Technical Report

ONTAP AutoSupport and AutoSupport On Demand

Configuration Guide

Sudip Hore, Leita Lewis, Pradeep Palukuri, Andris Dindzans, NetApp
October 2017 | TR-4444

Abstract

This configuration guide is intended to assist customers, partners, sales engineers (SEs), consulting sales engineers (CSEs), professional services engineers (PSEs), and professional services consultants (PSCs) with configuring NetApp® AutoSupport® and AutoSupport On Demand® on NetApp ONTAP® data management software.

For feedback or questions, send an e-mail to ng-activeiq-feedback@netapp.com.

NetApp®

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Introduction

AutoSupport is a mechanism that proactively monitors the system health and automatically sends messages to NetApp technical support, the internal support organization, and support partners. The AutoSupport tool from NetApp Support is one of the most important troubleshooting tools for our customers. This tool provides foundational data for support tools designed to expedite support case resolution and maximize customers' systems uptime.

Although AutoSupport messages to technical support are enabled by default, it is necessary to set the appropriate options and have a valid mail host so that the messages are sent to your internal support organization.

This document covers the steps required to configure AutoSupport and AutoSupport On Demand on ONTAP data management software.

1.1 Audience

This document is for customers, NetApp SEs, CSEs, PSEs, PSCs, and channel partner engineers.

1.2 AutoSupport

AutoSupport is a feature of ONTAP data management software for all NetApp systems, providing an integrated, efficient monitoring and reporting capability and supporting data collection. AutoSupport provides the capability to send system health status messages directly to NetApp Technical Support and system administrators. In the event of a support incident, information is automatically sent to NetApp Technical Support staff 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.

1.3 Benefits of AutoSupport

Unless otherwise prohibited by data security policy, AutoSupport should be enabled as a NetApp best practice. Some benefits for enabling and maintaining consistent AutoSupport functionality include:

- Automated call home function regarding critical events—you can even open a support case 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 AutoSupport analysis tools for known configuration issues
- Ongoing health check analyses of 600 system parameters and intelligent linking of detected issues to solution information
- Handling of Return Merchandise Authorization requests without customer action
- Sending of system alerts to NetApp and customer contacts

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 system support case is opened, NetApp Support will request that an AutoSupport message be manually retransmitted or forwarded to expedite troubleshooting.

1.4 Managing AutoSupport

With the ONTAP data management software, 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 technical 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.

Active IQ is a web-based application that is part of the NetApp Support site. It aggregates all of the AutoSupport messages received from systems and provides recommendations and views to help improve system availability and efficiency. For more information, see the Active IQ User Guide.

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 running 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 running 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. Starting with ONTAP 8.2, NetApp technical support can request messages from AutoSupport by using the AutoSupport On Demand feature.

Table 1 shows the 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 `system node autosupport invoke` command	Depends on the value specified by the `-type` parameter: • `test` 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 -

Type of Message	Type of Data the Message Contains
	`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, including troubleshooting data from each subsystem. Technical support typically requests this message.
Triggered by the `system node autosupport invoke-core-upload` command	Core dump file for a node. 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. Example: `cluster1::> system node autosupport invoke-coredump -core-filename core.4070309011.2014-12-20.17_06_03.nz -message "Latest core of problem" -case-number 2006123456`
Triggered by the `system node autosupport invoke-performance-archive` command	Performance archive files for a specified period of time. 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. `cluster1::> 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`
Triggered by NetApp Support by using AutoSupport On Demand	AutoSupport On Demand can retransmit failed messages and relay remote instructions that are equivalent to AutoSupport invoke commands offered through CLI: • `system node autosupport invoke` • `system node invoke-performance-archive` • `system node autosupport invoke-core-upload` • `system node invoke-diagnostic (in diag mode)`

1.5 Active IQ

Active IQ is a web-based application that is based on AutoSupport information from your NetApp systems providing predictive and proactive insights to help improve availability, efficiency, and performance.

It is important to continually monitor the Active IQ 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. The benefits of Active IQ include:

