# Amazon S3.

Quick Start Guide.

**\!!** Lepide

# Contents

1		Intro	oduct	tion	2
2		Prer	equi	sites	2
3		Acce	ess Ke	eys	2
	3.1	Lł	low	to Manage Access Keys for your AWS Account	2
		3.1.	1	To create, disable, or delete an access key for your AWS account root user	2
	3.2	2 4	Addir	ng an Amazon S3 Component	4
4		Viev	ving	the Reports	7
	4.1	1 4	All En	vironment Changes Report	7
	4.2	2 1	The C	Open AWS S3 Buckets Report	1
		4.2.3	1	Adding a Data Set and Running a Scan1	1
		4.2.2	2	Running the Open AWS S3 Buckets Report1	4
5		Supp	port.		16
6		Trad	lema	rks1	16

# 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 the Amazon S3 component. For information on installation, please see our <u>Installation and Prerequisites</u> <u>Guide</u>.

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 Prerequisites

The following are prerequisites to add an Amazon S3 component to the Lepide Data Security Platform:

• An S3 bucket needs to be created and the steps to do this can be found here:

https://docs.aws.amazon.com/AmazonS3/latest/userguide/creating-bucket.html

# 3 Access Keys

Access keys are long-term credentials for an AWS Identity and Access Management (IAM) user or the AWS account root user. Access keys consist of two parts: an access key ID (for example, AKIAIOSFODNN7EXAMPLE) and a secret access key (for example, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY). You must use both the access key ID and secret access key together to authenticate your requests.

## 3.1 How to Manage Access Keys for your AWS Account

Follow these steps to manage access keys for your AWS account. For information about managing access keys for IAM users, see <u>Managing Access Keys for IAM Users</u> in the IAM User Guide.

## 3.1.1 To create, disable, or delete an access key for your AWS account root user

Use your AWS account email address and password to sign in to the <u>AWS Management Console</u> as the AWS account root user.



- **NOTE:** If you previously signed in to the console with <u>IAM user</u> credentials, your browser might remember this preference and open your account-specific sign-in page. You cannot use the IAM user sign-in page to sign in with your AWS account root user credentials. If you see the IAM user sign-in page, choose **Sign-in using root user credentials** near the bottom of the page to return to the main sign-in page. From there, you can type your AWS account email address and password.
- 1. On the **IAM Dashboard** page, choose your account name in the navigation bar, and then choose **My Security Credentials**.
- If you see a warning about accessing the security credentials for your AWS account, choose Continue to Security Credentials.
- 3. Expand the Access keys (access key ID and secret access key) section.
- 4. Choose your preferred action:

#### To create an access key:

• Choose **Create New Access Key**. Then choose **Download Key File** to save the access key ID and secret access key to a file on your computer. After you close the dialog box, you can't retrieve this secret access key again.

#### To disable an existing access key

• Choose Make Inactive next to the access key that you are disabling. To reenable an inactive access key, choose Make Active.

#### To delete an existing access key

Before you delete an access key, make sure it's no longer in use. For more information, see
 <u>Finding unused access keys</u> in the IAM User Guide. You can't recover an access key after
 deleting it. To delete your access key, choose **Delete** next to the access key that you want to
 delete.



## 3.2 Adding an Amazon S3 Component

An Amazon S3 Component is added from the Web Console Manage Component screen and the steps to do this are as follows:

• From the Web Console Home screen, click the Settings icon (top right of the screen) to display the Admin Console

🕷 Lepide				© (0)
Welcome to the Lepide Data Get visibility over your m Click on one of the below	Security Platform st sensitive data. implement zero trust and detect/react to threats. tiles to get started.			
	Lepide Auditor Track user interactions to sensitive data and key infrastructure.	Lepide Trust Identify permission changes and users with privileged access.	000	My Lepide Jump right into your fevourite reports and destributeds.
¢	Lepide Detect Detect and respond to threass with anomaly detection and alerts.	Lepide identify Discover and classify sensitive data based on risk and value.		Global Dashboard Overview of data security capabilities for key infrastructure.

