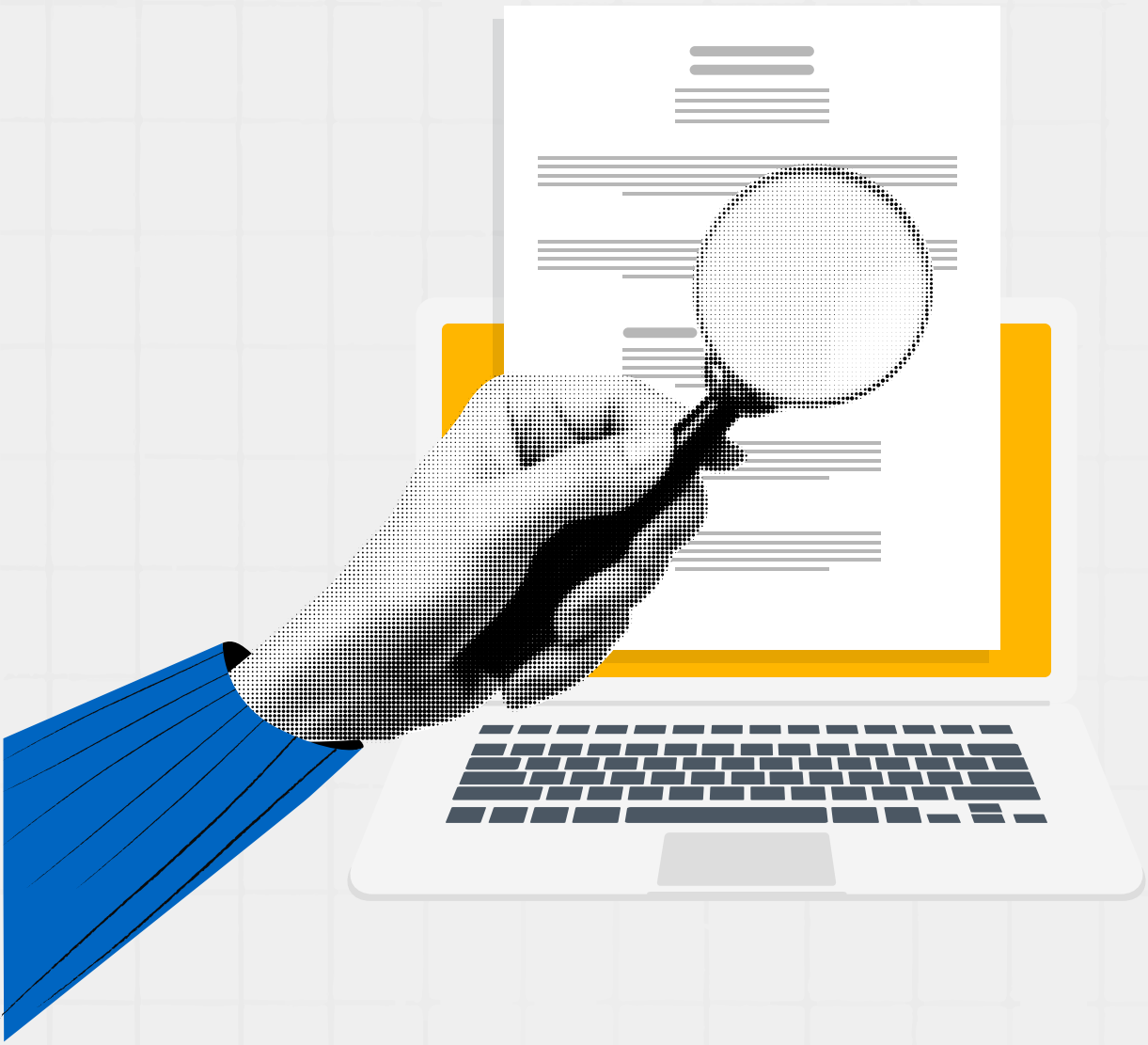
ManageEngine
DataSecurity Plus

NetApp Auditing Guide



www.datasecurityplus.com

Table of Contents

Guide to NetApp auditing with DataSecurity Plus

ManageEngine DataSecurity Plus is a unified data visibility and security platform that identifies sensitive data in NetApp CIFS shares and monitors file activity in NetApp devices. It helps organizations assess and improve their data security posture by identifying sensitive data, evaluating security risks to it, monitoring its usage and movement, and preventing its leakage via endpoints and web applications. Together, these help ensure the all-round protection of data at rest, in use, and in motion from exposure, tampering, and leaks.