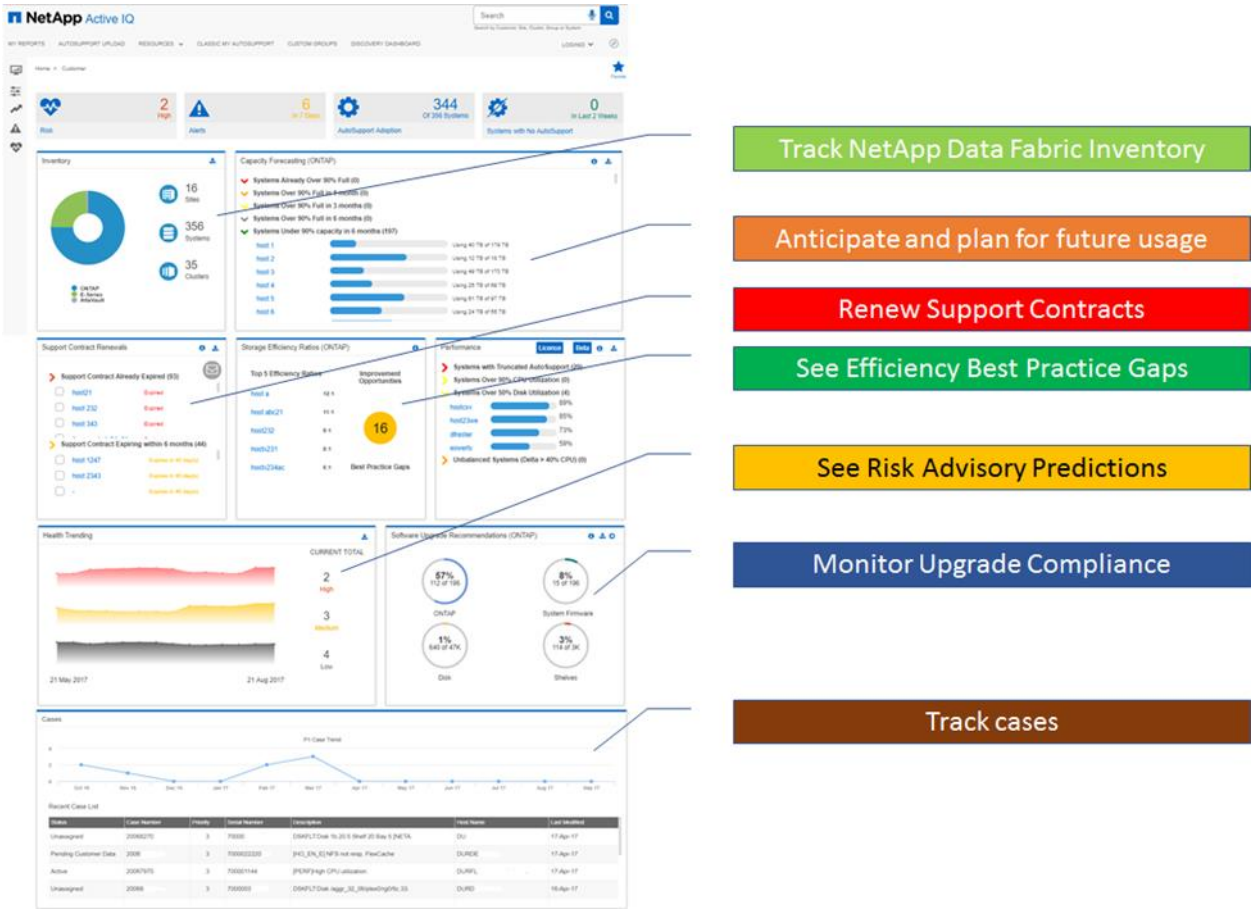
- Predicts storage capacity growth to identify capacity addition needs
- Recommends upgrade needs for ONTAP software and provides upgrade plans
- Proactively identifies system risks related to a configuration issue or known bugs
- Provides configuration, capacity, efficiency, and performance views and reports for better management of your NetApp systems

- Generate reports and export them to PDF or CSV files

You can access Active IQ by going to the Active IQ page on the NetApp Support site and clicking Launch Active IQ.

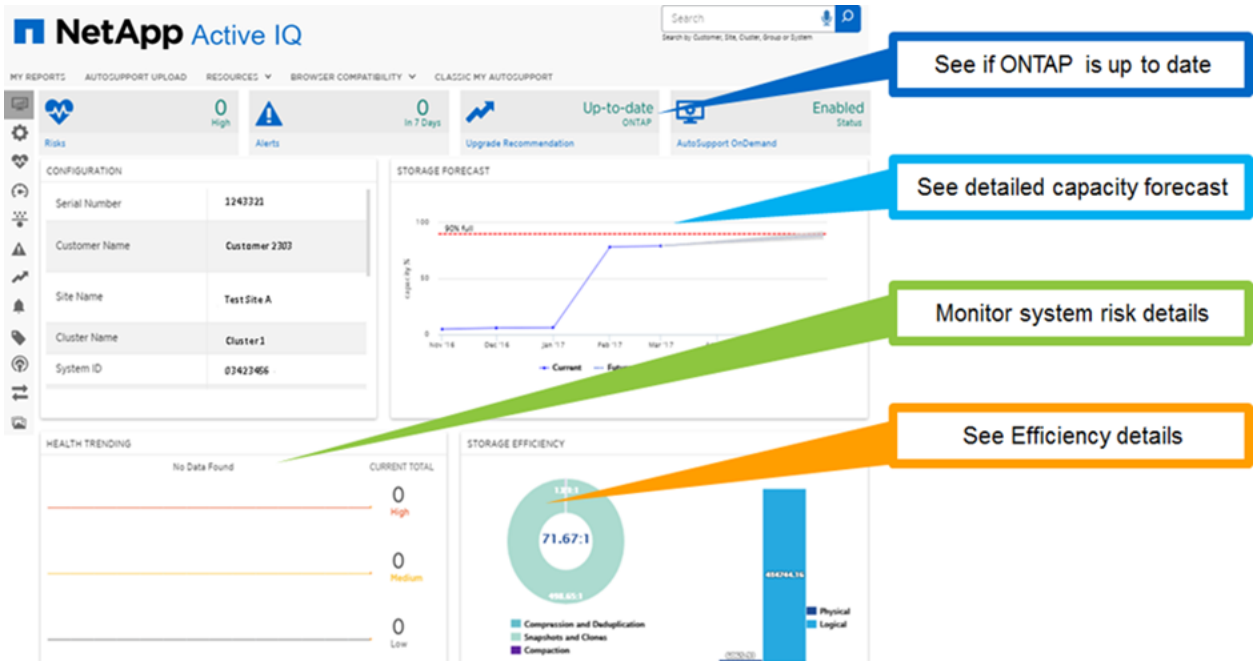
Figure 1 shows the Active IQ home page.