#### Figure 1: Home Screen

• From here select **Manage Components** from the options on the left-hand side of the screen and the Manage Components screen will be displayed:

🕷 Lepide	🏠 Home 🎧 Lepide Austitor 😗 Lepide Trust 🦉 Wy Lepide Detect. 🔯 Lepide Identity 🌐 Global Dushboard 🔞 🔇
Manage Components	
Categories	Components
<ul> <li>Role Management</li> <li>2 → Log5</li> </ul>	Microsoft365 SharePoint Online Exchange Online AWS S3
General Settings	G GSuite
Exported Files	
Application URL	
Manage Domains	
Subscription	
Configure Notifications	K Added Components
Components	Microsoft365     SharePoint Online       LepideSoftwa.     Iepidesoftwa.

#### Figure 2: Manage Components

• From the **Components** section, click on the **AWS S3** component and the Add Credential for AWS S3 window is displayed with the Component Credential category selected:

Add Credential for AWS S3 Manage Components / AWS S3			
Categories Component Credential C Database settings	Server Name AWS Access Key AWS Secret Key	0	
			Back Next

Figure 3: Component Credential

- Add the Server Name
- The specified name will appear in the 'Server Name' column for the All Environment Changes Report
- Add the AWS Access Key (see section 3.1 of this guide for information on how to create an Access Key)
- Add the **AWS Secret Key (**see section 3.1 of this guide for information on how to create a Secret Access Key)
- Click Next to continue

The Database Settings window is displayed.



d Credential for AWS S3 age Components / AWS S3				
ategories	Server Name			
Component Credential		Authentication Type		
Database settings		<ul> <li>Windows Authentication</li> <li>SQL Authentication (recommended)</li> </ul>		
		User Name Sa		
		Password		
	Create database	Test Con	nection	
	Select database	134_0365	~	
				8

Figure 4: Database Settings

Add the Database Settings as follows:

- Server Name enter the name of the server
- Authentication Type choose from either:
  - Windows Authentication or
  - SQL Authentication add the User Name and Password
- Select to either Create **database** enter the database name and click **Test Connection** to test the database connection

Or

- Select database use the drop-down arrow to select the name of an existing database
- Click Finish

The added component will be displayed in the Manage Component window:



Manage Components <sub>Categories</sub>	Components							
Role Management	Microsoft365		SharePoint Online	E Exchan	ige Online	Dropbox	aws sa	
General settings     Backup & Restore     Exported Files	GSuite							
Manage Domains	Added Components	~~	×	aws	aws	E	G	
Configure Notifications    Manage Components	Dropbox 1DropBox	Dropbox asda	Dropbox newDropBox	AWS S3 AWISS3	AWS 53 AWS53	Exchange Online DevSoft001.o.,	GSuite G-Suit Serve	
	~	~		_				



# 4 Viewing the Reports

## 4.1 All Environment Changes Report

The All Environment Changes Report will show all changes made to the AWS S3 Component.

To run the report:

- From the Web Console Home screen, select Lepide Auditor and the Lepide Auditor dashboard screen will be displayed
- From the Lepide Auditor menu at the top, select Reports

The Lepide Auditor Reports screen will be displayed:



oorts						Search	Q	Create Repo
arch Q	Report Name	Description 个	Shared With	↑ Shared By	↑ My Lepi	ide ↑	Report Type	↑ Ad
All Reports	۹	٩		Q	Q			Q
I Environment Changes	All Environment Changes (ALL ENVIRO	Shows all the changes happening across all the components.			III III		Predefined	
Active Directory	All Object Changes (Active Directory)	Shows all the changes related to active directory objects.			111		Predefined	
Exchange Server	Failed Logons (Active Directory)	Shows all the failed logons and analyze potential brute force attack.			111		Predefined	
Exchange Server Online	All Successful Authentication (Active Dir	Shows All Successful Authentication.			111		Predefined	
Group Policy	Concurrent Logons (Active Directory)	Shows the users who are logged on to multiple systems at the same time.			III III		Predefined	
File Server	User Logged on to Multiple Computers	Shows the users who are logged on to multiple systems.			III III		Predefined	
SharePoint Online	Admin Group Changes (Active Directory)	Shows all Admin Group Changes			III III		Predefined	
SharePoint Server	Security Group Changes (Active Directo	Shows All Security Group Changes			III III		Predefined	
Azure AD	Liser Password Reset and Change Atte	Shows all the Liser Password Reset and Change Attemnts			W III		Predefined	
	Schema Changes (Arthe Directory)	Shour all the artius directory rehease changer			III		Predeficed	
+ Create Folder	Science changes prease birectory)	anorezon die active on accivity scheme charages.			m			
X Remove Folder	Total Report(s) - 294	First Previous	1 / 30 Next	Last		_		10 / Page



