



# System health and events

## Cloud Volumes ONTAP

NetApp  
February 13, 2026

# Table of Contents

- System health and events ..... 1
- Verify AutoSupport setup for Cloud Volumes ONTAP ..... 1
- AutoSupport requirements ..... 1
- Troubleshoot your AutoSupport configuration ..... 1
- Configure EMS for Cloud Volumes ONTAP systems ..... 4

# System health and events

## Verify AutoSupport setup for Cloud Volumes ONTAP

AutoSupport proactively monitors the health of your system and sends messages to NetApp technical support. By default, AutoSupport is enabled on each node to send messages to technical support using the HTTPS transport protocol. It's best to verify that AutoSupport can send these messages.

The only required configuration step is to ensure that Cloud Volumes ONTAP has outbound internet connectivity. For details, refer to the networking requirements for your cloud provider.

### AutoSupport requirements

Cloud Volumes ONTAP nodes require outbound internet access for NetApp AutoSupport, which proactively monitors the health of your system and sends messages to NetApp technical support.

Routing and firewall policies must allow HTTPS traffic to the following endpoints so Cloud Volumes ONTAP can send AutoSupport messages:

- <https://mysupport.netapp.com/aods/asupmessage>
- <https://mysupport.netapp.com/asupprod/post/1.0/postAsup>

If an outbound internet connection isn't available to send AutoSupport messages, the NetApp Console automatically configures your Cloud Volumes ONTAP systems to use the Console agent as a proxy server. The only requirement is to ensure that the Console agent's security group allows *inbound* connections over port 3128. You'll need to open this port after you deploy the Console agent.

If you defined strict outbound rules for Cloud Volumes ONTAP, then you'll also need to ensure that the Cloud Volumes ONTAP security group allows *outbound* connections over port 3128.



If you're using an HA pair, the HA mediator doesn't require outbound internet access.

After you've verified that outbound internet access is available, you can test AutoSupport to ensure that it can send messages. For instructions, refer to the [ONTAP documentation: Set up AutoSupport](#).

### Troubleshoot your AutoSupport configuration

If an outbound connection isn't available and the Console can't configure your Cloud Volumes ONTAP system to use the Console agent as a proxy server, you'll receive a notification from the Console that your system is unable to send AutoSupport messages. Follow these steps to address this issue.

#### Steps

1. Connect securely (using SSH) to the Cloud Volumes ONTAP system to use the ONTAP CLI.

[Learn how to SSH to Cloud Volumes ONTAP.](#)

2. Check the detailed status of the AutoSupport subsystem:

```
autosupport check show-details
```

The response looks like this:

```
Category: smtp
  Component: mail-server
  Status: failed
  Detail: SMTP connectivity check failed for destination:
        mailhost. Error: Could not resolve host -
'mailhost'
  Corrective Action: Check the hostname of the SMTP server

Category: http-https
  Component: http-put-destination
  Status: ok
  Detail: Successfully connected to:
        <https://support.netapp.com/put/AsupPut/>.

  Component: http-post-destination
  Status: ok
  Detail: Successfully connected to:

https://support.netapp.com/asupprod/post/1.0/postAsup.

Category: on-demand
  Component: ondemand-server
  Status: ok
  Detail: Successfully connected to:
        https://support.netapp.com/aods/asupmessage.

Category: configuration
  Component: configuration
  Status: ok
  Detail: No configuration issues found.

5 entries were displayed.
```

If the status of the http-https category is OK it means that AutoSupport is configured properly and messages can be sent.

3. If not, verify the proxy URL for each Cloud Volumes ONTAP node:

```
autosupport show -fields proxy-url
```

4. If the proxy URL parameter is empty, configure Cloud Volumes ONTAP to use the Console agent as a proxy:

```
autosupport modify -proxy-url http://<console agent private ip>:3128
```

5. Verify the AutoSupport status again:

```
autosupport check show-details
```

6. If the status is still failed, validate that there is connectivity between Cloud Volumes ONTAP and the Console agent over port 3128.
7. If the status is still failed after verification, SSH to the Console agent.

[Learn more about Connecting to the Linux VM for the Console agent](#)

8. Go to `/opt/application/netapp/cloudmanager/docker_occm/data/`.
9. Open the proxy configuration file `squid.conf`. This is the structure of the file:

```
http_port 3128
acl netapp_support dst support.netapp.com
http_access allow netapp_support
request_header_max_size 21 KB
reply_header_max_size 21 KB
http_access deny all
httpd_suppress_version_string on
```

10. If your file doesn't have an entry for the CIDR block of the Cloud Volumes ONTAP system, add a new entry and allow access:

```
acl cvonet src <cidr>
```

```
http_access allow cvonet
```

Here's an example:

```
http_port 3128
acl netapp_support dst support.netapp.com
acl cvonet src <cidr>
http_access allow netapp_support
http_access allow cvonet
request_header_max_size 21 KB
reply_header_max_size 21 KB
http_access deny all
httpd_suppress_version_string on
```

11. After editing the config file, restart the proxy container as `sudo`. Then, depending on whether you're using Docker or Podman, run these commands:

For Docker, run `docker restart squid`.

If you are using Podman, run `podman restart squid`.

12. Go back to the ONTAP CLI and verify that Cloud Volumes ONTAP can send AutoSupport messages:

autosupport check show-details

#### Related links

- [Networking requirements for Cloud Volumes ONTAP in AWS](#)
- [Networking requirements for Cloud Volumes ONTAP in Azure](#)
- [Networking requirements for Cloud Volumes ONTAP in Google Cloud](#)

## Configure EMS for Cloud Volumes ONTAP systems

The Event Management System (EMS) collects and displays information about events that occur on ONTAP systems. To receive event notifications, you can set event destinations (email addresses, SNMP trap hosts, or syslog servers) and event routes for a particular event severity.

You can configure EMS using the CLI. For instructions, refer to the [ONTAP documentation: EMS configuration overview](#).

## Copyright information

Copyright © 2026 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, nonsublicensable, 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.