CONFIGURATION GUIDE

NETAPP FILE SERVER QUICK START GUIDE

Table of Contents

1	Intro	oduction	duction					
2	Req	uirements	and Prerequisites	3				
	2.1	Basic Syst	tem Requirements	3				
	2.2	Supporte	d Servers for Auditing	4				
3	Neta	app 7 - Mo	de	4				
	3.1	Prerequis	sites to Audit NetApp 7-Mode	4				
	3.2	Required	User Rights	4				
		3.2.1	Service Rights	4				
		3.2.2	Local System Rights	5				
	3.3	Add NetA	pp 7-Mode	5				
4	Neta	app Cluste	r Mode	12				
	4.1	Prerequis	sites to audit NetApp Cluster Mode	12				
	4.2	Recomme	endations for NetApp Cluster Mode	13				
	4.3	Add NetA	pp Cluster Mode	13				
	4.4	Steps afte	er Adding a File Server Component	18				
5	Sup	port		23				
6	Trac	lemarks		23				

1 Introduction

The Lepide Data Security Platform provides a comprehensive way to provide visibility across Active Directory, Group Policy, Exchange on-premises, M365, SharePoint, SQL Server, Windows File Server, NetApp Filer, and every platform which can provide an integration with Syslogs and RestAPI.

This guide takes you through the process of standard configuration of the Lepide Data Security Platform for NetApp File Servers.

If you have any questions at any point in the process, you can contact our Support Team. The contact details are listed at the end of this document.

2 Requirements and Prerequisites

Before you start installing the Lepide Data Security Platform for File Server, make sure that your computer meets the following requirements.

2.1 Basic System Requirements

- Required Processor
 - Minimum dual-core processor
 - Recommended quad-core processor
- Required RAM
 - Minimum 4 GB RAM
 - Recommended 8 GB RAM
- Required free disk space
 - Minimum 1 GB
 - Recommended 2 GB
- Any of the following 32-bit or 64-bit Windows Operating Systems.
 - Windows Server OS: Any Server above and including 2008 R2
- Any of the following SQL Servers (local or network hosted) for storing auditing logs:
 - Any SQL Server above and including SQL Server 2005 (standard or enterprise)
- .NET Framework 4.6 or later

2.2 Supported Servers for Auditing

Audited Servers	Supported Versions			
NetApp Filer	NetApp 7-Mode Configuration			
	 o Lepide Data Security Platform for File Server successfully audits and report events from NetApp Filer with Data ONTAP™ 7.2 or later. 			
	 The recommended version for the availability of all features is ONTAP 7.3.4 or later. 			
	 NetApp Cluster Mode Configuration (CIFS Protocol only) 			
	o 8.2.3 Clustered Data ONTAP or later.			

3 Netapp 7 - Mode

3.1 Prerequisites to Audit NetApp 7-Mode

- The agent to audit NetApp Filer can be installed on any client system or domain controller, but it requires GPMC.MSC (Group Policy Management Console) for installation.
- If you need the Permission Analysis of NetApp Filer, then we recommend you use synchronous mode to connect to NetApp Filer.

3.2 Required User Rights

To install and work with Lepide, you need to have appropriate rights to the system where it will be installed. You will also need to have appropriate rights to access Active Directory, SQL Server, Windows File System, and NetApp Filer.

3.2.1 Service Rights

To run the service of Lepide after installation, you can select any of the following:

- A local system administrator
- A member of Domain Admins Group
- Manage Service Account object

3.2.2 Local System Rights

The user should have the following permissions on the local computer where the software is installed:

- Full access permission to the drive on which Operating System is installed
- Read/Write permissions in the registry

3.3 Add NetApp 7-Mode

After you have installed the Solution and configured the Lepide service to run with administrative credentials, you can add a NetApp File Server for auditing.

											- 8 ×
	Settings										
	Component Management Eile Sequerr	Add Compone	nt								
8	General Settings										^
	- Delegation Control										
			Active Directory, Group		SharePoint Server		SQL Server	File Server		Exchange Online	
3			Vice Password Expiration Reminder and Active	S>		\square			E		
1	DSP Report Viewer (beta)	20	Directory Cleaner						Online		
			•								
			SharePoint Online		Cloud Components		Office 365	Session Recording		Universal Audit	
-		S>									
									XQ		
ន											~
		Added Compo	nent								
*											
2											
ø											
^											
	< >>				-						

Figure 1: Component Management Window

From the Component Management window, under the Add Component section, click on the File Server icon to add this component to the solution.

