



CONFIGURATION GUIDE

# THE PRINCIPLE OF LEAST PRIVILEGE FOR FILE SERVER COMPONENTS

# Table of Contents

- 1. Introduction.....3
- 2. Least Privilege Model for File Server Auditing (Windows File Server and NetApp Filer) .....3
  - 2.1. For Windows File Servers ..... **Error! Bookmark not defined.**
    - 2.1.1. What’s Available? .....3
    - 2.1.2. What’s Not Available?.....3
    - 2.1.3. Minimum Rights Required .....3
    - 2.1.4. Adding the Windows File Server with Least Privileges.....4
  - 2.2. For NetApp Cluster Mode .....5
    - 2.2.1. Minimum Rights Required .....5
    - 2.2.2. Adding the NetApp Cluster Mode with Least Privileges .....6
- 3. Support .....8
- 4. Trademarks .....8

# 1. Introduction

The purpose of this document is to detail the minimum rights and privileges required for configuring the Lepide File Server component for auditing and the steps which are needed to complete the configuration for a successful setup.

## 2. Least Privilege Model for Windows File Server Auditing

### 2.1. What's Available?

- a. All File Server Modification reports ie States and Changes.
- b. Permission Analysis.
- c. Alerting and Scheduling.
- d. Full reporting under Web Console.

### 2.2. What's Not Available?

All the features that are available on a Full Privileged Model are also available with the Least Privileged Model. The only difference is the specific rights and configuration that is required to be done.

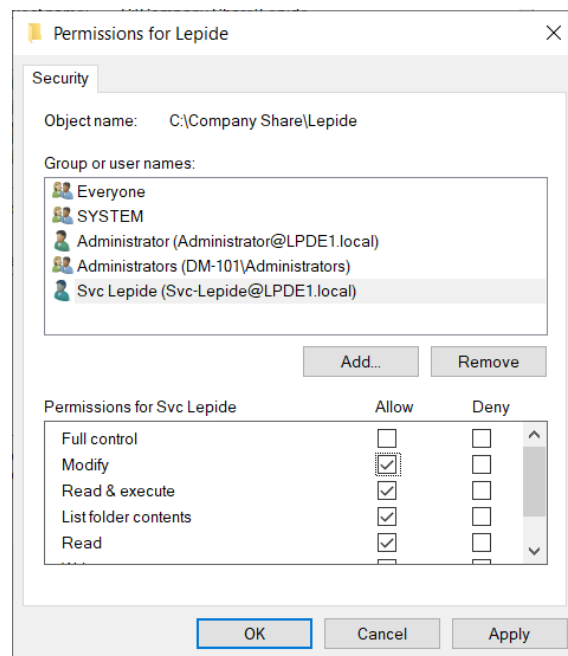
### 2.3. Minimum Rights Required

- a. A Domain User Account.
- b. This account should have db\_owner and db\_creator rights over the SQL databases. An SQL account with the mentioned privileges can also be used.
- c. This account should be a member of the Local Administrators Group on the File Server.
- d. This account should be a member of the Local Administrators Group on the Lepide Server.
- e. This account should have List Folder/Read Data, Traverse Folder/Execute File and Read Permissions rights on the Shares which are to be audited.
- f. This account should be used to Logon to the Lepide Server to Configure the File Server for Auditing.
- g. The SYSTEM account should have Modify rights on the folder where the agent is installed.

## 2.4. Adding the Windows File Server with Least Privileges

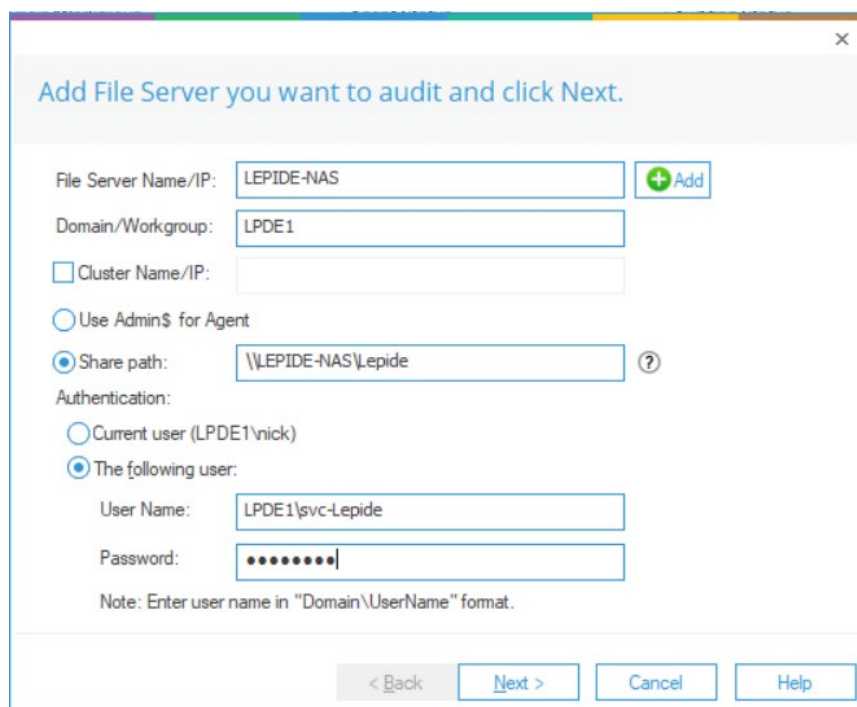
Follow the steps below to add a File Server with the Least Privileges:

1. Create a Shared Folder on the File Server and assign **Modify** rights to the Domain User account.



**Figure 1: Permissions**

2. Add the file server with the Name or IP and provide the path to the Shared folder in the column **Share Path** instead of selecting **Use Admin\$ for Agent**. Also, provide the user account created in the fields given at the bottom of the window.



**Figure 2: Add File Server**

3. The next steps are similar to the Full Privilege Model installation.
4. Permission Analysis can also be done in the same way once the rights are adjusted according to Section 3.1.2 above.

## 3. For NetApp Cluster Mode

Everything, except the **Permission Analysis Module** is available for NetApp Filers in the Least Privilege Model.

### 3.1. Minimum Rights Required

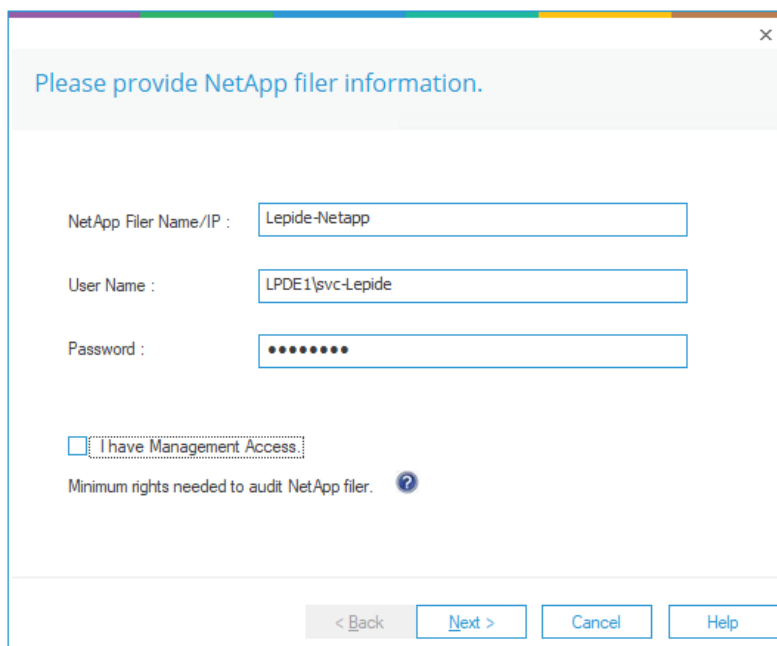
- a. A Domain User Account.
- b. This account should have db\_owner and db\_creator rights over the SQL databases. An SQL account with the mentioned privileges can also be used.
- c. This account should have **Change** Permission on the C\$ in NetApp.
- d. This account should have Modify Rights on the Audit Log Volume.
- e. This account should be a member of the Local **Administrators** Group on the Lepide Server.

- f. This account should be used to Logon to the Lepide Server to Configure the File Server for Auditing.

## 3.2. Adding the NetApp Cluster Mode with Least Privileges

To add the NetApp File Cluster Mode for auditing, the native auditing should be enabled manually, and it should meet the following pre-requisites:

- a. The minimum Log File Size (rotate-size) should be 1 MB.
  - b. The format of auditing should be XML.
  - c. The size of selected audit log volume should be at least 2 GB.
  - d. The rotate limit should be applied to the auditing configuration.
1. On the first page, provide the IP address and the domain user account. Please ensure to **Uncheck** the **I have Management Access** option.



The screenshot shows a configuration window titled "Please provide NetApp file information." with a close button (X) in the top right corner. The window contains the following fields and options:

- NetApp File Name/IP :** A text box containing "Lepide-Netapp".
- User Name :** A text box containing "LPDE1\svc-Lepide".
- Password :** A text box with masked characters (dots).
- I have Management Access :** A checkbox that is currently unchecked.
- Minimum rights needed to audit NetApp filer.** A text label followed by a question mark icon.

At the bottom of the window, there are four buttons: "< Back", "Next >", "Cancel", and "Help".

