%Lepide

CONFIGURATION GUIDE

THE PRINCIPLE OF LEAST PRIVILEGE

Table of Contents

1.	Introdu	uction	3
2.	Least P	Privilege Model for Active Directory, Group Policy and Exchange On-Premises	3
	2.1.	What's Available with the Least Privilege Model?	3
	2.2.	What's Not Available with the Least Privilege Model?	3
	2.3.	Minimum Rights Required	4
	2.4.	Setting up the Account Privileges	4
3.	Least P	rivilege Model for File Server Auditing (Windows File Server and NetApp Filer)	19
	3.1.	For Windows File Servers	19
		3.1.1. What's Available?	19
		3.1.2. What's Not Available?	19
		3.1.3. Minimum Rights Required	19
		3.1.4. Adding the Windows File Server with Least Privileges	20
	3.2.	For NetApp Cluster Mode	21
		3.2.1. Minimum Rights Required	21
		3.2.2. Adding the NetApp Cluster Mode with Least Privileges	22
4.	Least P	vivilege Model for Office 365 Auditing	23
	4.1.	Minimum Rights Required	24
5.	OneDr	ive, Azure AD, MS Team Auditing, Exchange Online and SharePoint Online	25
	5.1.	Prerequisites	25
	5.2.	Steps to Register an App and Generate the Client ID and Secret Key for the Solution	25
6.	Exchar	ge Online Non-Owner Mailbox Access Auditing	26
7.	Suppor	rt	27
8.	Traden	narks	27

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 with the Least Privilege Model?

- 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 with the Least Privilege Model?

- 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.
- h. Successful Logon 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 Active Directory and add it under the **Event Log Readers** group.

Svc Lepide	Properties	;			?	\times
Remote	control	Remote	Remote Desktop Services Profile			M+
General	Address	Account	Account Profile Telephones		Organiz	ation
Membe	r Of	Dial-in	Env	ironment	Sessio	ns
Member o	f:					
Name		Active Directo	ory Domain	Services Folder	r	
Domain	Users	LPDE1.local	/Users			
Event Lo	og Readers	LPDE1.local	/Builtin			
Add		Remove				

Figure 1: Add User Account in Active Directory

- 2. Add this user account under the **Local Admin Group** on the Lepide Server. To do this, follow the steps below:
 - i. In the **Run** window, type **mmc** and press **Enter**.

The following screen will be displayed:



Figure 2: Microsoft Management Console

ii. From the File Menu, choose Add/Remove Snap-IN.



Figure 3: File Menu

The following dialog box is displayed:

	vendor	^		Console Root	Edit Extensions
Failover Cluster Man	Microsoft Cor				
Folder	Microsoft Cor				Remove
Group Policy Manag	Microsoft Cor				
Group Policy Manag	Microsoft Cor				Movello
Group Policy Object	Microsoft Cor				Hove op
Group Policy Starter	Microsoft Cor				Move <u>D</u> own
Internet Informatio	Microsoft Cor	≡	<u>A</u> dd >		
Internet Informatio	Microsoft Cor				
IP Security Monitor	Microsoft Cor	-			
IP Security Policy M	Microsoft Cor				
Link to Web Address	Microsoft Cor				
Local Backup	Microsoft Cor				
Local Users and Gro	Microsoft Cor				
NAP Client Configur	Microsoft Cor	~			Advanced

Figure 4: Add or Remove Snap-ins

- i. Choose Local Users and Groups
- ii. Click Add

The following dialog box is displayed:

Choose Target Machine		x
Select the computer you want this snap-in to manage. This snap-in will always manage: Local computer: [the computer on which this console is running]		
◯ <u>A</u> nother computer:	Browse	
Allow the selected computer to be changed when launching from the comm only applies if you save the console.	and line. This	
< <u>B</u> ack Finish	Cance	el

Figure 5: Choose Target Machine

- iii. Select Local computer
- iv. Click **Finish**

- v. Click **OK**
- 1. When the **Choose Target Machine** wizard is closed, the **Local Users and Group** node is added to the console:

a	Cor	sole1 - [Console Root\Local U	Isers and Groups (Local)\Groups]		_ D X
🚡 Eile Action View Favorites Wind	ow <u>H</u> elp				_ 8 ×
♦ ≥ = × = ≥					
Console Root	Name	Description		Actions	
🔺 💭 Local Users and Groups (Local)	Access Control Assist	Members of this group can remot			
Users	Administrators	Administrators have complete an		Groups	-
🧰 Groups	A Backup Operators	Backup Operators can override se		More Actions	•
	Ecertificate Service DC	Members of this group are allowe		Administrators	
	Register Strate	Members are authorized to perfor		Mandations	
	A Distributed COM Users	Members are allowed to launch, a		Wore Actions	,
	Event Log Readers	Members of this group can read e			
	A Guests	Guests have the same access as m			
	Administrators	Members of this group have com			
	A IIS_IUSRS	Built-in group used by Internet Inf			
	🜆 Network Configuratio	Members in this group can have s			
	A Performance Log Users	Members of this group may sche			
	🜆 Performance Monitor	Members of this group can acces			
	🜆 Power Users	Power Users are included for back			
	🜆 Print Operators	Members can administer printers			
	ADS Endpoint Servers	Servers in this group run virtual m			
	🌆 RDS Management Ser	Servers in this group can perform			
	ADS Remote Access S	Servers in this group enable users			
	🕭 Remote Desktop Users	Members in this group are grante			
	🌆 Remote Management	Members of this group can acces			
	A Replicator	Supports file replication in a dom			
	🕭 Users	Users are prevented from making			
	A WinRMRemoteWMIU	Members of this group can acces			
				1	

Figure 6: Microsoft Management Console

- 2. Select **Administrator** from the middle pane and double click.
- 3. The Administrators Properties dialog box is displayed:



Administrators Pro	perties			?	×			
General								
Administrators								
Description: Administrators have complete and unrestricted access to the computer/domain								
the computer/domain Members: Administrator LPDE1\Domain Admins LPDE1\Svc-Lepide (Svc-Lepide@LPDE1.local)								
Add Remove Changes to a user's group membership are not effective until the next time the user logs on.								
	ОК	Cancel	Apply	He	lp			

Figure 7: Administrators Properties

- 4. From the Administrators Properties window, add the newly created user with default access rights.
- 5. Log in to the Lepide Server using the newly created user credentials.
- 6. Open **ADSIEdit** and provide access rights to the newly created user using the different naming context of Active Directory.
- 7. To do this, follow these steps:
 - i. From the **Run** window, type **ADSIEDIT**.**msc** and press **Enter**:
 - ii. Right click on the ADSI Edit node and Select **Connect to....**



		ADSI Edit
File Actio	on View Help	
	T 🖸 🛛 🎫	
📝 ADSI Ed	it	
	Connect to	Welcome to ADSI Ec
	View 🕨	
	Refresh	Active Directory Services Interf Editor (ADSI Edit) is a low-level
	Help	editor for Active Directory Don
		Lightweight Directory Services



iii. From the Connection Settings dialog box, select **Default naming context** and click **OK**

Connection Settings						
Name: Default naming context						
Path: LDAP://H-EX13.www.ldp13.com/Default naming context						
Connection Point						
Select or type a <u>D</u> istinguished Name or Naming Context:						
✓						
Select a well known Naming Context:						
Default naming context						
Computer						
O Select or type a domain or server: (Server Domain [:port])						
v						
Default (Domain or server that you logged in to)						
Use SSL-based Encryption						
Ad <u>v</u> anced OK Cancel						

Figure 9: Connection Settings

- iv. The **Default Naming context** node will be added to the console.
- v. Expand **Default naming context** node and right click on the domain name node as shown below:

2							
File Action View Help							
🗢 🔿 🙍 🏋 🗐 🖬 🖬 🖬							
📝 ADSI Edit							
Default naming context [H-EX13.v	vww.ldp13.com]						
DC=www,DC=Idp13,DC=com							
	New 🕨						
	View 🕨						
	Rename						
	Refresh						
	Export List						
	Properties						
	Help						



vi. From the Properties window, add the newly created user with default access rights:



C=LPDE1,DC=	local Propert	ties		?	×	
Attribute Editor	Security					
Group or user	names:					
Administrators (LPDE1\Administrators) Administrators (LPDE1\Pre-Windows 2000 Compatible Access (LPDE1\Pre-Windows 20 Incoming Forest Trust Builders (LPDE1\Incoming Forest Trust Bu ENTERPRISE DOMAIN CONTROLLERS System 1 (System 1 (System 2 (System						
					~	
			Add	Remove	,	
Permissions fo	r Svc Lepide		Allow	Deny		
Full control			Ξ,		^	
Read						
Write						
Create all ch	nild objects					
Delete all ch	nild objects				~	
For special permissions or advanced settings, click Advanced Advanced.						

Figure 11: Properties

Repeat the steps above to add another naming context. vii.

Please do not give any permissions to **RootDSE**, as the rights will not be accepted.