Figure 1) Active IQ home page.



Provide a NetApp storage serial number/system ID or site name in the search box. It opens the dashboard, as shown in Figure 2, with latest the AutoSupport information received by NetApp.

Figure 2) Active IQ System dashboard.



1.6 AutoSupport On Demand

AutoSupport On Demand 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 ONTAP AutoSupport capability. ONTAP software that is 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

The benefits of AutoSupport On Demand include:

- Improves customer support experience:
- Reduces customer time and overhead while gathering diagnostics for troubleshooting
- Requires minimal customer configuration
- Expedites NetApp case resolution
- Provides availability of up-to-date diagnostic and configuration information
- NetApp Support and support partners can obtain all of the information needed; even during customer off-hours, without customer involvement
- Enhances AutoSupport reliability by allowing retransmission of AutoSupport 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 AutoSupport 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 provides usage transparency:
  - Customers can review and execute all predefined delivery instructions by using 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.

  Note: The AutoSupport and AutoSupport On Demand solution was reviewed by Symantec. A white paper covering the results can be found on the NetApp Support site.

AutoSupport On Demand Operation

AutoSupport On Demand consists of the following components:

- An AutoSupport On Demand client that runs on each node
- An 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 7-Mode or clustered Data ONTAP 8.2 or later.

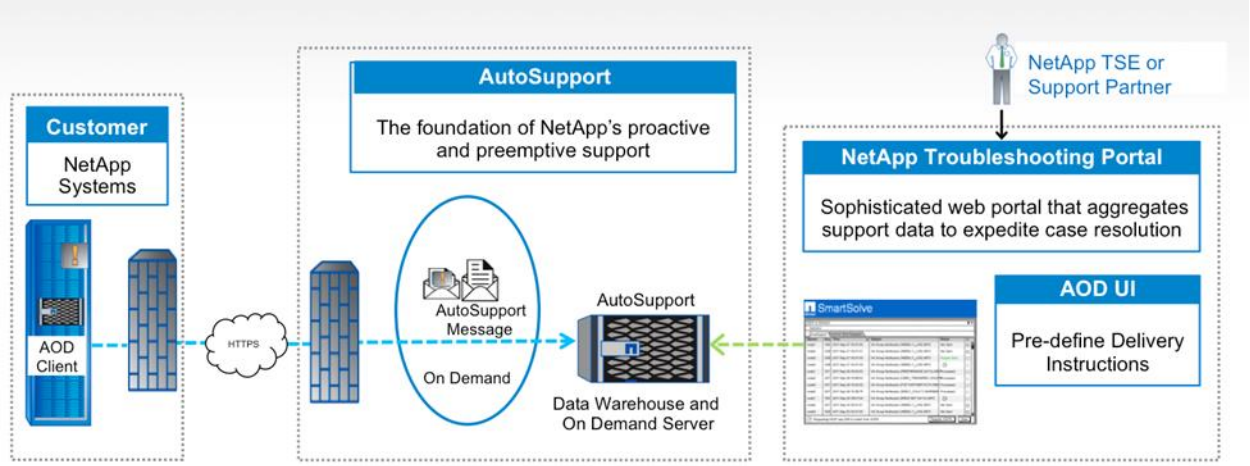
The AutoSupport On Demand client sends HTTPS requests to the same technical support location to which AutoSupport messages are sent. The AutoSupport On Demand client does not accept incoming connections.

Note: AutoSupport On Demand uses a predefined 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 3) AutoSupport On Demand workflow.



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

- Generate new AutoSupport messages.

  Note: 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.

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

- Retransmit previously-generated AutoSupport messages.

  Note: 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.

  Note: Technical support might disable delivery of certain types of AutoSupport data that is rarely needed or redundant.

2 Configure AutoSupport

This section describes how to set up AutoSupport and covers basic system requirements.

