LEPIDE DATA SECURITY PLATFORM

Principle of Least Privilege

Table of Contents

1. Introduction

The purpose of this document is to detail the minimum rights and privileges required for configuring the specific components for Auditing and the steps which are needed to complete the configuration for a successful setup.

2. Least Privilege Model for Active Directory, Group Policy and Exchange On-Premises

2.1 What's Available?

a. All AD/GPO/Exchange Modification reports, i.e. States and Changes.

b. Real time alerts and Schedules.

c. Full reporting under Web Console.

d. AD and GPO Backups.

e. AD and GPO State Reports.

f. Lepide Active Directory Cleaner.

g. Lepide User Password Expiration Reminder.

h. All AD/GPO Risk Analysis Reports.

i. Agent-Less Auditing

2.2 What's Not Available?

a. AD and GPO Restore.

b. Non-Owner Mailbox Auditing under Exchange.

c. Health Monitoring.

d. Automatic Enabling of the Native Auditing from the DCs. (This is a one time process and can be done manually)

e. Automatic Event Log Management of the DCs.

f. Data Discovery and Classification of Exchange Mailboxes.

g. Agent Based Auditing.

2.3 Minimum Rights Required

a. A Domain User Account.

b. This account should have Db_owner/Db_creator rights over the SQL databases. An SQL account with the mentioned privileges can also be used.

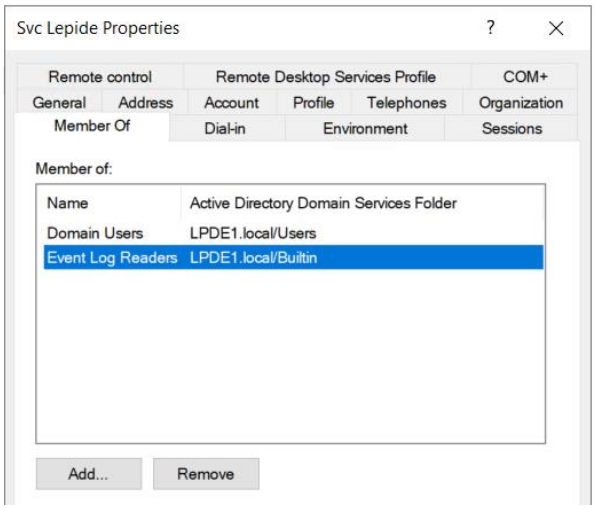
c. This account should be a member of the "Event Log Readers" group inside AD.

d. This account should be a member of the "Administrators" Group on the Lepide Server.

e. This account should be a member of "Organization Management" group inside AD for Exchange Auditing.