• From here, select the All Environment Changes Report:

port Name - A	II Envir	ronment Char	ges																								
ne / Lepide A	uditor	/ Reports /	All Erwi	ronment Chang	es															🗇 Ma	/ 14, 202	- May 14, 20		Gener	ate Report	Ð	
mponent me	1 s	Server Name	Ŷ	Object Path	Ŷ	Object Type	Ť,	Who	1	When	Ŷ	Operation	Ŷ	Content Type	Ŷ	Compliance	Ŷ	Risk Leve	1 Mon	tary Value	↑ w	at	Ŷ	Where	↑ c	riticality	
	Q		Q		Q		Q		Q		Q		Q		Q		Q		Q		Q		Q		Q		
										Please click	on the	"Generate Re	port" b	button to vie	w the	records for th	nis repo	ort.									
										Please click	on the	"Generate Rej	port" b	outton to vie	wthe	records for th	nis repo	ort.									

Figure 7: All Environment Changes Report

## To apply a filter for AWS S3:

Click the Filter icon:

• The Modify Filters dialog box is displayed



• Click the arrow to display the drop down menu:

Component Name	
Server Name	
Object Path	
Object Type	
Who	
Operation	_

Figure 8: Modify Filters drop down Menu

- Select Component Name from the list
- Click the components
- Click the arrow next to Filter Criteria and select Equals

ilter by Component Name	
itter by component Name	
Filter Criteria	
Equals	^
Equals	
Not Equals	
Active Directory	
Exchange Server	
Group Policy	
SQL Server	
CharaDoint Conver	
Cancel	y
	_

Figure 9: Filter Criteria

• From the list of components, select AWS S3:

Modify Filters	×
Filter by Component Name	
Filter Criteria	
Equals	~
Search	Q
Skype For Business	
Microsoft Teams	
🗍 Dropbox	
AWS S3	
GSuite	
Cancel	Apply
Cancel	Apply

Figure 10: Filter by Component Name

- Click Apply, Apply to close the Modify Filter box and go back to the report screen
- Change the time period if required
- Click Generate Report

The example below shows the All Environment Changes Report with the AWS S3 filter applied:

ne / Lepide A	uditor / Reports /	All Environment Ch	anges							🕼 🏆 🕩	🛗 May 1, 2025 - M	ay 31, 2025 👻	Cancel Repo
omponent ame	Server 1 Name	Object Path 1	Object Type 🕇	Who 1	When 1	Operation 1	Content Type	Compliance 1	Risk Level 1	Monetary 个 Value	What 1	Where	Criticality
G	Q Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q	
/5 53	Awss3 fgf	lepidesupport	Bucket	07f088ecc27d8	31-05-2025 05:1	REST.GET.OBJECT	N/A	N/A	N/A	N/A	{ "bucketName"	119.82.89.131	Low
/S S3	Awss3 fgf	lepidesupport	Bucket	07f088ecc27d8	31-05-2025 05:1	REST.GET.OBJECT	N/A	N/A	N/A	N/A	{ "bucketName"	119.82.89.131	Low
/S S3	Awss3 fgf	lepidesupport	Bucket	07f088ecc27d8	31-05-2025 05:1	REST.GET.OBJECT	N/A	N/A	N/A	N/A	{"bucketName"	119.82.89.131	Low
'S S3	Awss3 fgf	lepidesupport	Bucket	07f088ecc27d8	31-05-2025 05:1	REST.GET.OBJECT	N/A	N/A	N/A	N/A	{ "bucketName"	119.82.89.131	Low
S 53	Awss3 fgf	lepidesupport	Bucket	07f088ecc27d8	31-05-2025 05:1	REST.GET.OBJECT	N/A	N/A	N/A	N/A	{ "bucketName"	119.82.89.131	Low
/5 53	Awss3 fgf	lepidesupport	Bucket	07f088ecc27d8	31-05-2025 05:1	REST.GET.OBJECT	N/A	N/A	N/A	N/A	{ "bucketName"	119.82.89.131	Low
/5 53	Awss3 fgf	lepidesupport	Bucket	07f088ecc27d8	31-05-2025 05:1	REST.GET.OBJECT	N/A	N/A	N/A	N/A	{ "bucketName"	119.82.89.131	Low
/5 53	Awss3 fgf	lepidesupport	Bucket	07f088ecc27d8	31-05-2025 05:1	REST.GET.BUCKET	N/A	N/A	N/A	N/A	{ "bucketName"	119.82.89.131	Low
/S S3	Awss3 fgf	lepidesupport	Bucket	svc:s3.amazona	31-05-2025 05:1	REST.PUT.OBJECT	N/A	N/A	N/A	N/A	{ "bucketName"		Low
/S S3	Awss3 fgf	lepidesupport	Bucket	svc:s3.amazona	31-05-2025 05:1	REST.PUT.OBJECT	N/A	N/A	N/A	N/A	{ "bucketName"		Low
/S S3	Awss3 fgf	lepidesupport	Bucket	svc:s3.amazona	31-05-2025 05:1	REST.PUT.OBJECT	N/A	N/A	N/A	N/A	{ "bucketName"		Low
'S S3	Awss3 fgf	lepidesupport	Bucket	svc:s3.amazona	31-05-2025 05:1	REST.PUT.OBJECT	N/A	N/A	N/A	N/A	{ "bucketName"	-	Low
5 53	Awss3 fgf	lepidesupport	Bucket	svc:s3.amazona	31-05-2025 05:1	REST.PUT.OBJECT	N/A	N/A	N/A	N/A	{ "bucketName"	-	Low
	Awee3 fof	lepidesupport	Bucket	svr:s3 amazona	31-05-2025 05:0	REST PLITORIECT	N/A	N/A	N/A	N/A	{ "bucketName"		Low

Figure 11: All Environment Changes Report

#### 4.2 The Open AWS S3 Buckets Report

An open AWS S3 bucket is called "open" because anyone can access the data in the bucket without authentication. This can be a major security risk, as anyone can view, download, or even delete the data in the bucket. So, because an open S3 bucket is a potential source of a data breach, it is important to have visibility over all open S3 buckets. This can be achieved by running the Open AWS S3 Buckets Report, part of the Lepide Data Security Platform.

#### 4.2.1 Adding a Data Set and Running a Scan

Before the Open AWS S3 Buckets Report can be run, you will need to create a data set and run a Current Permissions Scan to have visibility over the current state of open buckets. This is done from the Lepide Main Console, and the steps are as follows:

#### To Add a Data Set:

From the icons on the left-hand side of the screen, click the **Settings** icon and the Settings screen will be displayed:

Constraint Margarent     Constraint Array     Constraint     Constraint     Constraint     Constraint     Con	10
Image: Second	10
Constraint and a constraint of the first stress     Constraint of the first stres	10
• In placetanese set similares • In placetanese set set set set set set set set set	18
a) <ul> <li>             a)             for a former         </li> <li>             c)             for a former         </li> <li>             c)             construction         </li> </ul> c)             construction               And points               Superfact Sorrer               Solution               Former               Extendem               Solution	90
Image: Constraint of the constraint	ne
<sup>3</sup> <sup>3</sup> <sup>4</sup> <sup>4</sup> <sup>5</sup> <sup>4</sup>	
Control Fermiosion Stating     Control Control and Active	
Marga Delay Strains     M	
A dia Usa Val Server Stating     A dia Usa Val Server Stating     A dia Usa Val Server Val Server A dia Usa Val Val Server A dia Usa Val Val Val Val Val Val Val Val Val Va	
30         27 Append Setting:           30         102 Mode Cancello	
- A straining of the st	
Archive & Import	
Added Component	
Added Component	
	1
	1
	1
lade Local DillulisLi 🔤 Lilulitie Serveri 🔤 Lilulitie Serveri	admin.shar
Adve Dector, Grup SOL Server E 23	1
Policy and Exchange Server	1e
	1
	1
	1
	1
	1
	1
	I
	I
	I
	I

Figure 12: Settings Screen

- Select Current Permissions Scan Settings from the tree on the left-hand side of the screen
- Click the 🖸 icon