2.1 AutoSupport Requirements

To provide the best security and to support all of the latest AutoSupport features, use HTTPS for delivery of AutoSupport messages. Although AutoSupport supports HTTP and SMTP for delivery of AutoSupport messages, NetApp recommends using HTTPS.

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.

HTTP

- HTTP uses TCP port 80.
- This protocol is preferred over SMTP.
- This protocol supports uploads of large files, but not AutoSupport On Demand.

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 or HTTP.
- This protocol does not support uploads of large files and AutoSupport On Demand.
- SMTP data is not encrypted end-to-end by the node, making data in AutoSupport messages easier to intercept and read.
- 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 HTTP and 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 and HTTP protocols when you generate and send AutoSupport messages that upload core dump or performance archive files to the NetApp Support site or a specified URL.

2.2 Set Up AutoSupport

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

Configure DNS

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

Data ONTAP Operating in 7-Mode

To configure DNS on Data ONTAP operating in 7-Mode, complete the following steps:

1. Create or edit `/etc/resolv.conf` in the root volume using a text editor in the following format. Enter name server and IP address of the DNS name server.

```
nameserver     ip_address
```

2. Enter the following command to specify the DNS domain name. domain is the new domain name, which follows the host name of your storage system in the fully qualified domain name.

```
options dns.domainname domain
```

3. Enter the following command to enable DNS.

```
options dns.enable on
```

Clustered Data ONTAP

To configure DNS on clustered Data ONTAP, complete the following steps:

1. Enable DNS on the cluster.

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

Allow ONTAP IP Addresses Through the Firewall (if Applicable)

If applicable, allow ONTAP IP addresses through the firewall by completing the following steps:

1. For ONTAP AutoSupport messages to NetApp through HTTPS, allow all node-mgmt and cluster-mgmt logical interfaces (LIFs) on ONTAP clusters.
2. Service Processor AutoSupport messages are sent through SMTP only.
3. For ONTAP AutoSupport messages through SMTP, they need to reach the local SMTP gateway and be allowed to send e-mails to autosupport@netapp.com.

Enable AutoSupport

Enable AutoSupport to receive AutoSupport messages.

Data ONTAP Operating in 7-Mode

To enable AutoSupport on Data ONTAP operating in 7-Mode, complete the following steps:

1. To enable AutoSupport, run the following command:

```
options autosupport.enable on
```

2. To enable NetApp technical support to receive AutoSupport messages, run the following command:

```
options autosupport.support.enable on
```

Clustered Data ONTAP

To enable AutoSupport on clustered Data ONTAP, complete the following steps:

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
```

Note: 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.

Specify Transport Protocol for Messages

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

Data ONTAP Operating in 7-Mode

To specify the transport protocol to send AutoSupport messages on Data ONTAP operating in 7-Mode, complete the following steps:

1. Choose the protocol (HTTPS, HTTP, or SMTP) to transmit AutoSupport messages by running the following command:

```
options autosupport.support.transport transport_protocol
```

Note: HTTPS is the default protocol. Use SMTP only if the network connection does not allow HTTPS or HTTP.

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

Clustered Data ONTAP

To specify the transport protocol to send AutoSupport messages on clustered Data ONTAP, complete the following steps:

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

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

2. If you choose HTTP or 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.

Specify Proxy Configuration Details for HTTP or HTTPS Systems

If the `-transport` parameter is set to HTTP or 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
```

Notes:

- 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 user name 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 "?".
- For Data ONTAP 8.3 and earlier, the password in both `autosupport show` and `options autosupport` output is in plain text.
- For ONTAP 9.0 and later, password entry uses the secure (entered twice) interactive method. In addition, "*******" password in the URL text is displayed in various clustershell CLI commands (autosupport show, autosupport check show).
- For ONTAP 9.0 and later, AutoSupport options are removed entirely from `options` output in `nodeshell/dBlade` CLI.

  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
```

Configure Mail Server for SMTP Transport

Configure an e-mail server name or IP address that is able to 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.

Data ONTAP Operating in 7-Mode

To configure a mail server for SMTP transport on Data ONTAP operating in 7-Mode, complete the following steps:

1. Specify the mail host name or IP address by running the following command. You can set up to five hosts.

```
options autosupport.mailhost mailhost
```

2. Configure the `from` address. This command defines the e-mail address to be designated as the sender of the notification. This can be a common address used by all nodes or unique for each node.

```
options autosupport.from node1@itsupport.com
```

3. Configure the `to` addresses. Define the list of recipients who receive AutoSupport e-mail notifications for only significant and important events. You can define up to five e-mail addresses.

```
options autosupport.to asp@itsupport.com, me@itsupport.com
```

4. Configure `noteto` and `partner e-mail` addresses.

   Note: Partner e-mail destinations receive all AutoSupport messages.

```
options autosupport.noteto email_addresses
options autosupport.partner.to email_addresses
```

Clustered Data ONTAP

To configure a mail server for SMTP transport on clustered Data ONTAP, complete the following steps:

1. Configure a mail host by running 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. Make sure that the addresses are correctly configured by listing destinations.

