AutoSupport message transmissions to `-to`, `-noteto` or `-partner-address` email destinations.

```
::> system node autosupport modify -node * -transport https
```

2. Upgrade to a ONTAP 8.3.2P3 or later

-OR-

Run the following commands to manually modify the AutoSupport configuration:

```
::> set -privilege diagnostic
::*> system node autosupport modify -node * -max-http-size 50MB
::*> system node autosupport budget modify -node * -subsystem performance_asup -size-limit 350MB -time-limit 10m
::*> system node autosupport budget modify -node * -subsystem performance -size-limit 150MB -time-limit 10m
::*> system node autosupport budget modify -node * -subsystem mhost -size-limit 17MB -time-limit 4m
::*> system node autosupport budget modify -node * -subsystem storage -size-limit 26MB -time-limit 6m
::*> system node autosupport budget modify -node * -subsystem asup_ems -size-limit 4MB -time-limit 2m
::*> system node autosupport budget modify -node * -subsystem kernel -size-limit 6MB -time-limit 2m
::*> system node autosupport budget modify -node * -subsystem wafl -size-limit 30MB -time-limit 10m
```

3. It is recommended that EMS event notifications be configured to desired destinations (e-mail, syslog, SNMP). EMS event notifications from Data ONTAP are the recommended method to be alerted of events that have occurred on the cluster. See the EMS Configuration Express Guide for help with configuring EMS event notifications from your cluster.

## NetApp does not receive AutoSupport messages sent through HTTPS with certificate validation enabled

AutoSupport messages are successfully delivered to NetApp using SMTP as the transport but fail when using HTTPS with certificate validation enabled.

There are two known kinds of failure for this issue. The signature can be determined by viewing the errors logged by the AutoSupport subsystem by reviewing the `/mroot/etc/log/mlog/notifyd.log`:

- The first signature is the "error setting certificate verify locations" error message, highlighted as follows:

```
00000008.0004cbb8 069e8daa Thu Mar 28 2013 10:33:04 -04:00 [kern_notifyd:info:711]
(category: 711:651:deliver) (emittime: 3/28/2013 10:33:04) (message: Connected
to support.netapp.com(216.240.21.18) port 443)
00000008.0004cbb9 069e8daa Thu Mar 28 2013 10:33:04 -04:00 [kern_notifyd:info:711]
(category: 711:651:deliver) (emittime: 3/28/2013 10:33:04) (message: error setting
certificate verify locations:
00000008.0004cbba 069e8daa Thu Mar 28 2013 10:33:04 -04:00
[kern_notifyd:info:711] CAfile: /mroot/etc/keymgr/root/cacert.pem
00000008.0004cbbb 069e8daa Thu Mar 28 2013 10:33:04 -04:00
[kern_notifyd:info:711] CApath: none)
00000008.0004cbbc 069e8daa Thu Mar 28 2013 10:33:04 -04:00 [kern_notifyd:info:711]
(category: 711:651:deliver) (emittime: 3/28/2013 10:33:04) (message: Closing
connection #0)
00000008.0004cbbd 069e8daa Thu Mar 28 2013 10:33:04 -04:00 [kern_notifyd:info:711]
(category: 711:651:deliver) (emittime: 3/28/2013 10:33:04) (message:
deliver_http_asup: HTTP PUT response error, status code 60.)
```