Connection Settings ×
Name: Default naming context
Path: LDAP://H-EX13.www.ldp13.com/Default naming context
Connection Point
○ Select or type a <u>D</u> istinguished Name or Naming Context:
✓
Select a well known Naming Context:
Default naming context 🗸 🗸
Default naming context
Complexition
⊖ S∉Schema
v
Default (Domain or server that you logged in to)
Use SSL-based Encryption
Ad <u>v</u> anced OK Cancel

Figure 12: Connection Settings

1. From the Properties dialog box, select **Organization Management**:



DC=LPDE1,DC=local	Properties	? X				
Attribute Editor Security						
<u>G</u> roup or user names:						
& NETWORK SERVICE		~				
Signalization Management (LPDE1\Organ	nization Manage	ement)				
Relegated Setup (LPDE1\Delegated Setup	(qu					
Exchange Servers (LPDE1\Exchange Servers)	rvers)					
Exchange Trusted Subsystem (LPDE1\E	«change Truste	d Subs				
Exchange Windows Permissions (LPDE1)	Exchange Win	idows 🖄				
	A <u>d</u> d	<u>R</u> emove				
Permissions for Organization		_				
Management	Allow	Deny				
Full control						
Read	✓					
Write						
Create all child objects						
Delete all child objects						
For special permissions or advanced settings, click Advanced						
OK Cancel	<u>A</u> pply	Help				

Figure 13: Properties

- 2. Give **Full Control** access rights to this account on the installation folder (C:\Program Files (x86)\LepideAuditor Suite).
- 3. Configure the Lepide service with the newly created user.
- 4. In SQL, create a login by adding the newly created user and selecting **DB Creator** as the role.
- 5. For Active Directory Cleaner, select Delegation Control for this user account:

3	
File Action View Help	
🗢 🔿 🛅 🖬 🗐 🖾 🕞 🚺 📆 🗏	i ү 🗾 🐍
Active Directory Users and Computers [DCD01.LPDE1.local Saved Queries PDE1.local P C PDE1.local P C PDE1.l	al) Name Builtin Computers ForeignSecurity Managed Servic Users Austin Computer Pool Computer Pool Compool E Delhi Delhi Delhi Delhi Delhi E Lepide 2020 Microsoft Excha NYC E test User Pool

Figure 15: Delegate Control

The Delegation of Control Wizard will start:



Figure 14: Delegation of Control Wizard

6. Click Next

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:
Add Remove
< Back Next > Cancel Help

Figure 16: Add User

7. Click **Add** to add a user

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

Figure 17: Added User

Delegation of Control Wizard X
Tasks to Delegate You can select common tasks or customize your own.
Delegate the following common tasks: Create, delete, and manage user accounts Reset user passwords and force password change at next logon Read all user information Modify the membership of a group Join a computer to the domain Manage Group Policy links Generate Resultant Set of Policy (Planning) III
< Back Next > Cancel Help

Figure 18: Tasks to Delegate

- 8. Select Create a custom task to delegate
- 9. Select User Objects and Computer Objects from the list

Delegation of Control Wizard X
Active Directory Object Type Indicate the scope of the task you want to delegate.
Delegate control of:
\bigcirc This folder, existing objects in this folder, and creation of new objects in this folder
Only the following objects in the folder:
 transportStack objects Trusted Domain objects ✓ User objects x25Stack objects x25X400Link objects x400Link objects ✓
< Back Next > Cancel Help
Figure 19: Active Directory Object Type

10. Click Next

Delegation of Control Wizard	x
Permissions Select the permissions you want to delegate.	R
Show these permissions: ✔ General ✔ Property-specific ✔ Creation/deletion of specific child objects Permissions:	
 Full Control Read Write Create All Child Objects Delete All Child Objects Read All Properties 	<
< Back Next > Cancel	Help

Figure 20: Permissions

11. Select the **Permissions** to delegate

12. Click Next

The last step of the Wizard will appear with a summary of delegation of control you have set up:



D	elegation of Control Wizard
	Completing the Delegation of Control Wizard You have successfully completed the Delegation of Control wizard. You chose to delegate control of objects in the following Active Directory folder: LPDE1.local/ The groups, users, or computers to which you have given control are: Sam (Sam@LPDE1.local) They have the following permissions: Vouces this wizard, click Enrish
	< Back Finish Cancel Help

Figure 21: Summary of Delegation of Control

13. Click Finish

NOTE: A new account must 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)

3.1. For Windows File Servers

3.1.1. 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.

3.1.2. 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.

3.1.3. 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.



3.1.4. Adding the Windows File Server with Least Privileges

Follow the below steps 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.

Permissions for Lepide		×
Security		
Object name: C:\Company Shar	e\Lepide	
Group or user names:		
Sector Everyone		
SYSTEM		
Administrator (Administrator@L	strators)	
Svc Lepide (Svc-Lepide@LPD)	E1.local)	
	Add	Remove
Permissions for Svc Lepide	Allow	Deny
Full control		□ ^
Modify	\checkmark	
Read & execute	\checkmark	
List folder contents	\checkmark	
Read	\checkmark	
ОК	Cancel	Apply

Figure 22: 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.