```
system node autosupport destinations show
```

Configure Additional AutoSupport Options

Data ONTAP Operating in 7-Mode

To configure additional AutoSupport options on Data ONTAP operating in 7-Mode, complete the following steps:

1. To hide private data by removing, masking, or encoding sensitive data in the messages, set `autosupport.content` to `minimal`. If you change the setting from complete to minimal, all AutoSupport history and the associated files are deleted.
2. To stop sending periodic performance data AutoSupport messages, set `autosupport.performance_data.enable` to `disable`.

Clustered Data ONTAP

To configure additional AutoSupport options on clustered Data ONTAP, complete the following steps:

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

   Notes:

   - Limiting AutoSupport content and disabling performance data is not recommended because all of the AutoSupport content is used to monitor and troubleshoot 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 Clustered Data ONTAP 8.3 and later

For clustered ONTAP 8.3 and later, by default, performance content is collected and stored (archived) on every system. This content is built on top of a new functionality in ONTAP, which automatically stores

Quality of Service performance statistics on a per-volume basis for diagnostic purposes for up to 28 days on each clustered Data ONTAP node.

Using the AutoSupport infrastructure, a performance archive can be created and uploaded to NetApp.

EMS events report the following message if the performance archive is disabled:

Note: 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.
```

Upload Performance Archive

Run the `system node autosupport invoke-performance-archive` subcommand 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: The maximum duration for any single collection is six hours; the recommended sample period is four hours. Performance archives can only be uploaded through HTTP/HTTPS. SMTP is not currently supported as an upload method for performance archives. Performance archives can also be requested for support troubleshooting by using AutoSupport On Demand.

Check Overall AutoSupport Configuration

Data ONTAP Operating in 7-Mode

To check the overall AutoSupport configuration on Data ONTAP operating in 7-Mode, run the following commands:

```
node> options autosupport
autosupport.cifs.verbose off
autosupport.content complete
autosupport.doit MANAGEMENT_LOG
autosupport.enable on
autosupport.from postmaster
autosupport.local_collection on
autosupport.mailhost mailhost
autosupport.max_http_size 10485760
autosupport.max_smtp_size 5242880
autosupport.minimal.subject.id systemid
autosupport.nht_data.enable on
autosupport.noteto alerts@itsupport.com
autosupport.partner.to
autosupport.payload_format 7z
autosupport.performance_data.doit DON’T
autosupport.performance_data.enable on
autosupport.periodic.tx_window 1h
autosupport.retry.count 15
autosupport.retry.interval 4m
autosupport.support.enable on
autosupport.support.proxy
autosupport.support.put_url support.netapp.com/put/AsupPut
autosupport.support.to autosupport@netapp.com
autosupport.support.transport https
autosupport.support.url support.netapp.com/asupprod/post/1.0/postAsup
autosupport.throttle on
autosupport.to me@itsupport.com
autosupport.validate_digital_certificate on
```

Clustered Data ONTAP

To check the overall AutoSupport configuration on clustered Data ONTAP, run the following commands:

Note: 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
      Validate Digital Certificate Received: true
           AutoSupport On Demand Server URL: https://support.netapp.com/aods/asupmessage
```

2.3 Test AutoSupport Configuration

After AutoSupport is configured, test it 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 was received. If you do not receive the confirmation e-mail from NetApp, or if NetApp did not receive the message, perform the troubleshooting task for blocked network ports or access policies relative to the transport protocol (HTTPS, HTTP, or SMTP) in use to resolve the problem.

Data ONTAP Operating in 7-Mode

To test the AutoSupport configuration on Data ONTAP operating in 7-Mode, complete the following steps:

1. Use the option `autosupport.doit test` command.
2. Confirm that NetApp is receiving the AutoSupport messages by checking the e-mail addresses that are specified in the `autosupport.to` option and verify who should have received an automated response from the NetApp e-mail handler. Additionally, log in to Active IQ to confirm reception.
3. (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 `autosupport.to`, `autosupport.noteto`, or `autosupport.partner` options.

Clustered Data ONTAP

To test the AutoSupport configuration on Data ONTAP operating in 7-Mode, complete the following steps:

1. If you are running clustered Data ONTAP 8.3 or later, run the `system node autosupport check show` command to check the AutoSupport configuration.
2. Run 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 the AutoSupport messages by checking the e-mail address that are specified in the `–to` parameter and verify who should have received an automated response from the NetApp mail handler. Additionally, log in to 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.

   Example message to test AutoSupport e-mail:

