Manage syslog

SANtricity software

NetApp
August 22, 2025

This PDF was generated from https://docs.netapp.com/us-en/e-series-santricity-118/sm-settings/view-audit-log-activity.html on August 22, 2025. Always check docs.netapp.com for the latest.

Table of Contents

Manage syslog . . . 1
View audit log activity . . . 1
Define audit log policies . . . 3
Delete events from the audit log . . . 4
Configure syslog server for audit logs . . . 5
Edit syslog server settings for audit log records . . . 6

Manage syslog

View audit log activity

By viewing audit logs, users with Security Admin permissions can monitor user actions, authentication failures, invalid login attempts, and the user session lifespan.

Before you begin

You must be logged in with a user profile that includes Security admin permissions. Otherwise, the Access Management functions do not appear.

Steps

1. Select **Settings › Access Management**.
2. Select the **Audit Log** tab.

   Audit log activity appears in tabular format, which includes the following columns of information:

   - **Date/Time** — Timestamp of when the storage array detected the event (in GMT).
   - **Username** — The user name associated with the event. For any non-authenticated actions on the storage array, "N/A" appears as the user name. Non-authenticated actions might be triggered by the internal proxy or some other mechanism.
   - **Status Code** — HTTP status code of the operation (200, 400, etc.) and descriptive text associated with the event.
   - **URL Accessed** — Full URL (including host) and query string.
   - **Client IP Address** — IP address of the client associated with the event.
   - **Source** — Logging source associated with the event, which can be System Manager, CLI, Web Services, or Support Shell.
   - **Description** — Additional information about the event, if applicable.
3. Use the selections on the Audit Log page to view and manage events.

Selection details

Selection	Description
Show events from the…	Limit events shown by date range (last 24 hours, last 7 days, last 30 days, or a custom date range).
Filter	Limit events shown by the characters entered in the field. Use quotes ("") for an exact word match, enter `OR` to return one or more words, or enter a dash (—) to omit words.
Refresh	Select **Refresh** to update the page to the most current events.
View/Edit Settings	Select **View/Edit Settings** to open a dialog box that allows you to specify a full log policy and level of actions to be logged.
Delete events	Select **Delete** to open a dialog box that allows you to remove old events from the page.
Show/hide columns	Click the **Show/Hide** column icon to select additional columns for display in the table. Additional columns include: • **Method** — The HTTP method (for example, POST, GET, DELETE, etc.). • **CLI Command Executed** — The CLI command (grammar) executed for Secure CLI requests. • **CLI Return Status** — A CLI status code or a request for input files from the client. • **SYMbol Procedure** — The SYMbol procedure executed. • **SSH Event Type** — Secure Shell (SSH) events type, such as login, logout, and login_fail. • **SSH Session PID** — Process ID number of the SSH session. • **SSH Session Duration(s)** — The number of seconds the user was logged in. • **Authentication Type** — Types can include Local user, LDAP, SAML, and Access token. • **Authentication ID** — ID of the authenticated session.
Toggle column filters	Click the **Toggle** icon to open filtering fields for each column. Enter characters within a column field to limit events shown by those characters. Click the icon again to close the filtering fields.
Undo changes	Click the **Undo** icon to return the table to the default configuration.
Export	Click **Export** to save the table data to a comma separated value (CSV) file.

Define audit log policies

You can change the overwrite policy and the types of events recorded in the audit log.

Before you begin

You must be logged in with a user profile that includes Security admin permissions. Otherwise, the Access Management functions do not appear.

About this task

This task describes how to change the audit log settings, which include the policy for overwriting old events and the policy for recording event types.

Steps

1. Select **Settings › Access Management**.
2. Select the **Audit Log** tab.
3. Select **View/Edit Settings**.

   The Audit Log Settings dialog box opens.

4. Change the overwrite policy or types of events recorded.

Field details

Setting	Description
Overwrite policy	Determines the policy for overwriting old events when the maximum capacity is reached: • **Allow the oldest events in the audit log to be overwritten when the audit log is full** — Overwrites the old events when the audit log reaches 50,000 records. • **Require audit log events to be manually deleted** — Specifies that events will not be automatically deleted; instead, a threshold warning appears at the set percentage. Events must be deleted manually. If the overwrite policy is disabled and the audit log entries reach the maximum limit, access to System Manager is denied to users without Security Admin permissions. To restore system access to users without Security Admin permissions, a user assigned to the Security Admin role must delete the old event records. Overwrite policies do not apply if a syslog server is configured for archiving audit logs.
Level of actions to be logged	Determines types of events to be logged: • **Record modification events only** — Shows only the events where a user action involves making a change in the system. • **Record all modification and read-only events** — Shows all events, including a user action that involves reading or downloading information.