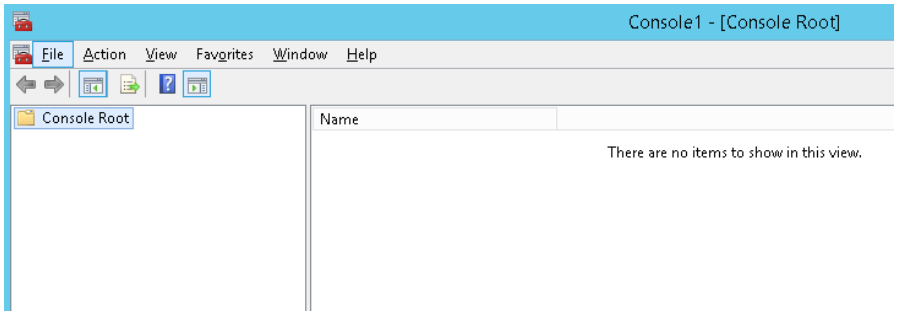
2.4 Setting up the Account Privileges

1. Create a user account in AD and add under "Event Log Readers" group.

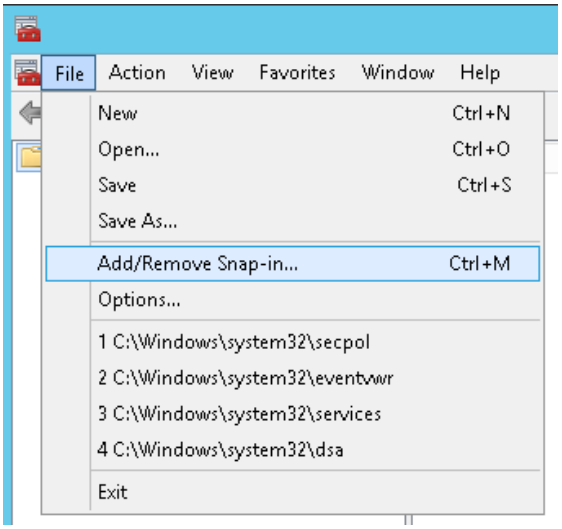


2. Add this user account under the "Local Admin Group" on the Lepide Server. To do this, follow the below steps:

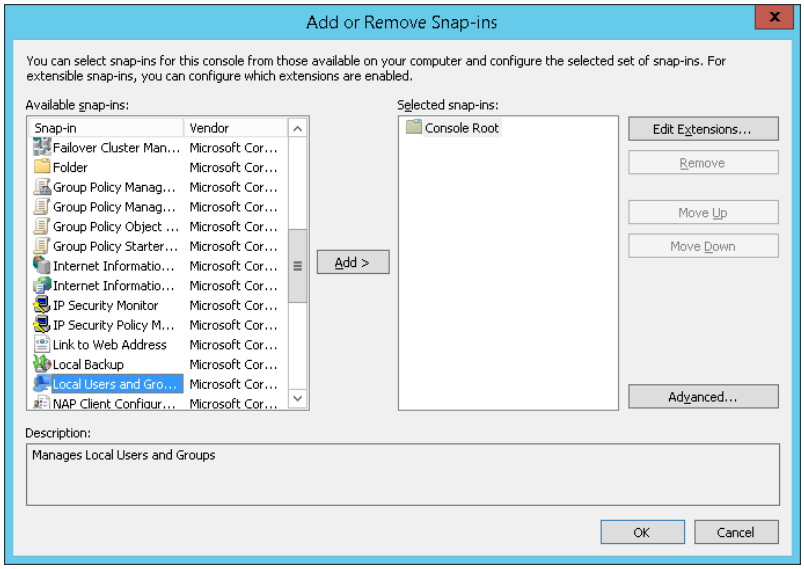
   2.1. In the run window, type mmc and press enter. You will get following screen:



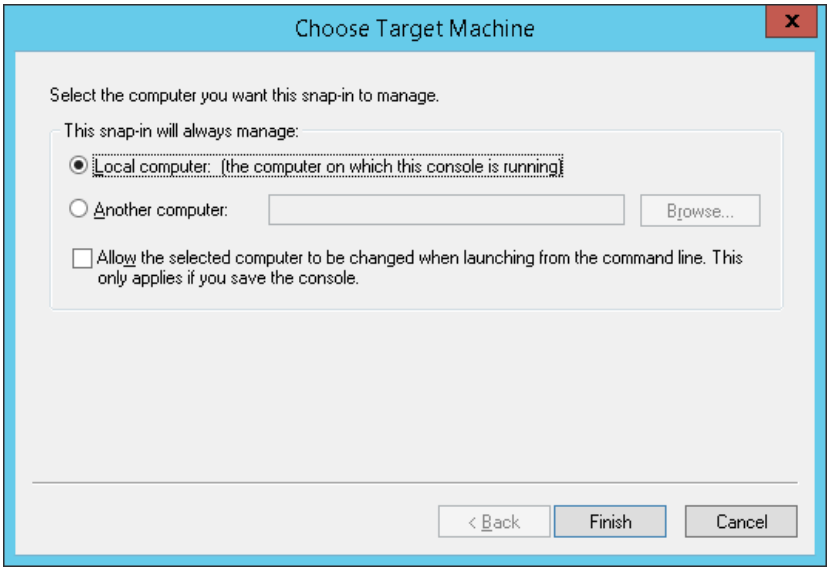
2.2. Select Add/Remove Snap-IN.



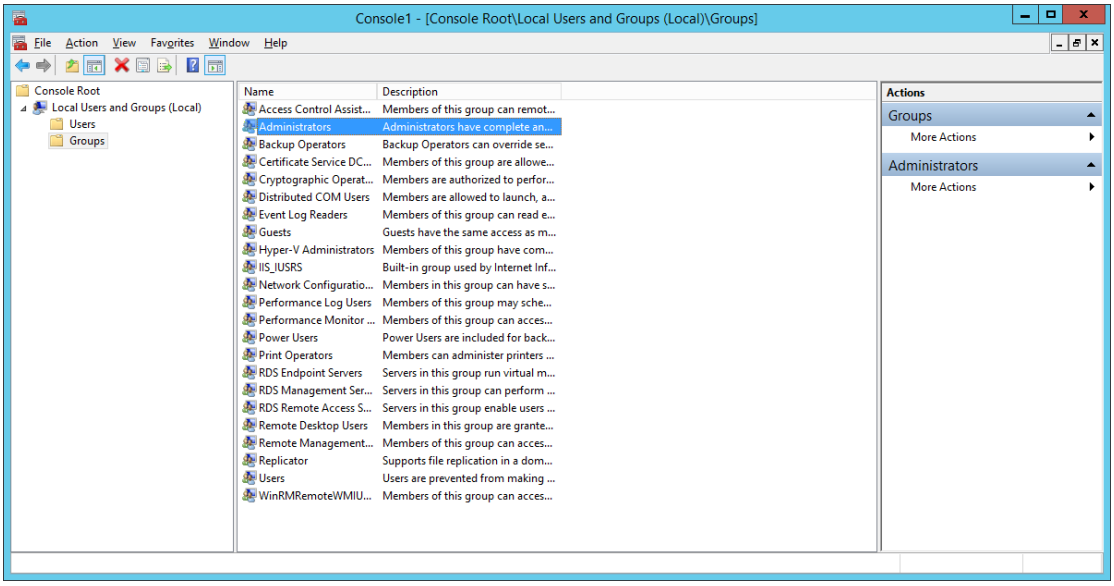
2.3. After selecting this you will get following screen:



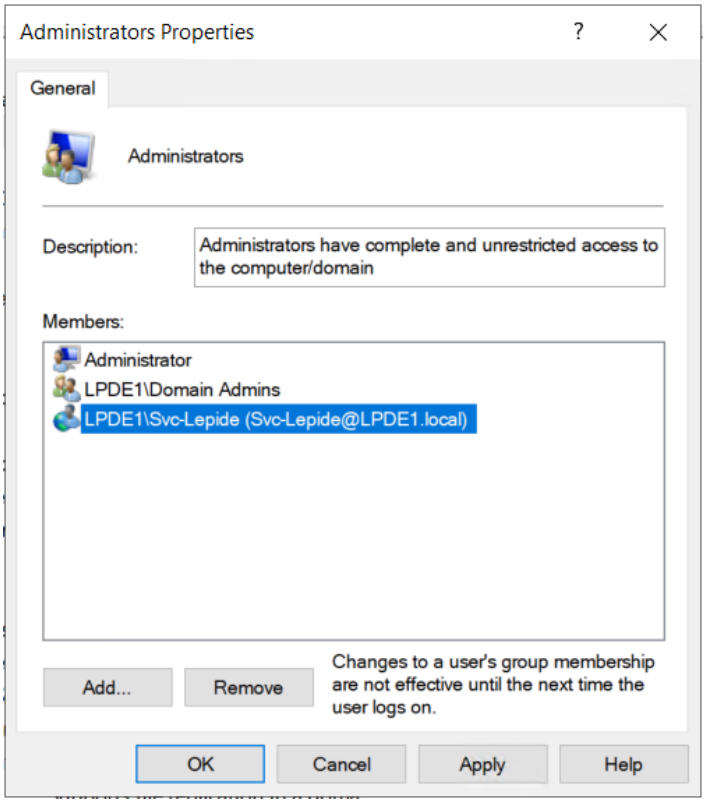
2.4. Click Add from the above screen and select the first option. Click the finish button.



2.5. When the "Choose Target Machine" wizard is closed, the "Local Users and Group" node is added in the console. Select Administrator from the right pane and double click.



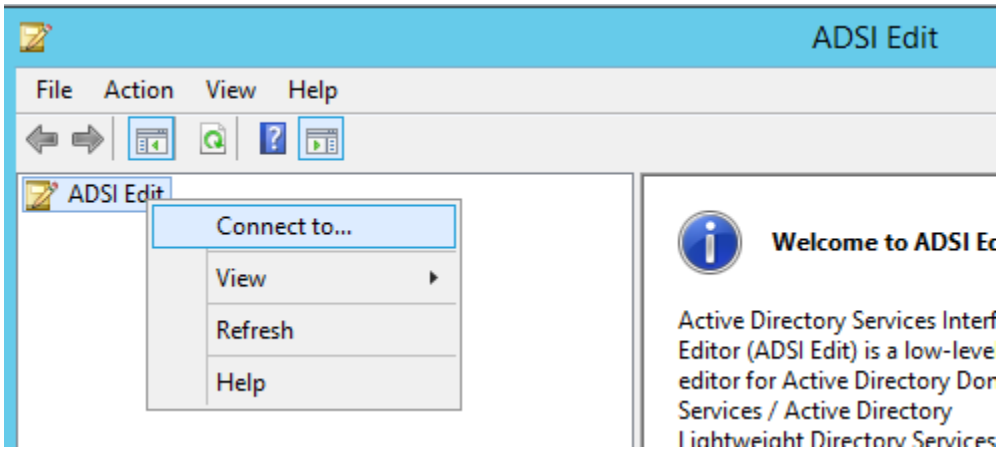
2.6. In the Administrators properties window, add the newly created user with default access rights.



3. Log in on the Lepide Server through the newly created user credentials.

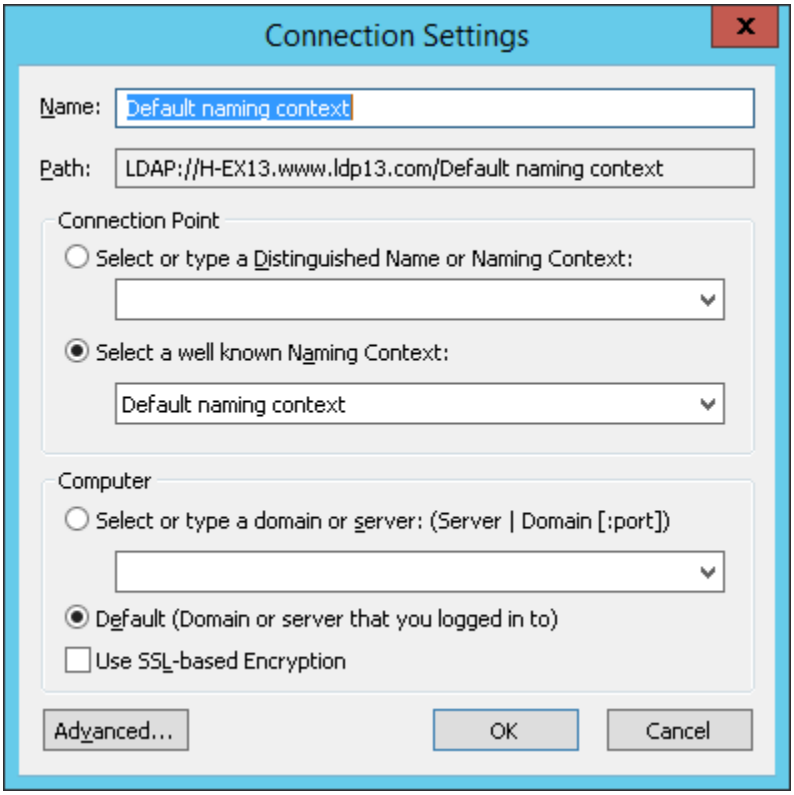
4. Open ADSIEdit and provide access rights to the newly created user over different naming context of active directory. To do this follow these steps:

4.1. Type ADSIEDIT.msc into run and press enter:

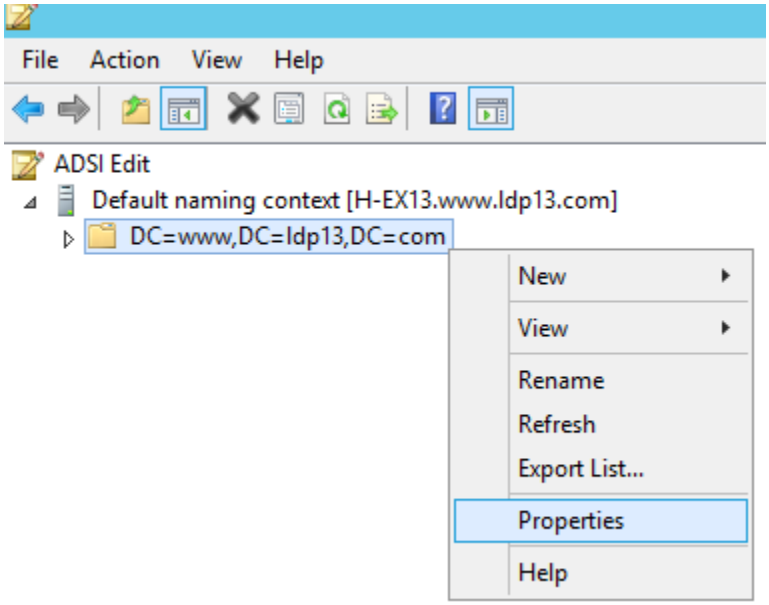


4.2. Right click on ADSI Edit node and Select “Connect to...”.

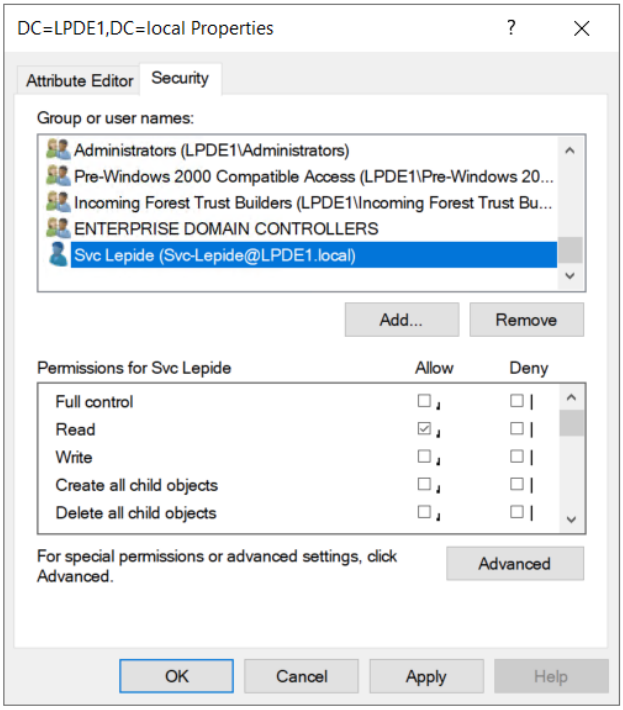
4.3. From the Connection Settings dialog, select “Default naming context” and click OK:



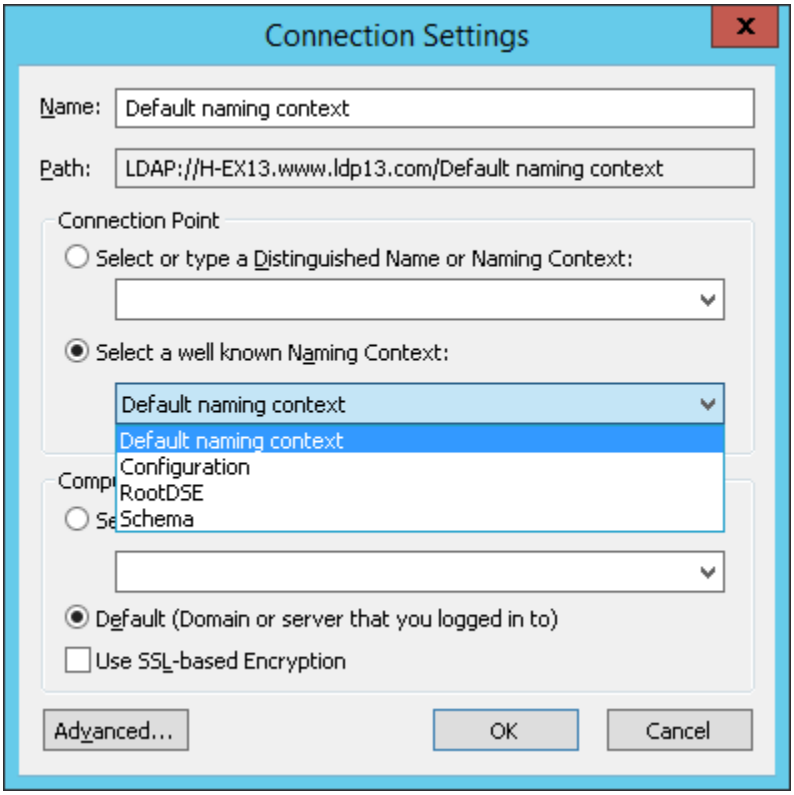
4.4. The "Default Naming context" node will be added in the console. Expand "Default naming context" node and right click on the domain name node as shown below:



4.5. From the properties window, add the newly created user with default access rights:



4.6. Repeat the steps mentioned above for another naming context. Please don't give any permissions to RootDSE, as the rights will not be accepted.