or

The second signature is the "SSL certificate problem: self signed certificate in certificate chain" error message, highlighted as follows.

```
00000017.00975b3d 0437a7d3 Tue Mar 01 2016 11:21:11 -06:00 [kern_notifyd:info:43017]
(category: 43017:1359:deliver) (emittime: 3/1/2016 11:09:08) (message: Connected
tosupport.netapp.com (216.240.21.18) port 443 (#0))
00000017.00975b3e 0437a7d3 Tue Mar 01 2016 11:21:11 -06:00 [kern_notifyd:info:43017]
(category: 43017:1359:deliver) (emittime: 3/1/2016 11:09:08) (message: successfully
set certificate verify locations:)
00000017.00975b3f 0437a7d3 Tue Mar 01 2016 11:21:11 -06:00 [kern_notifyd:info:43017]
(category: 43017:1359:deliver) (emittime: 3/1/2016 11:09:08) (message: CAfile:
/mroot/etc/keymgr/root/cacert.pem
00000017.00975b40 0437a7d3 Tue Mar 01 2016 11:21:11 -06:00
[kern_notifyd:info:43017] CApath: none)
00000017.00975b41 0437a7d3 Tue Mar 01 2016 11:21:11 -06:00 [kern_notifyd:info:43017]
(category: 43017:1359:deliver) (emittime: 3/1/2016 11:09:08) (message: SSLv3, TLS
handshake, Client hello (1):)
00000017.00975b42 0437a7d3 Tue Mar 01 2016 11:21:11 -06:00 [kern_notifyd:info:43017]
(category: 43017:1359:deliver) (emittime: 3/1/2016 11:09:08) (message: SSLv3, TLS
handshake, Server hello (2):)
00000017.00975b43 0437a7d3 Tue Mar 01 2016 11:21:11 -06:00 [kern_notifyd:info:43017]
(category: 43017:1359:deliver) (emittime: 3/1/2016 11:09:08) (message: SSLv3, TLS
handshake, CERT (11):)
00000017.00975b44 0437a7d3 Tue Mar 01 2016 11:21:11 -06:00 [kern_notifyd:info:43017]
(category: 43017:1359:deliver) (emittime: 3/1/2016 11:09:08) (message: SSLv3, TLS
alert, Server hello (2):)
00000017.00975b45 0437a7d3 Tue Mar 01 2016 11:21:11 -06:00 [kern_notifyd:info:43017]
(category: 43017:1359:deliver) (emittime: 3/1/2016 11:09:08) (message: SSL certificate
problem: self signed certificate in certificate chain)
00000017.00975b46 0437a7d3 Tue Mar 01 2016 11:21:11 -06:00 [kern_notifyd:info:43017]
(category: 43017:1359:deliver) (emittime: 3/1/2016 11:09:08) (message: Closing
connection #0)
```

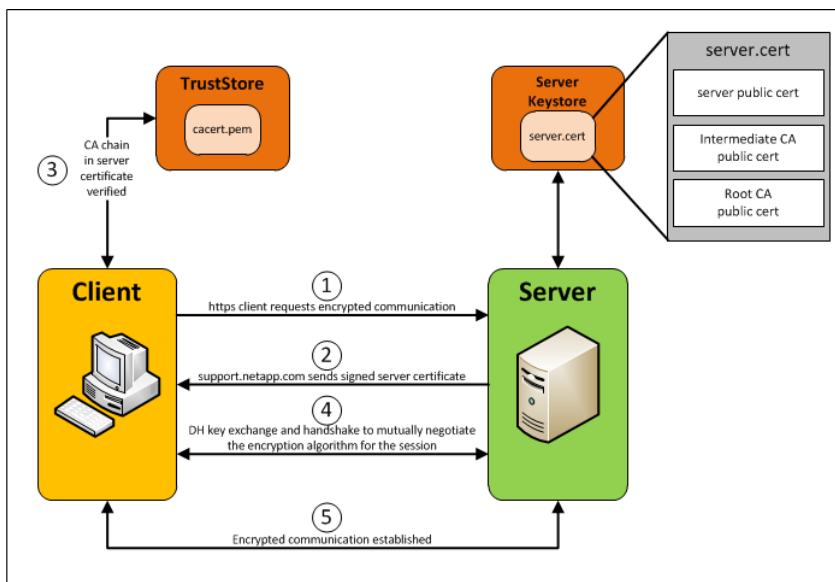
```

00000017.00975b47 0437a7d3 Tue Mar 01 2016 11:21:11 -06:00 [kern_notifyd:info:43017]
(category: 43017:1359:deliver) (emittime: 3/1/2016 11:09:08) (message:
deliver_http_asup: HTTP PUT response error, status code 60.)
00000017.00975b48 0437a7d3 Tue Mar 01 2016 11:21:11 -06:00 [kern_notifyd:info:43017]
(category: 43017:1359:deliver) (emittime: 3/1/2016 11:09:08) (message: asup_job HTTP
attempt failed '/mroot/etc/log/autosupport/201603011107.0')
00000017.00975b49 0437a7d3 Tue Mar 01 2016 11:21:11 -06:00 [kern_notifyd:info:43017]
(category: 43017:1359:deliver) (emittime: 3/1/2016 11:09:08) (message: Failed to
deliver http with subject: HA Group Notification from ho-0001-cn-as50t-01
(USER_TRIGGERED (ALL:debuglevel)) INFO)

```

When a Data ONTAP controller sends an AutoSupport message via the HTTPS protocol, it is acting as an HTTPS client. Here's a diagram of the basic steps that occur when an HTTPS client attempts to establish encrypted communication with a server.