```
++++++++++++++++++
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
```

2.4 AutoSupport Configuration Recommendation Through Active IQ

NetApp recommends the HTTPS 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 the Health Summary tab.

Users are able to view this information at the single system level, cluster level, or at aggregated levels (customer, site, and group) through the Health Summary tab in Active IQ, as shown in the examples in Figure 4 and Figure 5.

Figure 4) Health summary (example 1).

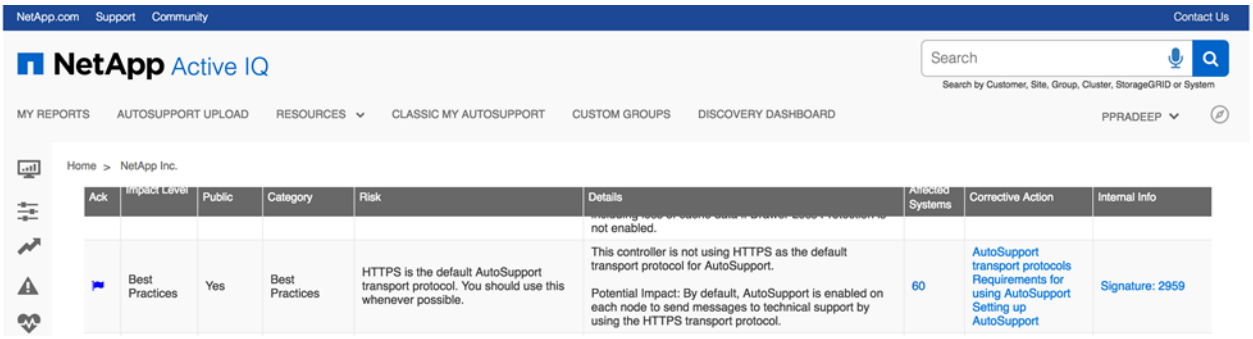
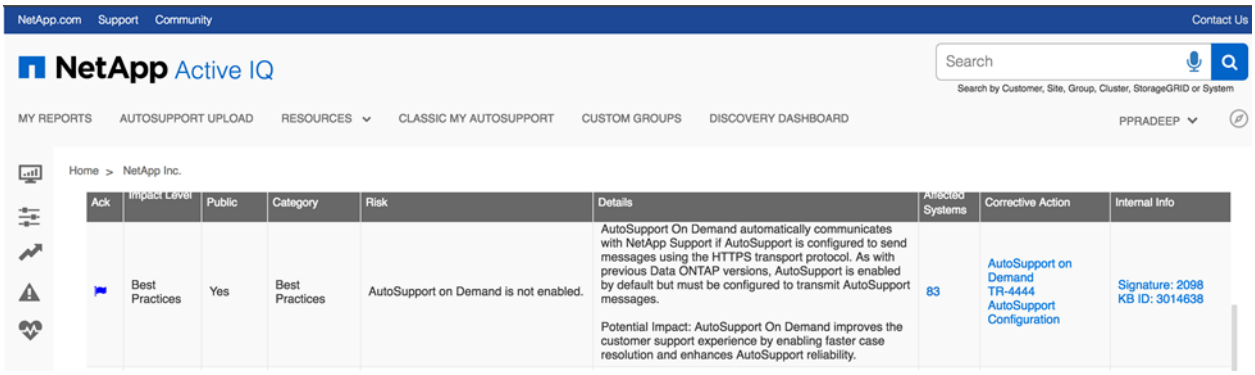


Figure 5) Health summary (example 2).



2.5 Decommission and Decline AutoSupport

This section describes the necessary steps to decline and decommission systems that are no longer in use. Before you decommission or decline AutoSupport, compete the following steps:

1. Identify the storage system serial number for the system on which 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.
2. Log in to the NetApp Support site.
3. Select the My Support tab.
4. Click Systems and then View Installed Products.
5. Enter the serial number of the system.

Decline AutoSupport

To decline AutoSupport, complete the following steps:

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

Decommission AutoSupport

To decommission AutoSupport, complete the following steps:

1. From the Manage Product Location & Details drop-down menu, select Decommission This System and click Go.
2. Complete the information on the Decommission Form and click Submit.

3 Troubleshooting AutoSupport

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

3.1 Troubleshooting AutoSupport When Messages Are Not Received

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

1. Check delivery status of the messages by running the `system node autosupport history show` command.
2. Read the status:
   - **Initializing**. The collection process is starting. If this state is temporary, then all is well. However, if this state persists, then 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 running the `system node autosupport history show -detail` command.
   - **Collection-in-progress**. AutoSupport is collecting AutoSupport content. You can view what AutoSupport is collecting by running 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 running the `system node autosupport history show -delivery` command.
   - **Ignore**. AutoSupport has no destinations for the message. You can view the delivery details by running the `system node autosupport history show -delivery` command.
   - **Requeued**. 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 running 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 running the `system node autosupport history show` command.
   - **On Demand-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, requeued, or transmission failed**. Make sure that the destinations are correctly configured for SMTP, HTTP, or HTTPS because AutoSupport cannot deliver the message.

3.2 Troubleshooting AutoSupport over HTTP and HTTPS

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

Data ONTAP Operating in 7-Mode

To troubleshoot AutoSupport over HTTP and HTTPS on Data ONTAP operating in 7-Mode, complete the following steps:

1. At the storage system's CLI, make sure that DNS is enabled and configured correctly by running the following command:

```
dns info
```

2. Read the error for the AutoSupport message by running the `autosupport history show` command with the `-seq-num` and `-destination` parameters.
3. At the storage system's CLI, make sure that the system is routing out to the Internet successfully by running the following command:

```
traceroute -p port support.netapp.com
```

4. The default port is 80 for HTTP and 443 for HTTPS.
5. If AutoSupport is configured to use a proxy, run the `traceroute -p` command to test the path to the proxy.
6. Run the `rdfile` command to read the `/etc/log/mlog/notifyd.log` file.

Clustered Data ONTAP

To troubleshoot AutoSupport over HTTP and HTTPS on clustered Data ONTAP, complete the following steps:

1. Confirm basic network connectivity and DNS lookup. If you are running clustered 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
```

Note: 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
```

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

6. Confirm that the cluster can access the NetApp 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
```

Note: If any of these destinations are not reachable, try the same route from a functioning host on the same subnet as the cluster by using the `traceroute` or `tracert` utility found on most third-party network clients. This approach assists you with 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, user name, password, and port.
   b. Access `https://support.netapp.com` with the web client.

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

3.3 Troubleshooting AutoSupport over SMTP

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

Data ONTAP Operating in 7-Mode

To troubleshoot AutoSupport over SMTP on Data ONTAP operating in 7-Mode, complete the following steps:

1. At the storage system's CLI, make sure that DNS is enabled and configured correctly by running the following command (DNS is required if using host names for mail host destinations):

```
dns info
```

2. At the storage system's CLI, verify that the mail host specified in the configuration is reachable by running the following command:

```
ping mailhost
```

   Note: `Mailhost` is the name or IP address of your mail host.

3. Log on to the host designated as the mail host and make sure that it can serve SMTP requests by running the following command.

   Note: 25 is the listener SMTP port number.

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

   A message similar to the following text is displayed:

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

4. At the CLI for the storage system, make sure that the system is reaching the mail host successfully by running the following command:

```
traceroute -p mailhost
```

   Note: `Mailhost` is the name or IP address of your mail host.

5. From some other host, Telnet to the SMTP port by running the following command:

```
telnet mailhost 25
```

   A message similar to the following text is displayed:

```
Trying 192.9.200.16 ...
Connected to filer.
Escape character is "^]".
220 smtp.yourco.com Sendmail 4.1/SMI-4.1 ready at Thu, 30 Nov 2015 10:49:04 PST
```

6. Run the `rdfile` command to read the `/etc/log/mlog/notifyd.log` file.

Clustered Data ONTAP

To troubleshoot AutoSupport over SMTP on clustered Data ONTAP, complete the following steps:

1. Confirm basic network connectivity and DNS lookup. If you are running clustered 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
```

   Note: 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 host names for mail host destinations, make sure that DNS is enabled and configured correctly.

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

5. Display all of 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.

   Note: 25 is the listener SMTP port number.

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

   A message similar to 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 similar to 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: the domain name of your network

   If an error is returned saying that relaying is denied, then 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
```

    Notes:
    - 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 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 of your SMTP mail hosts or use HTTPS as a transport protocol.

If the message to the locally administered e-mail 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

3.4 Truncated Content in AutoSupport Budgets

As the ONTAP data management software 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.

Data ONTAP 8.1 operating in 7-Mode and clustered Data ONTAP introduced 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 new AutoSupport collection framework, all of 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 HTTP/S. 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.

To determine if certain content is missing due to budget constraints, complete the following steps:

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
```

   Note: 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 commands:

```
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
```

Note: 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 (for example, 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, it is clear that 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: 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, complete the following steps to change the AutoSupport configuration to mitigate truncation:

1. Make sure that HTTPS or HTTP is the AutoSupport transport in use. If AutoSupport is currently configured to use SMTP (e-mail), 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. Make

sure 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 or HTTP 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` e-mail 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. NetApp recommends that EMS event notifications be configured to desired destinations (e-mail, syslog, or SNMP). EMS event notifications from ONTAP are the recommended methods to be alerted of events that have occurred on the cluster.

   For help with configuring EMS event notifications from your cluster, see the EMS Configuration Express Guide.

3.5 NetApp Does Not Receive AutoSupport Messages Sent Through HTTPS with Certificate Validation Enabled

AutoSupport messages are successfully delivered to NetApp by using SMTP or HTTP 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-cnas50t-01 (USER_TRIGGERED (ALL:debuglevel)) INFO)
```

When a clustered Data ONTAP controller sends an AutoSupport message through the HTTPS protocol, it is acting as an HTTPS client. Figure 6 illustrates the basic steps that occur when an HTTPS client attempts to establish encrypted communication with a server.

Figure 6) HTTPS client establishing encrypted communication with a server.