Tho	Eilo	Sorvor	Cottings	Concolo	dialog	hoy ic	dicplay	od.
me	гпе	Server	Settings	CONSOLE	ulalug	DOY 12	uispia	eu.

LepideDSP for File Server - Settings Co	nsole				- 0
Add File Server + ? Help					
LepideDSP for File Server					
File Servers	Overview of file server	configuration. Use options to add, modify	file servers and options in tasks pane f	for other settings.	
Audit Policies					
					○
	Hie Server Name/IP	Domain/Workgroup	Agent Status	Auditing Status	Tasks
					Port Settings
					S Refresh
					Install Agent
					Uninstall Agent
					Stan Auditing
					Stop Additing
					Service Rights
					Domain Controller(s)
					📚 Data Classification Settings
					Audit Notification: OFF
	<		Ш		>
	File servers are the	machines that are being audited for change	es. Agent must be installed and auditin	ng should be started to audit all the chang	es performed on file servers.
Visit http://www.lepide.com/file-serv	er-audit/				CAP NUM SCR
Here, you can cl • Winc	ick Add File Ser lows File Server	ver icon 🕀 🔹 c	n the toolbar to	o add either of the	e following file servers:
• NetA	pp Filer				
		-			
1 Click th	Add Eilo Sorv	ericon 😌 🔻 se	lect Single ther	soloct NetAnn 7	Mode
I. CIICK UI	e Auu File Sel V	er icon, se	lect single the	i select iverApp /	-Mode.
	c	- <i>≥</i> ×			
		Single 🕨 🕨	Windows		
		Multiple 🕨 🖡	Netapp 7-Mod	e	
		M Defred	Netapp Cluster	r Mode	
		× Kerresi	1		
		📑 Install	Agent		

Figure 3: Option to Add Netapp 7-Mode File Server

2. The **Add File Server** wizard starts:

File Server Name/IP:		 🔂 Add]
User Name:			
Password:			

Figure 4: Select File Server Type

3. Either enter the name or IP Address of NetApp Filer Name manually or click **Add** to select a NetApp Filer from the network.

Add File Server from Dor	nain.			×
Select Domain : Select-		*	Find	
Name		Distinguishe	d-Name	
Q	Q			9
< III				>
L				
ОК	Can	cel		

Figure 5: Select a NetApp Filer



- 4. Here, you can select a domain name and click **Find** to list the available Filers in it.
- 5. Select a NetApp Filer and click **OK**.
 - 6. After the required NetApp Filer is selected, enter the login credentials of a NetApp Administrator to add it.
- 7. Click **Next** to go to the next step, to provide the details of SQL Server to create a database for storing auditing logs.

Please provide SC	L Server informatio	n.		×
Server Name : 192.168	.40.238		Browse	
Insert audit data directly to	database from file server :		Yes 🔹	0
OWindows Auther	tication O SQL Server A	uthenticatior	n(Recommended)	
User Name :	sa			
Password :	•••••		Test Connectio	on 🖻
NOTE: Windows authent Database Option :	ication credentials only applicabl	e for insert d	ata from file serve	r directly.
 Create Database 	LepideFSA DB			
O Select Database	<select database=""></select>	×		
NOTE: If you do not have	SQL Server installed then click	this link to d	ownload SQL Exp	ress edition.
https://www.mic	rosoft.com/en-in/download/deta	ails.aspx?id=	56840	
	< <u>B</u> ack	<u>V</u> ext >	Cancel	Help

Figure 6: SQL Server Details to add NetApp Filer

- 8. Click the Server Name dropdown to select the desired SQL Server.
- 9. There are two authentication options available:

Windows Authentication: This mode can be selected if SQL Server is installed on the same computer where the solution is installed.

SQL Server Authentication: Select this mode if SQL Server is installed on a remote or local computer. We recommend that this option is selected.

Provide the username and password of a SQL user, who has sufficient rights to create the database.