**Figure 3: NetApp Filer Information**

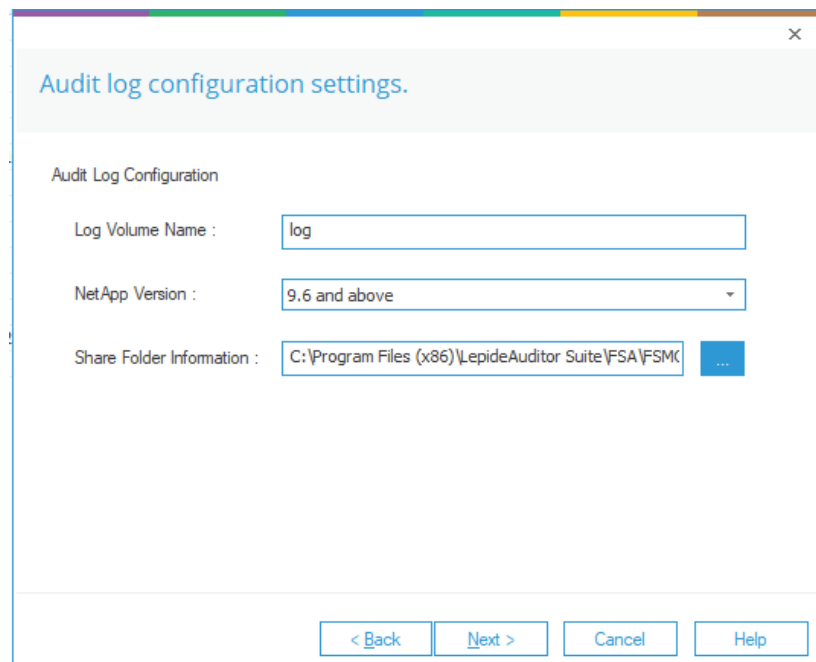
2. In the Least Privilege Model, the **ShareInfo.txt** file is not created itself by the solution. The users will have to create this file manually in a txt format and should have the entries like this for every Share:

**SharePath#JunctionPath#ShareName**

**Share Path:** This can be taken from the OnTap Manager in the Share section.

**Junction Path:** This can be taken from the OnTap Manager in the Volume section

3. On the next page, please provide the audit log volume details along with the version of the NetApp and the location of the **ShareInfo.txt** file.

The image shows a screenshot of a software window titled "Audit log configuration settings." with a close button (X) in the top right corner. The window contains a section labeled "Audit Log Configuration" with three input fields: "Log Volume Name" with the text "log", "NetApp Version" with a dropdown menu showing "9.6 and above", and "Share Folder Information" with the text "C:\Program Files (x86)\LepideAuditor Suite\FSA\FSMC" and a browse button (three dots). At the bottom of the window are four buttons: "< Back", "Next >", "Cancel", and "Help".

**Figure 4: Audit Log Configuration Settings**

4. All the other steps are the same as the Full Privilege Model where the next step is to put in the SQL server details where the audit logs will be stored.

## 4. Support

If you are facing any issues whilst installing, configuring or using the solution, you can connect with our team using the below contact information.

### Product Experts

USA/Canada: +1(0)-800-814-0578

UK/Europe: +44 (0) -208-099-5403

Rest of the World: +91 (0) -991-004-9028

### Technical Gurus

USA/Canada: +1(0)-800-814-0578

UK/Europe: +44 (0) -208-099-5403

Rest of the World: +91(0)-991-085-4291

Alternatively, visit <https://www.lepide.com/contactus.html> to chat live with our team. You can also email your queries to the following addresses:

[sales@lepide.com](mailto:sales@lepide.com)

[support@lepide.com](mailto:support@lepide.com)

To read more about the solution, visit <https://www.lepide.com/data-security-platform/>.

## 5. Trademarks

Lepide Data Security Platform, Lepide Data Security Platform App, Lepide Data Security Platform App Server, Lepide Data Security Platform (Web Console), Lepide Data Security Platform Logon/Logoff Audit Module, Lepide Data Security Platform for Active Directory, Lepide Data Security Platform for Group Policy Object, Lepide Data Security Platform for Exchange Server, Lepide Data Security Platform for SQL Server, Lepide Data Security Platform SharePoint, Lepide Object Restore Wizard, Lepide Active Directory Cleaner, Lepide User Password Expiration Reminder, and LiveFeed are registered trademarks of Lepide Software Pvt Ltd.

All other brand names, product names, logos, registered marks, service marks and trademarks (except above of Lepide Software Pvt. Ltd.) appearing in this document are the sole property of their respective owners. These are purely used for informational purposes only.

Microsoft®, Active Directory®, Group Policy Object®, Exchange Server®, Exchange Online®, SharePoint®, and SQL Server® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

NetApp® is a trademark of NetApp, Inc., registered in the U.S. and/or other countries.