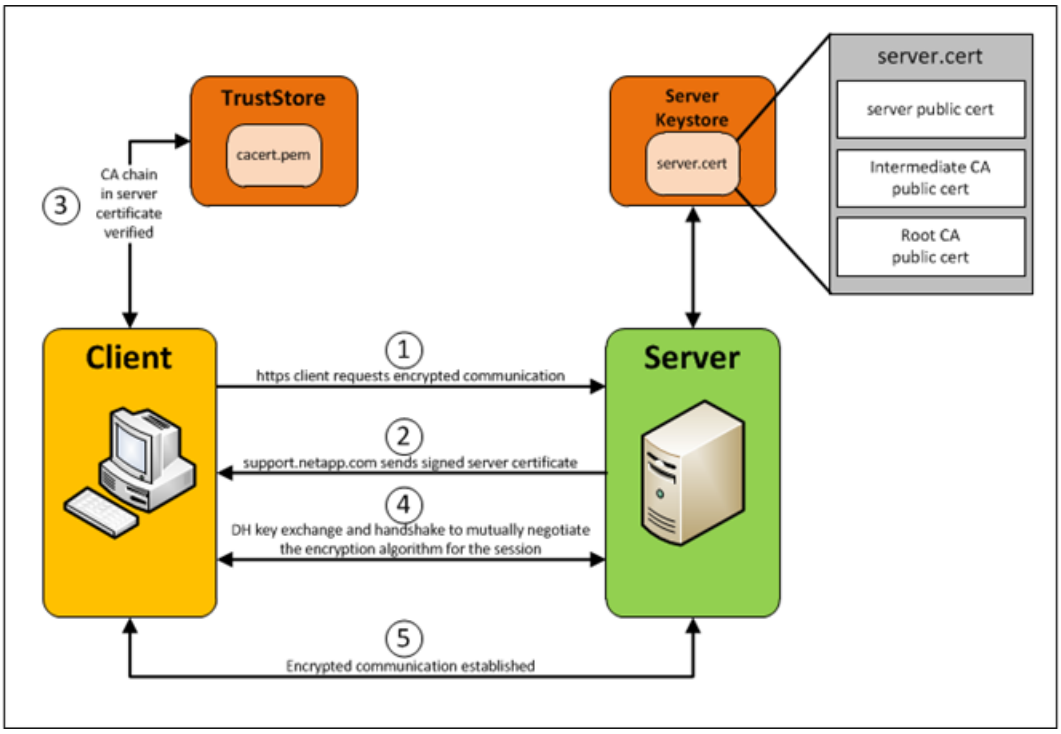


Figure 6 includes the following major components:

- **Client.** The system that initiates the communication and desires an encrypted communication channel. In this case, the autosupport subsystem in ONTAP is the client.
- **Server.** 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**. 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.** Resides on the client, contains a list the public keys of all of the CAs the client trusts. The `cacert.pem` file is where ONTAP stores the public keys for all of the CAs that are trusted by the AutoSupport HTTPS client and is used during certificate validation.

The encrypted channel is established by completing the following procedure:

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 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 event of an `error setting certificate verify locations` error message, the `cacert.pem` file can become damaged during creation; therefore, ONTAP will not be able to use the file to validate received certificates.

In the event of an `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 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. It intercepts the HTTPS packets that handle certificate exchange handshake and it 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 ONTAP `cacert.pem` TrustStore. This event causes 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 ONTAP system files and services.

Where to Find Additional Information

To learn more about the information described in this document, refer to the following documents and/or websites:

- AutoSupport FAQs:
  http://support.netapp.com/NOW/knowledge/docs/olio/autosupport/asup_faqs.shtml
- AutoSupport how-to's:
  http://support.netapp.com/NOW/knowledge/docs/olio/autosupport/how_to.shtml
- AutoSupport on the NetApp Support site:
  http://support.netapp.com/NOW/knowledge/docs/olio/autosupport/
- AutoSupport and On Demand security assessment:
  http://www.netapp.com/us/media/NetApp-AutoSupport-On Demand.pdf (Symantec)
- AutoSupport and AutoSupport On Demand overview:
  https://library.netapp.com/ecmdocs/ECMP1196798/html/GUID-239B1BFC-D883-4CB4-A9B2-FD58F299570E.html
- KB article about AutoSupport On Demand settings:
  https://kb.netapp.com/support/index?page=content&id=S%3A3014638&actp=LIST
- RSDT EOL customer notification:
  http://mysupport.netapp.com/info/communications/ECMLP2465089.html
- KB about how to transition to AutoSupport On Demand:
  https://kb.netapp.com/support/index?page=content&actp=LIST&id=1015768

Version History

Version	Date	Document Version History
Version 1.2	October 2017	Rename of My ASUP to Active IQ and other minor updates.
Version 1.1	February 2016	Minor updates to AutoSupport On Demand section.

Version	Date	Document Version History
Version 1.0	August 2015	Initial release.

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

Trademark Information

TR-4444-1017