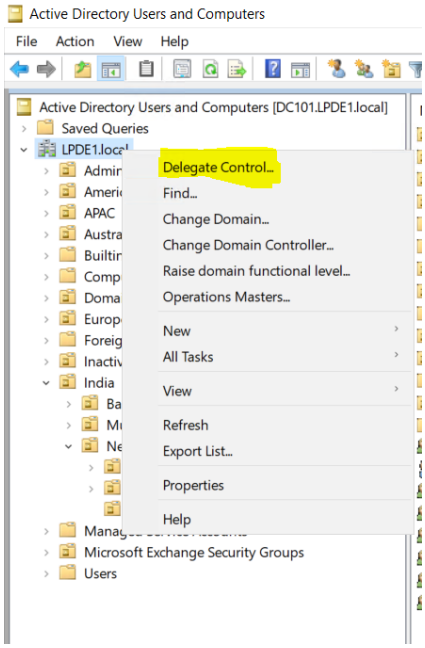
5. Add User under "Organization Management" Group for Getting Exchange Server changes.

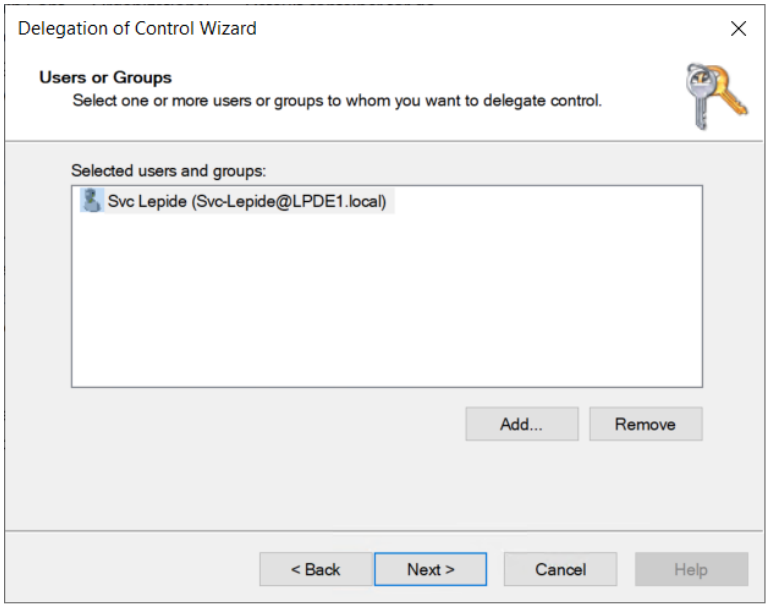
6. Give "Full Control" access rights to this account on the installation folder (C:\Program Files (x86)\LepideAuditor Suite).

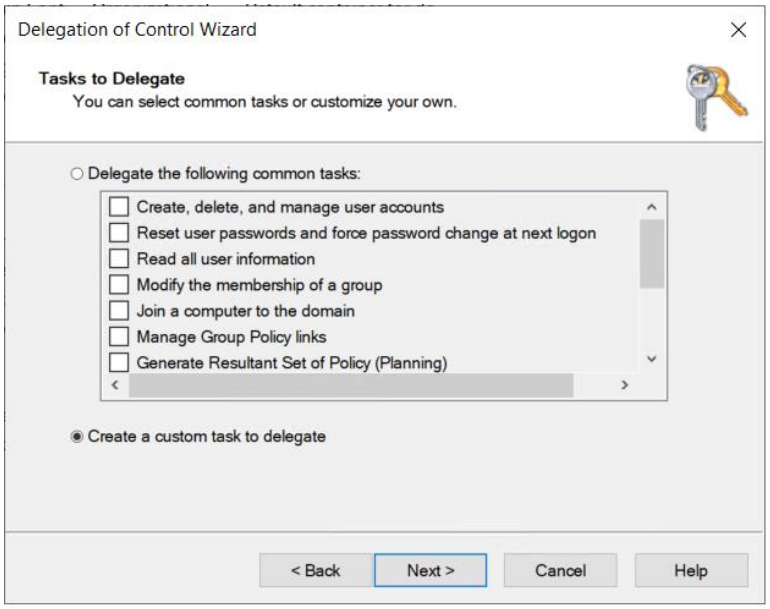
7. Configure the Lepide service with the newly created user.