File Server Name/IP:	LEPIDE-NAS	Add
Domain/Workgroup:	LPDE1	
Cluster Name/IP:		
Use Admin\$ for Ag	ent	
• Share path:	\\LEPIDE-NAS\Lepide	(?)
Authentication:	1	
OCurrent user (LPD	E1\nick)	
• The <u>following</u> use	r:	
User Name:	LPDE1\svc-Lepide	
Password:	******	

Figure 23: Add File Server

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

3.2. For NetApp Cluster Mode

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

3.2.1. 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.

3.2.2. Adding the NetApp Cluster Mode with Least Privileges

To add the NetApp Filer 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.

		×
Please provide Net/	App filer information.	
NetApp Filer Name/IP :	Lepide-Netapp]
		7
User Name :	LPDE1(svc-Lepide	
Password :	•••••	
I have Management /	Access.	
Minimum rights needed to	audit NetApp filer. 🛛 🛛	
	< <u>B</u> ack <u>N</u> ext > Cancel	Help

Figure 24: 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.

Audit log configuratio	on settings.	×
Audit Log Configuration		
Log Volume Name :	log	
NetApp Version :	9.6 and above ×	
Share Folder Information :	C:\Program Files (x86)\LepideAuditor Suite\FSA\FSM(
	< <u>B</u> ack <u>N</u> ext > Cancel He	lp

Figure 25: 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. Least Privilege Model for Microsoft 365 Auditing

Auditing under Lepide DSP covers the following five components of M365:

- Exchange Online
- SharePoint Online
- Azure Active Directory



- OneDrive
- Skype for Business

All the reports and functionalities are available for M365 auditing with the Least Privilege Model as they are available with the Full Privilege one.

4.1. Minimum Rights Required

a. A normal M365 user account which is a member of the **Organization Management** Group in the Exchange Admin Center.

III Admin	
Exchange admin cer	nter
dashboard	admin roles user roles Outlook Web App policies
recipients	
permissions	+ 🖍 面 陥 P 😂
compliance management	NAME
organization	Compliance Management Discovery Management
protection	ExchangeServiceAdmins_1110988958 GlobalReaders552082112
mail flow	Help Desk Hygiene Management
mobile	Organization Management
public folders	Recipient Management Records Management
unified messaging	RIM-MailboxAdminsedd2694c85824a3da5882f044d553686 Security Administrator
hybrid	Security Reader TenantAdmins_1029498801 UM Management View-Only Organization Management

Figure 26: Admin Exchange 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. OneDrive, Azure AD, MS Team Auditing, Exchange Online and SharePoint Online

5.1. Prerequisites

To add OneDrive, Azure AD, MS Teams, Exchange Online and SharePoint Online to the Lepide Data Security Platform for Auditing, an app has to be registered on the Microsoft 365 portal.

NOTE: This app can be created by using an existing Global Administrator account. The app is not going to use the Global Administrator permissions of this account it is only required for the creation of the app.

5.2. Steps to Register an App and Generate the Client ID and Secret Key for the Solution

- 1. Log onto the Microsoft 365 Admin Center
- 2. Select Azure Active Directory from the Admin Center
- 3. Click on **App Registration** and follow the steps below to generate Client ID and Secret Key:
 - Select **New Registration** and provide a valid name for the registration (Global Administrator)
 - Click on **Register Account** and the Client ID will be displayed which the user can copy for future use
 - For the given Client Id generated in the Azure Account Dashboard, click on Certificates and Secrets
 - Click on Add New Client Secret (with expiry period) and a Secret ID will be generated which the user can copy for future use

NOTE: Copy Client ID and Secret Key for adding Microsoft 365 components

- 4. Click on the API permission tab for the given Client ID and select Request API Permissions
- 5. Select API my organization uses as follows:

Microsoft 365 Management APIs and select permission type(s) as detailed below:

>ActivityFeed.Read

Delegated

>ActivityFeed.Read Application

Lej

>ActivityFeed.ReadDlp

Delegated

>ActivityFeed.ReadDlp Application

6. Grant Admin consent for registered Domain after API Permissions selection

NOTE: Every permission change required must be granted admin consent for a given Domain

- 7. Go to the Azure Active Directory Dashboard and select **Tab Roles and Administrators**
- Under Roles and Administrator select Global Reader
 Double click to Add Assignments
 In Add Assignments go to Select Member(s) and select newly created members
- 9. Assignment type will be eligible. Unlock permanently eligible and selection assignment duration and click **Assign**
- 10. Now add the components with Client ID and Secret Key

6.Exchange Online Non-Owner Mailbox Access Auditing

To enable the exchange online non-owner mailbox access auditing in the Lepide Data Security Platform, the app which is registered must be assigned **Exchange Administrator** role rather than Global Reader in step 8 above.



7.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 <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>.

8.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.

