

NetApp Storage Auditing

How to enable logging of important changes to files on NetApp Storage

□ Set System Access Control Lists

- Navigate to the CIFS root shared folder, right-click it and select "Properties"
- Select the "Security" tab > "Advanced" button > "Auditing" tab > Click "Add" button
- Select Principal: "Everyone"; Select "Type: All"; Select "Applies to: This folder, subfolders and files"; Select the following "Advanced Permissions": List folder / read data; Create files / write data; Create folders / append data; Write attributes; Write extended attributes; Delete subfolders and files; Delete; Change permissions; Take ownership
- Click "OK"

□ Configure CIFS Auditing

- Connect to NetApp storage using ssh client.
- Event auditing is turned off by default. If you want to turn auditing on run "[options cifs.audit.enable on](#)". Then enable gathering of:
 - File access events, run "[options cifs.audit.file_access_events.enable on](#)"
 - Logon/logoff events, run "[options cifs.audit.logon_events.enable on](#)"
 - Local account management events, run "[options cifs.audit.account_mgmt_events.enable on](#)"
- When enabled audit log file will be created once a day or when it becomes 75% full of 384mb size, this can be adjusted:
 - Set size of log in bytes, run "[options cifs.audit.logsize 524288-68719476736](#)"
 - Set % threshold run "[options cifs.audit.autosave.onsize.threshold 75%](#)"
- Default audit log file location **etc/log** on storage, it's possible to change it if you run "[options cifs.audit.saveas <fullpath>](#)"

Event ID Reference:

- 560 – Object open
- 562 – Handle closed
- 563 – Object open for delete
- 564 – Object deleted
- 567 – Object access attempt

Full list of events can be found here:

<http://url2open.com/ontapauditing>

□ Audit Event Logs

- Copy log files from the /etc/log folder and run **eventvwr.msc** > Action > Open Saved Log
- Search Security log for event id's listed in the Event ID Reference box

□ For Detailed NetApp Storage Auditing, Try Netwrix Auditor — netwrix.com/go/trial-fs

- **Change auditing:** detection, reporting and alerting on all configuration changes across your entire IT infrastructure with Who, What, When, Where details and Before/After values.
- **More than 200 predefined reports and dashboards** with filtering, grouping, sorting, export (PDF, XLS etc.), email subscriptions, drill-down, access via web, granular permissions and ability to create custom reports.
- **Long-Term Archiving:** scalable two-tiered storage (file-based + SQL database) holding consolidated audit data for up to and beyond 10 years.
- **Unified platform** to audit the entire IT infrastructure, as opposed to multiple hard-to-integrate standalone tools from other vendors.

netwrix
#1 for change auditing

Try NetApp Storage
Auditing for Free:
netwrix.com/go/trial-fs