8. In SQL, create a login by adding the newly created user and selecting "DB Creator" as the role.

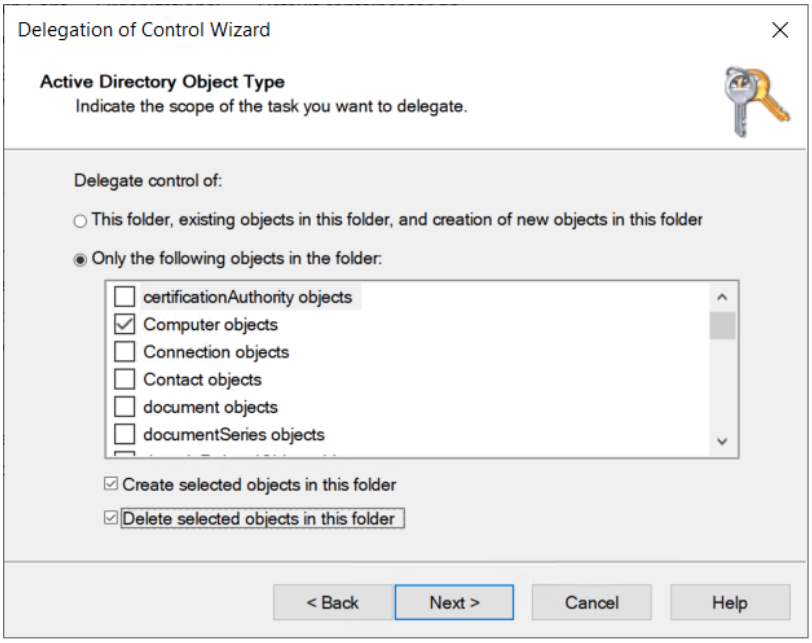
9. For Active Directory Cleaner, add the Delegation Control for this user account and choose the following options:

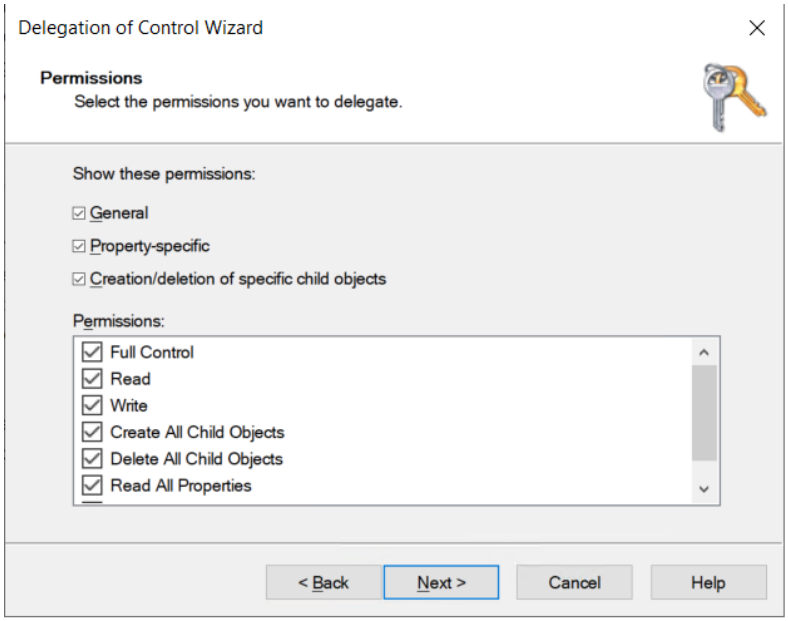

Active Directory Users and Computers
File Action View Help
Active Directory Users and Computers [DC101.LPDE1.local]
Saved Queries
Delegate Control...
Find...
Change Domain...
Change Domain Controller...
Raise domain functional level...
Operations Masters...
New
All Tasks
View
Refresh
Export List...
Properties
Help
Microsoft Exchange Security Groups
Users


Delegation of Control Wizard
Users or Groups
Select one or more users or groups to whom you want to delegate control.
Selected users and groups:
Svc Lepide (Svc-Lepide@LPDE1.local)
Add...
Remove
< Back
Next >
Cancel
Help



Select User Objects and Computer Objects from the list.





Disclaimer: A new account has to be created for using AD Cleaner and then the lepide server should be logged on with the same account.

3. Least Privilege Model for File Server Auditing (Windows File Server and Netapp Filer)

FOR WINDOWS FILE SERVERS

3.1 What's Available?

a. All File Server Modification reports i.e. States and Changes.

b. Permission Analysis.

c. Alerting and Scheduling.

d. Full reporting under Web Console.

3.2 What's Not Available?

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

3.3 Minimum Rights Required

a. A Domain User Account.

b. This account should have Db_owner/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.

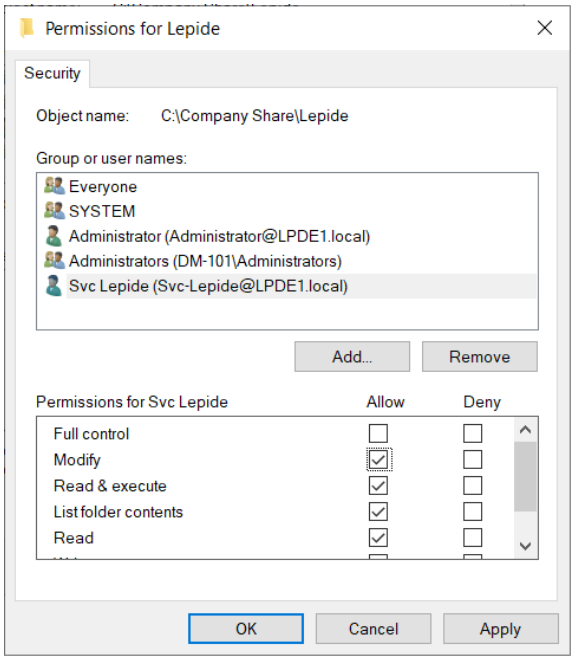
f. This account should be used to Logon to the Lepide Server to Configure the File Server for Auditing.

g. The SYSTEM account should have "Modify" rights on the folder where the agent is installed.