DataSecurity Plus consists of these components:

- **The DataSecurity Agent:** A lightweight agent is deployed to collect file change information from FPolicy.

- **Event Processor:** All events that are collected from the NetApp FPolicy are processed here before they are stored in the database or a corresponding alert is triggered. It filters unneeded logs—as configured by the administrator—and normalizes raw logs to standard formats.

- **The DataSecurity Plus console:** The web console enables users to deploy and manage agents, configure monitoring and alerting, and export reports.

Installing and configuring DataSecurity Plus

Prerequisites and supported versions

This document features the FPolicy application for DataSecurity Plus for NetApp storage systems. For help with installing the entire DataSecurity Plus platform, see this help documentation.

DataSecurity Plus can audit file changes in NetApp ONTAP 8.3 and above.

For NetApp server auditing with DataSecurity Plus, configuring a collector server is required. The collector server acts as an intermediary server that collects file access events from the NetApp server and forwards them to the DataSecurity Plus server. This collector server must run Windows Server 2008 R2 and above.

Configure a service account with minimum privileges

Certain minimum permissions and privileges are required by DataSecurity Plus to audit NetApp servers. To provide these, create a dedicated DataSecurity Plus NetApp user and provision them with the following commands and permissions. Note that NetApp management details are necessary for smooth and uninterrupted collection of file activity.

Commands	Permissions
Vserver fpolicy	Full access
Volume	Read only
Vserver cifs	Read only
System node	Read only

To create roles for the user, use the below commands:

- security login role create –role dsp_role –cmddirname “vserver fpolicy”
- security login role create –role dsp_role -cmddirname “volume” –access readonly
- security login role create –role dsp_role –cmddirname “vserver cifs” –access readonly
- security login role create -role dsp_role -cmddirname "system node" -access readonly

Note:

Users can be created for a cluster or a particular Vserver using the above commands. To create a role for a particular Vserver, add -vserver <vserver_name> in the above commands.

Connect the vsadmin role to the ONTAP management console. The user created with this role can either be a domain user or local user, but they should have access to the target NetApp server via ONTAPI.

Configuring a NetApp server

To configure a NetApp server, follow the steps listed below:

1. Log in to the **DataSecurity Plus web console.**
2. Configure the domain in which the file server you want to configure is located.
3. Select **File Audit** from the modules drop-down.
4. Go to **Configuration > Data Source > NetApp Server.**
5. Click **+ Add NetApp Server.**
6. Select the target **NetApp Server Name** and click **Next.**
7. Select the **shares** you want to audit and click **Next.**
8. Under *Management Details*, enter the management IP. You can enter the IP of either a Vserver or a cluster, depending on what type your target machine is.
9. Enter the **User Name** and **Password** of the DataSecurity Plus NetApp user account.
10. Specify the **Port Number** through which communication should happen and click **Next.**
11. Under the *Collector Server* tab, choose the **Domain Name** and **Collector Server Name**, specify the **Collector Port**, and click **Next.**
12. The *Review Summary* tab will give you an overview of the configured NetApp server, Shares, Management Details, and the Collector Server. After verifying the details, click **Configure.**

Alerts, notifications, and response actions

You can create and manage web console and email notifications for critical events in your NetApp servers.

For optimal control over alert scopes, DataSecurity Plus supports two types of alerts:

- Global alert profiles, which can be configured for all or a combination of servers.
- Server-specific alert profiles, which are configured individually for specific servers.