- 10. Enter a database name in the database name field to create a new database. You can also select an existing database created earlier by Lepide or another application.
- 11. Click Next



The NetApp Agent Information dialog box is displayed:

	NetApp Agent Information		×			
Enter agent server details and click Next.						
This agent server will collect changes from the NetApp filer.						
Server Name/IP:						
User Name:	User Name: COD\Administrator					
Password:	Password: ••••••					
Connection Type:	Connection Type: Asynchronous Synchronous					
Note: * Use "Doma * Agent Server sy	Note: * Use "Domain\UserName" format for User Name. * Agent Server system is used to install file server agent.					
Automatically change required agent server settings						
< <u>B</u> ack <u>N</u> ext > Cancel Help						

Figure 7: NetApp Agent Information

12. Enter the details of the system where you wish to install the agent to collect the changes from NetApp Filer.

NOTE: You can install the agent on another system apart from NetApp Filer. However, it is important to note that the agent can only be installed on any one client system or the domain controller. We recommend that you do not to install it on workgroup computers and the agent is installed only on the domain connected Windows Computer and not on NetApp Filer.

- 13. Enter the name or IP Address of the agent system.
- 14. Provide the Username and Password of an administrator of the agent system to allow access to the software to install the agent.



- NOTE: The provided user should be a member of Administrators, Domain Admins, Group Policy Creator Owners, Enterprise Admins, and Schema Admins groups, at the agent system, to enable the auditing of NetApp Filer. If the above rights are not assigned to the user, then follow the steps below.
 - a. Go to Administrative Tools.
 - b. Open Active Directory Users and Computers.
 - c. Select User Properties.
 - d. Go to Member Of \rightarrow Add Group.
 - e. Select any of the following groups as per the above requirements.
 - i. Administrators
 - ii. Domain Admins
 - iii. Group Policy Creator Owners
 - iv. Enterprise Admins
 - v. Schema Admins
 - f. Click Apply and OK
 - 15. Now you need to choose the Connection Type. Lepide provides the following two types of connections with the NetApp Filer from the agent:
 - a. Asynchronous: This option is quick, but it cannot capture security details. It captures the security events but does not show details.
 - b. Synchronous: This option captures security details, but the process slightly slows down the performance of the Filer.

NOTE: If you need the Permission Analysis of NetApp Filer, we recommend using synchronous mode to connect to NetApp Filer.

- 16. Certain changes are required in the Local Security Policies to allow the software to audit Filers. The software provides a checkbox to make such changes automatically from its end.
- 17. If you do not want to go for automatic changes or face an error in applying these changes automatically, then uncheck this option and make these manually.
- 18. Click the checkbox to make the changes automatically. The software displays the list of required changes in the next screen and reconfirms it.



NetApp Agent Information	×
 Following settings need to be changed on agent system to connect with the NetApp filer Network access: Let Everyone permissions apply to anonymous users:- Enable Network access: Restrict anonymous access to Named Pipes and Shares:- Disable Network access: Shares that can be accessed anonymously:- add NTAPVSRQ. Please reboot the agent system if reports are not being generated after change settings. Do you want to change these settings now? 	
<u>Y</u> es <u>N</u> o	

Figure 8: List of Changes to be made for Auditing NetApp Filer

19. Click **Yes** to make these changes and to install the agent.

If you click **No**, then the changes will not be made, but still, the agent will be installed. Because of no agent installation, the audit reports will not be generated in this case.

To generate the audit reports after clicking **No**, you must make these changes manually.

itatus				
atus:				
Installing Agent for 192.168.40.2	242 The	operation complet	ed successfully.	
<	III			

Figure 9: Installing the Agent for NetApp Filer

20. Click **Finish** to complete the process.

4 Netapp Cluster Mode

4.1 Prerequisites to audit NetApp Cluster Mode

- Please verify the settings on the NetApp Cluster Mode before installing the agent.
- Ensure that the time on NetApp Cluster Mode is synchronized with the time on the computer where the solution is installed to get precise report timings.
- When you install the agent for NetApp Cluster Mode, use only the NetApp domain user.



4.2 Recommendations for NetApp Cluster Mode

In NetApp, the auditing framework is provided by Data ONTAP. It is similar to the auditing performed on Windows® Servers. This feature was available from the early versions of Data ONTAP, but NetApp itself recommends using Data ONTAP version 8.2.3 or higher, which is the same as we recommend.