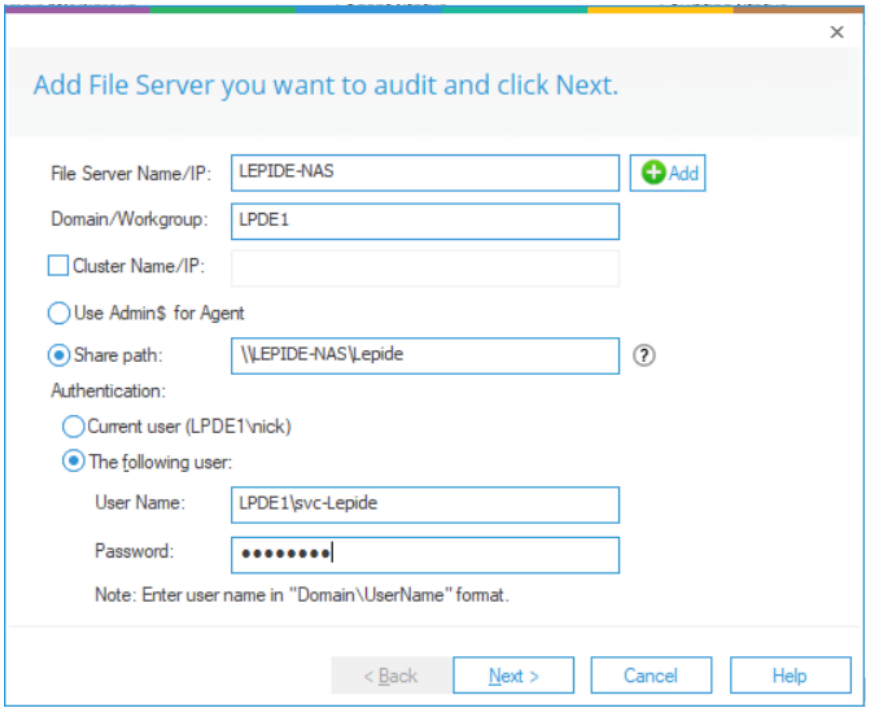
3.4 Adding the Windows File Server with Least Privileges

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

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



b. 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.



c. The next steps are similar to the Full Privilege Model installation.

d. Permission Analysis can be also be done in the same way once the rights are adjusted according to Section 3.3

FOR NETAPP CLUSTER MODE

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

3.5 Minimum Rights Required

a. A Domain User Account.

b. This account should have Db_owner/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.

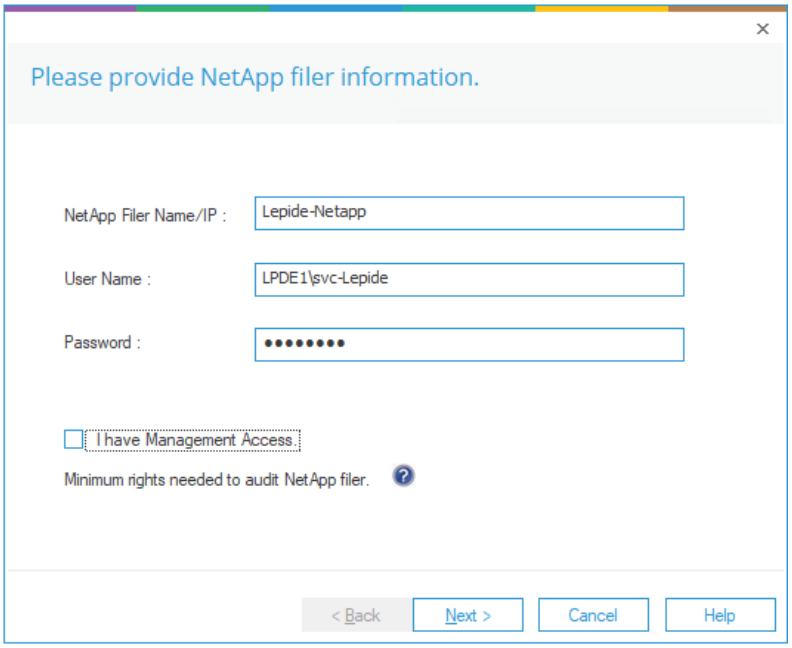
f. This account should be used to Logon to the Lepide Server to Configure the File Server for Auditing.

3.6 Adding the NetApp Cluster Mode with Least Privileges

In order to add the Netapp Filer Cluster Mode for auditing, the native auditing should be enabled manually, and it should meet the following pre-requisites:

- The minimum Log File Size (rotate-size) should be 1 MB.
- The format of auditing should be XML.
- The size of selected audit log volume should be at least 2 GB.
- The rotate limit should be applied to the auditing configuration.

a. On the first page, provide the IP address and the domain user account. Please ensure to Uncheck the "I have Management Access" option.