Together, these help IT technicians detect access anomalies efficiently while still preventing alert fatigue. Further, responses—in the form of PowerShell scripts, VBScript, executables, and batch files—can also be automated along with a triggered alert to mitigate the potential damage caused by an incident.

For more information on configuring alerts, refer to the File Audit alert configuration help page.

Creating custom reports

While there are numerous built-in reports available for tracking changes made to files and folders, organizations tend to require reports for unique use cases. To achieve this, you can create personalized reports for a particular user, file share, set of actions, or any combination of the filters available in DataSecurity Plus.

There are two types of custom reports:

- Global Reports: These are applied to all configured servers and list details of selected file activities across the selected servers.
- Server-Specific Reports: These are applied to specific servers.

For more information on creating custom reports, refer to the File Audit custom reports help page.

Retention and archiving

You can use the retention policy to define the number of days for which details of triggered alerts will be stored by DataSecurity Plus. This period can be edited by following the steps in the retention policy help page.

At the end of this period, historical alerts will be deleted permanently, however, audit data will be retained.

To manage disk space and limit database growth further, you can configure a suitable data archival schedule. Audit data that is older than a specified time range can be cleared from the primary database, zipped, and archived.

The archive process only moves the data from the database to a secondary location; it does not delete the event data. You will still be able to generate reports and analytics for it by loading the archived events onto the console when necessary.

The archive process will happen automatically at user-specified intervals. The schedule runs at 2am to minimize disruptions to your environment. You can modify this schedule as well as the archive location by following the steps in the archive configuration help page.

Troubleshooting issues in NetApp auditing with DataSecurity Plus

1. How do I resolve the "NetApp server is not connected to FPolicy server" issue?

This issue arises when the NetApp server cannot communicate with the collector server due to firewall restrictions.

The firewall settings should be set to **allow** in the collector server, without which no events will be collected. To resolve this:

Check if inbound rules are allowed in the system where the agent is installed and try again:

- Go to **Control Panel > System and Security > Windows Defender Firewall.**
- Select **Advanced Settings.**
- Right-click **Inbound Rules** and click **New Rule** (under the *Windows Defender Firewall with Advanced Security on Local Computer* section).
- Create a rule with the desired port number to allow the executable to operate.

To learn more about the ports to be configured for the proper functioning of DataSecurity Plus, refer to the port configuration guide.

If the problem persists, contact support@datasecurityplus.com for further assistance.

DataSecurity Plus

ManageEngine DataSecurity Plus is a unified data visibility and security platform. It audits file changes in real time, triggers instant responses to critical events, shuts down ransomware intrusions, and helps organizations comply with numerous IT regulations. It analyzes file storage and security permissions, deletes junk files, and detects security vulnerabilities. Users can assess the risks associated with sensitive data storage by locating and classifying files containing personally identifiable information (PII), payment card information (PCI), and electronic protected health information (ePHI). It also prevents data leaks via USBs, email, printers, and web applications; monitors file integrity; and audits cloud application usage. Together, these capabilities ensure the all-round protection of data at rest, data in use, and data in motion.

To explore these features and see DataSecurity Plus in action, check out the online demo.
To learn more about DataSecurity Plus, visit www.datasecurityplus.com.

Download free trial $ Get a quote

Explore DataSecurity Plus' capabilities

File server auditing
Audit and report on file accesses and modifications, with real-time alerts and automated responses for critical file activities.

Learn more

File analysis
Analyze file security and storage, manage junk files, optimize disk space usage, and identify permission vulnerabilities.

Learn more

Data risk assessment
Discover and classify files containing sensitive data such as PII, PCI, and ePHI by combining content inspection and contextual analysis.

Learn more

Data leak prevention
Detect and disrupt data leaks via USBs, email, web applications, and printers; monitor endpoint file activity; and more.

Learn more

Cloud protection
Track enterprise web traffic and enforce policies to block the use of inappropriate, risky, or malicious web applications.

Learn more

Our Products

AD360 | Log360 | ADAudit Plus | EventLog Analyzer

Exchange Reporter Plus | SharePoint Manager Plus