Manage auditing configurations

ONTAP 9

NetApp
January 23, 2026

This PDF was generated from https://docs.netapp.com/us-en/ontap/nas-audit/manual-rotate-audit-event-logs-task.html on January 23, 2026. Always check docs.netapp.com for the latest.

Table of Contents

Manage auditing configurations . . . 1
Manually rotate the audit event logs to view specific ONTAP SVM event logs . . . 1
Enable or disable auditing on ONTAP SVMs . . . 1
Display information about ONTAP auditing configurations . . . 2
ONTAP commands for modifying auditing configurations . . . 4
Delete an auditing configuration on an ONTAP SVM . . . 4
Understand the implications of reverting an audited ONTAP cluster . . . 5
Reverting to a version of ONTAP that does not support the auditing of SMB logon and logoff events and central access policy staging events . . . 5

Manage auditing configurations

Manually rotate the audit event logs to view specific ONTAP SVM event logs

Before you can view the audit event logs, the logs must be converted to user-readable formats. If you want to view the event logs for a specific storage virtual machine (SVM) before ONTAP automatically rotates the log, you can manually rotate the audit event logs on an SVM.

Step

1. Rotate the audit event logs by using the `vserver audit rotate-log` command.

   ```
   vserver audit rotate-log -vserver vs1
   ```

   The audit event log is saved in the SVM audit event log directory with the format specified by the auditing configuration (`XML` or `EVTX`), and can be viewed by using the appropriate application.

Enable or disable auditing on ONTAP SVMs

You can enable or disable auditing on storage virtual machines (SVMs). You might want to temporarily stop file and directory auditing by disabling auditing. You can enable auditing at any time (if an auditing configuration exists).

Before you begin

Before you can enable auditing on the SVM, the SVM's auditing configuration must already exist.

Create the auditing configuration

About this task

Disabling auditing does not delete the auditing configuration.

Steps

1. Perform the appropriate command:

If you want auditing to be…	Enter the command…
Enabled	`vserver audit enable -vserver vserver_name`
Disabled	`vserver audit disable -vserver vserver_name`

2. Verify that auditing is in the desired state:

   ```
   vserver audit show -vserver vserver_name
   ```

Examples

The following example enables auditing for SVM vs1:

```
cluster1::> vserver audit enable -vserver vs1

cluster1::> vserver audit show -vserver vs1

                              Vserver: vs1
                      Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops, cifs-logon-logoff
                           Log Format: evtx
                  Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
         Log Rotation Schedule: Day: -
        Log Rotation Schedule: Hour: -
      Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 10
```

The following example disables auditing for SVM vs1:

```
cluster1::> vserver audit disable -vserver vs1

                              Vserver: vs1
                      Auditing state: false
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops, cifs-logon-logoff
                           Log Format: evtx
                  Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
         Log Rotation Schedule: Day: -
        Log Rotation Schedule: Hour: -
      Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 10
```

Display information about ONTAP auditing configurations

You can display information about auditing configurations. The information can help you determine whether the configuration is what you want in place for each SVM. The displayed information also enables you to verify whether an auditing configuration is enabled.

About this task

You can display detailed information about auditing configurations on all SVMs or you can customize what information is displayed in the output by specifying optional parameters. If you do not specify any of the optional parameters, the following is displayed:

- SVM name to which the auditing configuration applies
- The audit state, which can be `true` or `false`

  If the audit state is `true`, auditing is enabled. If the audit state is `false`, auditing is disabled.

- The categories of events to audit
- The audit log format
- The target directory where the auditing subsystem stores consolidated and converted audit logs

Step

1. Display information about the auditing configuration by using the `vserver audit show` command.

   Learn more about `vserver audit show` in the ONTAP command reference.

Examples

The following example displays a summary of the auditing configuration for all SVMs:

```
cluster1::> vserver audit show

 Vserver     State  Event Types Log Format Target Directory
 ----------- ------ ----------- ---------- --------------------
 vs1         false  file-ops    evtx       /audit_log
```

The following example displays, in list form, all auditing configuration information for all SVMs:

```
cluster1::> vserver audit show -instance

                              Vserver: vs1
                       Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops
                          Log Format: evtx
                  Log File Size Limit: 100MB
         Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
           Log Rotation Schedule: Day: -
          Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
             Log Files Rotation Limit: 0
```

ONTAP commands for modifying auditing configurations

If you want to change an auditing setting, you can modify the current configuration at any time, including modifying the log path destination and log format, modifying the categories of events to audit, how to automatically save log files, and specify the maximum number of log files to save.

If you want to…	Use this command…
Modify the log destination path	`vserver audit modify` with the `-destination` parameter
Modify the category of events to audit	`vserver audit modify` with the `-events` parameter To audit central access policy staging events, the Dynamic Access Control (DAC) SMB server option must be enabled on the storage virtual machine (SVM).
Modify the log format	`vserver audit modify` with the `-format` parameter
Enabling automatic saves based on internal log file size	`vserver audit modify` with the `-rotate-size` parameter
Enabling automatic saves based on a time interval	`vserver audit modify` with the `-rotate-schedule-month`, `-rotate-schedule-dayofweek`, `-rotate-schedule-day`, `-rotate-schedule-hour`, and `-rotate-schedule-minute` parameters
Specifying the maximum number of saved log files	`vserver audit modify` with the `-rotate-limit` parameter

Delete an auditing configuration on an ONTAP SVM

In you no longer want to audit file and directory events on the storage virtual machine (SVM) and do not want to maintain an auditing configuration on the SVM, you can delete the auditing configuration.

Steps

1. Disable the auditing configuration:

```
vserver audit disable -vserver vserver_name
```

```
vserver audit disable -vserver vs1
```

2. Delete the auditing configuration:

```
vserver audit delete -vserver vserver_name
```

```
vserver audit delete -vserver vs1
```

Understand the implications of reverting an audited ONTAP cluster

If you plan to revert the cluster, you should be aware of the revert process ONTAP follows when there are auditing-enabled storage virtual machines (SVMs) in the cluster. You must take certain actions before reverting.

Reverting to a version of ONTAP that does not support the auditing of SMB logon and logoff events and central access policy staging events

Support for auditing of SMB logon and logoff events and for central access policy staging events starts with clustered Data ONTAP 8.3. If you are reverting to a version of ONTAP that does not support these event types and you have auditing configurations that monitor these event types, you must change the auditing configuration for those audit-enabled SVMs before reverting. You must modify the configuration so that only file-op events are audited.

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.