Auditing can be enabled on either CIFS shares or NFS exports.

- **CIFS Auditing**: It refers to auditing access events from NetApp filers through Windows clients/Mac OS, which allows data access on the storage system using the CIFS protocol.
- **NFS Auditing**: It refers to auditing access events from NetApp filers through UNIX/Linux® clients, which allows data access on the storage system using the NFS protocol. We currently do not support the auditing of the NFS Shares.

4.3 Add NetApp Cluster Mode

Follow the steps below to add NetApp Cluster Mode for auditing.

1. Click the Add File Server button on the toolbar and click NetApp Filer.



Figure 10: Option to Add File Server

You can also click the 😌 🕆 icon in the Right Panel, go to **NetApp Filer** sub-menu and click **NetApp Cluster-Mode**.

~

The Wizard to add **NetApp Cluster Mode** is displayed:

Plazza provida NatApp filor information

		^
Please provide Net/	App filer information.	
NetApp Filer Name/IP :	Netapp-Corp20]
User Name :	Corp\administrator]
Password :	•••••]
Enable remote agent a	uditing	0
 I have Management A Minimum rights needed to 	Access. audit NetApp filer.	
	< <u>B</u> ack <u>N</u> ext > Cancel	Help

Figure 11: Wizard to Add NetApp Cluster Mode

- 2. Add the following details:
 - a. **Domain Name:** Enter the name or IP Address of the domain, where the NetApp Cluster Mode is located, in the **Domain** text field.
 - b. User Name: Enter the name of a user, who is a member of **Domain Admins** group.
 - c. **Password**: Enter the password of the selected user.
 - d. Check the Box which says, I have Management Access.
- 3. Click Next

The Add File Server dialog box is displayed:



		×
Audit log configur	ation settings	
Addit log conligui	adon settings.	
User Name :	vsadmin	
	Enter user name assigned with vsadmin role	
Password :	•••••	
Audit Configuration :		
Manual 🕜		
Volume Name :	Enter volume name (case sensitive). Detect	
-		
 Automatic 		
Volume Name :	cifs_logs	
Aggregate Name :	aggr 1	
	< Back Next > Cancel He	elp

Figure 12: Audit Log Configuration Settings

- 4. Add the following details:
 - a. **User Name**: Enter the name of a user, who has vsadmin role. You can use the default vsadmin user as well.
 - b. **Password:** Enter the password of the selected user.
 - c. **Audit Configuration**: Select **Automatic Auditing**. Select this option if you have not already configured auditing. You need to provide the following inputs:
 - Volume Name
 - Aggregate Name
- 5. Click **Next** to proceed. The Solution enables auditing with the following settings:
 - Log Volume Size :3 GB
 - Log format: XML
 - Log File Size: 1 MB

NOTE: The Lepide Data Security Platform needs at least 3 GB of free space at the selected aggregate to enable the auditing automatically.



Add File Serve	er		×
V V	nable to create volume. 'aggr1 server SVM832_04May.	' aggregate is not in aggregate list of	
		ОК	
	Figure 13: Error Message while	e Enabling Automatic Auditing	
solve this iss	ue, add the aggregate in the	Vserver's list by the following comm	and:
erver modi	fy -vserver <server_r< td=""><td>ame> -aggr-list <aggregate< td=""><td>value></td></aggregate<></td></server_r<>	ame> -aggr-list <aggregate< td=""><td>value></td></aggregate<>	value>
see whether	the aggregate has been add	led to the list, use the following com	mand:

- 6. Click Next
- 7. The **SQL Server Information** dialog box is displayed. Here, you need to provide the details of SQL Server to create a database for storing auditing logs.