**Figure 3) HTTPS encrypted communication diagram**



The major components are the following:

- **Client** is the system that initiates the communication and desires an encrypted communication channel. In this case, the autosupport subsystem in ONTAP is the client.
- **Server** is the system that provides services that can be communicated over an encrypted communication channel. The AutoSupport service at <https://support.netapp.com/put/AsupPut> and <https://support.netapp.com/asupprod/post/1.0/postAsup>
- **Server Keystore**, which resides on the server, contains a copy of the CA signed server public certificate file and private key file. Only the server public certificate is provided.
- The server public certificate contains the server's public key as well as the Certificate Authority (CA) public key chain of the CAs that have signed the server certificate.
- **TrustStore**, which resides on the client, contains a list the public keys of all the CAs the client trusts. The `cacert.pem` file is where Data ONTAP stores the public keys of all the CAs that are trusted by the AutoSupport HTTPS client and is used during certificate validation.

Here is how the encrypted channel is established:

1. The HTTPS client connects to the server (<https://support.netapp.com/put/AsupPut>) and requests an encrypted communication channel.
2. The server responds back with the CA-signed server certificate. The signed certificate contains the server's public key, and the public key chain of the CAs that signed the certificate.
3. The client checks the CA chain in the received server certificate and then verifies that the CA can be trusted by checking the client's TrustStore. In Data ONTAP, there is a setting that can be set to bypass this step.
  - a) If CA is trusted, certificate exchange continues in step #4.
  - b) If CA is not trusted, then the client rejects the certificate and terminates the connection.
4. Diffie-Hellman (DH) key exchange and encrypted handshake takes place to mutually determine the encrypted algorithm that is used for the session
5. After encrypted handshake is complete, encrypted communication begins between the client and server.

In the case of the "error setting certificate verify locations" error message, the cacert.pem file can become damaged during creation, thus Data ONTAP will not be able to use the file to validate received certificates.

In the case of the "SSL certificate problem: self signed certificate in certificate chain" error message, the storage controller is receiving a certificate that contains a CA chain that the HTTPS client is not able to validate. This can most likely can occur when a network device such as a firewall or transparent proxy is in the middle of the communication path between support.netapp.com and the storage controller, and it intercepts the HTTPS packets which handles certificate exchange handshake and specifies a different CA certificate chain for the support.netapp.com server certificate than the one support.netapp.com directly provides. The CA certificate chain that is injected by the firewall or transparent proxy appears as if it is being provided by support.netapp.com, however the CA public keys that are in the chain are not in the Data ONTAP cacert.pem TrustStore. This will cause Data ONTAP to reject the server certificate that was received and AutoSupport deliver fails.

Contact your support partner or NetApp technical support to resolve this problem. The solution requires modification of Data ONTAP system files and services.

## Additional Information

For more information about AutoSupport, see:

AutoSupport documentation on the NetApp Support Site  
[https://docs.netapp.com/us-en/active-iq/concept\\_autosupport.html](https://docs.netapp.com/us-en/active-iq/concept_autosupport.html)

TR-4688: Security and privacy of NetApp telemetry data  
<https://www.netapp.com/media/10439-tr4688.pdf>

## Version History

Version	Date	Document Version History
Version 1.0	August 2015	Initial release



Version	Date	Document Version History
Version 1.1	February 2016	Minor updates to AutoSupport On Demand section
Version 1.2	September 2017	Rename of My ASUP to Active IQ and other minor updates
Version 1.3	August 2023	Updated terminology; updated old content; removed 7-Mode instructions; updated links; added E-Series; added StorageGRID; added SolidFire and HCI; made clear which sections were ONTAP-specific

Refer to the [Interoperability Matrix Tool \(IMT\)](#) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

### Copyright information

Copyright © 2023 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

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

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

**Trademark information**

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