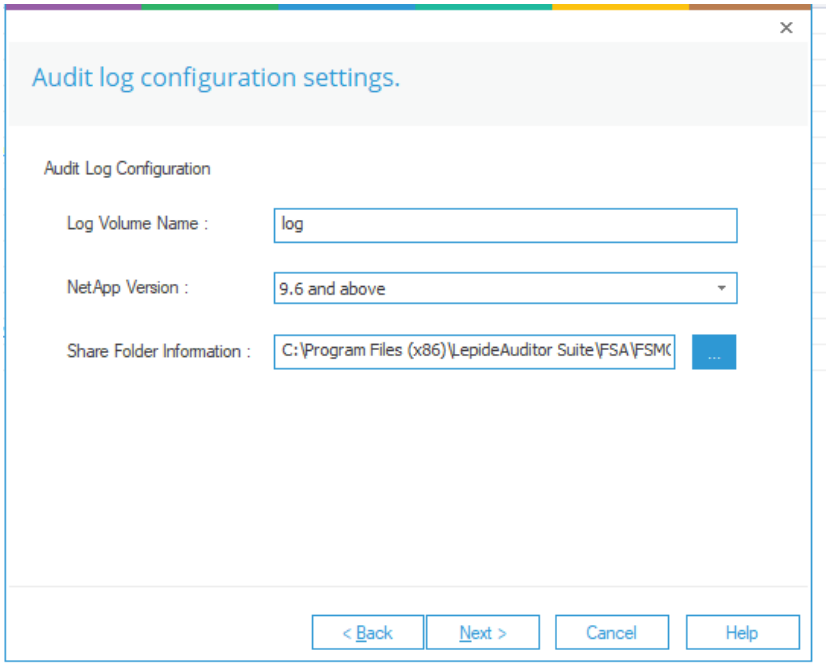
b. In the Least Privilege Model, the "ShareInfo.txt" file is not created itself by the solution. The users will have to create this file manually in a txt format and should have the entries like this for every Share:

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

c. 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.



d. 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. Least Privilege Model for Office 365 Auditing

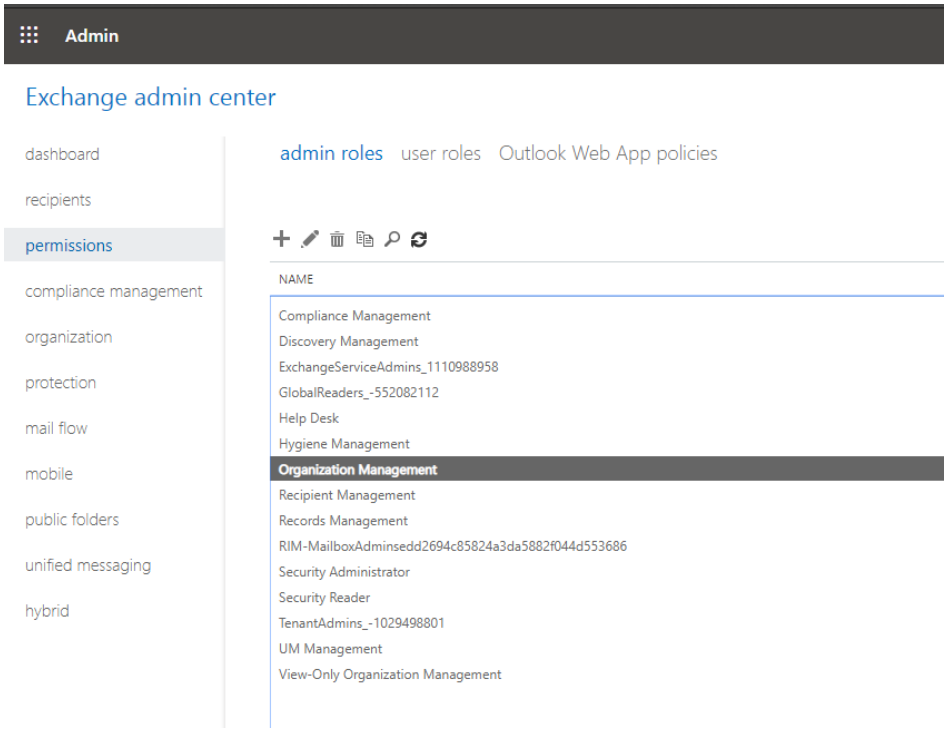
Auditing under Lepide DSP covers the following five components of O365:

- Exchange Online
- SharePoint Online
- Azure Active Directory
- OneDrive
- Skype for Business

All the reports and functionalities are available for O365 auditing with the Least Privilege Model as they are available with the Full Privilege one.

4.1 Minimum Rights Required

a. A normal O365 user account which is a member of the "Organization Management" Group in the Exchange Admin Center.



The procedure to add the component is the same as in the Full Privilege Model and the document can be found here:

https://www.lepide.com/configurationguide/configuration-guide-auditing-cloud-components.pdf

5. Support

If you face 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 http://www.lepide.com/contactus.html 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 http://www.lepide.com/data-security-platform/.

6. Trademarks

Lepide Data Security Platform, LepideAuditor, LepideAuditor App, LepideAuditor App Server, LepideAuditor (Web Console), LepideAuditor Logon/Logoff Audit Module, LepideAuditor for Active Directory, LepideAuditor for Group Policy Object, LepideAuditor for Exchange Server, LepideAuditor for SQL Server, LepideAuditor 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.