5. Click **Save**.

Delete events from the audit log

You can clear the audit log of old events, which makes searching through events more manageable. You have the option of saving old events to a CSV (comma-separated values) file upon deletion.

Before you begin

You must be logged in with a user profile that includes Security admin permissions. Otherwise, the Access Management functions do not appear.

Steps

1. Select **Settings › Access Management**.
2. Select the **Audit Log** tab.

3. Select **Delete**.

   The Delete Audit Log dialog box opens.

4. Select or enter the number of oldest events that you want to delete.
5. If you want to export the deleted events to a CSV file (recommended), keep the checkbox selected. You will be prompted to enter a file name and location when you click **Delete** in the next step. Otherwise, if you do not want to save events to a CSV file, click the checkbox to deselect it.
6. Click **Delete**.

   A confirmation dialog box opens.

7. Type `delete` in the field, and then click **Delete**.

   The oldest events are removed from the Audit Log page.

Configure syslog server for audit logs

If you want to archive audit logs onto an external syslog server, you can configure communications between that server and the storage array. After the connection is established, audit logs are automatically saved to the syslog server.

Before you begin

- You must be logged in with a user profile that includes Security admin permissions. Otherwise, the Access Management functions do not appear.
- The syslog server address, protocol, and port number must be available. The server address can be a fully qualified domain name, an IPv4 address, or an IPv6 address.
- If your server uses a secure protocol (for example, TLS), a Certificate Authority (CA) certificate must be available on your local system. CA certificates identify website owners for secure connections between servers and clients.

Steps

1. Select **Settings › Access Management**.
2. From the Audit Log tab, select **Configure Syslog Servers**.

   The Configure Syslog Servers dialog box opens.

3. Click **Add**.

   The Add Syslog Server dialog box opens.

4. Enter information for the server, and then click **Add**.
   - **Server address** — Enter a fully qualified domain name, an IPv4 address, or an IPv6 address.
   - **Protocol** — Select a protocol from the drop-down list (for example, TLS, UDP, or TCP).
   - **Upload certificate (optional)** — If you selected the TLS protocol and have not yet uploaded a signed CA certificate, click **Browse** to upload a certificate file. Audit logs are not archived to a syslog server without a trusted certificate.

If the certificate becomes invalid later, the TLS handshake will fail. As a result, an error message is posted to the audit log and messages are no longer sent to the syslog server. To resolve this issue, you must fix the certificate on the syslog server and then go to **Settings › Audit Log › Configure Syslog Servers › Test All**.

- **Port** — Enter the port number for the syslog receiver. After you click **Add**, the Configure Syslog Servers dialog box opens and displays your configured syslog server on the page.

5. To test the server connection with the storage array, select **Test All**.

Results

After configuration, all new audit logs are sent to the syslog server. Previous logs are not transferred. To further configure syslog settings for alerts, see Configure syslog server for alerts.

```
NOTE: If multiple syslog servers are configured, all configured syslog
servers will receive an audit log.
```

Edit syslog server settings for audit log records

You can change the settings for the syslog server used for archiving audit logs, and also upload a new Certificate Authority (CA) certificate for the server.

Before you begin

- You must be logged in with a user profile that includes Security admin permissions. Otherwise, the Access Management functions do not appear.
- The syslog server address, protocol, and port number must be available. The server address can be a fully qualified domain name, an IPv4 address, or an IPv6 address.
- If you are uploading a new CA certificate, the certificate must be available on your local system.

Steps

1. Select **Settings › Access Management**.
2. From the Audit Log tab, select **Configure Syslog Servers**.

   Configured syslog servers are displayed on the page.

3. To edit the server information, select the **Edit** (pencil) icon to the right of the server name, and then make desired changes in the following fields:
   - **Server Address** — Enter a fully qualified domain name, an IPv4 address, or an IPv6 address.
   - **Protocol** — Select a protocol from the drop-down list (for example, TLS, UDP, or TCP).
   - **Port** — Enter the port number for the syslog receiver.
4. If you changed the protocol to the secure TLS protocol (from either UDP or TCP), click **Import Trusted Certificate** to upload a CA certificate.
5. To test the new connection with the storage array, select **Test All**.

Results

After configuration, all new audit logs are sent to the syslog server. Previous logs are not transferred.

Copyright information

Copyright © 2025 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.