Please provide SQL	Server information.	×
Server Name : 192, 168, 40	242	Browse
Insert audit data directly to dat	abase from file server :	No 🔻
Windows Authentical	tion SQL Server Authenticatio 	n(Recommended)
User Name : sa		
Password :	•••••	Test Connection
NOTE: Windows authenticati	on credentials only applicable for insert d	lata from file server directly.
Database Option :		
 Create Database 	LepideFSA DB]
Select Database	<select database=""></select>	
NOTE: If you do not have SG	L Server installed then click this link to d	lownload SQL Express edition.
https://www.microso	ft.com/en-in/download/details.aspx?id=	56840
	< <u>B</u> ack <u>N</u> ext >	Cancel Help

Figure 14: SQL Server Details to Add NetApp Cluster Mode

8. Click the Server Name dropdown to select the desired SQL Server.

There are two authentication options under it:

- a. **Windows Authentication**: This mode can be selected if SQL Server is installed on the same computer where the solution is installed.
- b. **SQL Server Authentication**: Select this mode if SQL Server is installed on a remote or local computer. We recommend that this option is selected.
- 9. Provide the username and password of a SQL user, who has sufficient rights to create the database.
- 10. Enter a database name in the database name field to create a new database. You can also select an existing database created earlier by Lepide or another application.
- 11. Click Next

The installation of the agent starts:



Status			-	×
Status:				
Tasks Installing Agent for 192.168.40.	242 The o	s peration complete	ed successfully.	
<	III			>
	< <u>B</u> ack	Finish	Cancel	Help

Figure 15: Install Agent on NetApp Cluster Mode

12. Click **Finish** to complete the process.

4.4 Steps after Adding a File Server Component

A dialog box is displayed asking whether you want to apply a rule to the newly added file server:



Figure 16: Add Rule to the File Server Wizard



13. Click **Yes** and create a new rule from the next window.

NOTE: You need an Audit Rule to start monitoring of the newly added File Server. If you want to skip the step of creating a rule, then click **No**. However, the audit reports will not be generated until you create an Audit Rule and update the agent. It is necessary to **Update Agent** if you are creating or modifying an Audit Rule.

		×
Enter audit rul click Next.	e name and select file server to apply this rule and	
Create new rule or se	lect existing rule to apply on selected file server(s).	
Create new ru	le	
Use existing n	ıle	
Rule Name :	Test Rule	
File Servers :	192.168.40.242 ×	
	< Back Next > Cancel Help	

Figure 17: Enter Rule Name and Select File Server

- 14. Enter a rule name and select the File Server for which you want to create the rule if it is not already selected in the **File Servers** drop-down menu.
- 15. Click **Next**. The audit policies dialog box is displayed:

				×
Select the policy type new policy using opt	that will be ap ion in drop dov	plied in this vn.	rule. You ca	an create
Select Policy Type	dit All	*		
Individual User Policy	ar Ai			
0,				

Figure 18: Audit Policies

NOTE: In this example, we are creating an audit rule with predefined policy. To create an auditing rule with a user- configured policy refer to the Advanced File Server Configuration Guide.

For this example, we will select the Audit All policy:

				×
Select the policy t new policy using	ype that will be ap option in drop dov	oplied in thi wn.	is rule. You	can create
Select Policy Type				
 Selected Policy 	Audit All	*		
O Individual User P	blicy			
Group Policy				
	< Back	Next >	Cancel	Help

Figure 19: Select Policy Type

16. Click Next

			×
Add users to audit in this	s rule and click Next.		
Select user or group to audit			
Audit User : All users	*		
Name	Туре	Add User	
		Add Group	
		Remove	
<			
	< <u>B</u> ack <u>N</u> ext > C	ancel Help	

Figure 20: Add Users to Rule

- 17. Select **All Users** in the **Audit User** tab and click **Next**. The rule is applied to all users in this case.
- 18. Click Next

The Summary box is displayed:



				×
Summary				
Rule Name: Test Rule				^
File Servers: 192.168.40.242				
Policy Type: Selected Policy -> Audit All				
Audit User: All Users				
1				
				~
<				>
	< Profe	Dininh	Caraal	Uala
	< <u>в</u> аск	Finish	Cancel	нер

Figure 21: Summary

- 19. Click **Finish** to complete the process. The newly added audit rule is displayed in the list.
- 20. Click **Update Agent on all File Servers to apply new Settings** notification and follow the on-screen instructions to update the agent.

NOTE: It is necessary to update the agent each time you change the applied Audit Rule. If this is not done, the auditing will not be updated, and the reports will not include the new modifications when generated.

21. After you have created the auditing rules, Restart the main console, and go to the **Audit Reports** tab in the main panel to view the reports.



5 Support

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

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

sales@Lepide.com

support@Lepide.com

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

6 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.