The Data Set Information dialog box will be displayed:



## Lepide Data Security Platform

Settings										
Component Management	Current Permission	Scan Settings								
Isportputtd-admin.sharepoi     Isportputtd-admin.sharepoi     Isportputtd-admin.sharepoi     Isportputtd-admin.sharepoi     CODA_NEW     UpSoftPuttd.onmicrosoft.co     General Settings	Primary Database Configure primary database	to store common information	/ 5	Secondary Database secondary database will s	:[S] tore NTFS and Share permission for files and	olders selected in the datasets			c	<b>) / X</b> #
	SQL Server : D8251	N Server: DB251		A File Server(s)	Sql server name		Database			-
	Debases CE Discontinue and and			<u>م</u>	P		ρ	0010000 100100 100100		_ م
rent Permission Scan Settings	Contract Contracting	oure loads		192.168.112.140	D8251		CPA_Secondary CPA_Secondary	OB1@239_192.168.112.140		
ault SQL Server Settings				DB251	D8251		CPA_Secondary	OB1@239_DB251		-
tings	Stale Object Settings :	90 Days *	🖌 Soly	Find All Shares						XI
sole	Data Set Name	Agent	Last Scan				×	Scan Type	Component Type	
	CPA_SWM97	Local	3/19/2024 4:17:12	2 Data Cat Infor			d.\\\$VH97\dept_share\$The network name	Scheduled Scan	File Server	
	AD_CPA	Local	3/13/2024 11:07:0	Plasta set mio	Set same and description			Scan Once Only	Active Directory	
	CPA_FSDB251 CPA_FS239	192, 168, 112, 126 192, 168, 112, 126	3/18/2024 1:19:35 3/15/2024 4:16:30	6	accinante ana acacipaan			Scheduled Scan Scheduled Scan	File Server File Server	
	CPA_FS112140 CPA_FS112126	192, 168, 112, 126 192, 168, 112, 126	3/18/2024 1:27:13 12/13/2023 1:57:4	3			he path '\\192.168.112.140\Share 3_140\New fol	Scheduled Scan Scan method not defined	File Server	
	CPA_dmojan-16	192.168.112.126	12/20/2023 4:20:3	3	There are a second seco			Scan method not defined	File Server	
				Data Set Name:	AWS3 Open Buckets					
				Description:		2				
						<i>u</i>				
				-						
					< 8.m	k Ned > Cancel				
							-1			
										~
>	<									

Figure 13: Data Set Information

- Enter a Data Set Name and an optional Description
- Click Next

The Component and Server Information dialog box will be displayed

Enter the following information:

- Component Name
- Server Name
- AWS Access Key
- AWS Secret Key

**NOTE:** The instructions to generate the **AWS Access Key ID** and **AWS Secret Key** are given in Section 3 - Access Keys.

- Click Validate Information to validate the details which have been entered
- The Information validated successfully message box will be displayed:



Settings										
G Component Management	Current Permission	n Scan Settings								
Iepsoftpvtltd-admin.sharepoi	Primary Database		/	Secondary Database	[5]				c	11 × 1
⊕-III <sub>6</sub> File Servers IIII AWS3-IAM/AWS S31	Configure primary database	to store common information		Secondary database will st	ore NTFS and Share permission for files and fol	sers selected in the datas	sets			
CODA_NEW										120
C LepSoftPvtLtd.onmicrosoft.co	SQL Server: D8251			D Hie Server(t)	Sq otriver name		P			Q
Current Permission Scan Settings	Database : CPA_Primary	yD61@10.239		192.168.112.126	D8251		CPA_Secondar	DB1@239_192.168.112.126		
Message Delivery Settings				DB251	D8251 D8251		CPA_SecondaryOB1@239_192.168.112.140 CPA_SecondaryOB1@239_09213			
- So UEBA										
A Agent Settings	Stale Object Settings :	90 Days -	🖌 Joply	Find Al Shares					c	t × 1
	Data Set Name	Agent	Last Scan				×	Scan Type	Component Type	
	CPA_SIN97 CPA_NPCMFS183	Local	3/19/2024 4:17	h12 KS Component at	nd Server Information		id.\{\$\M97\dept_share\$The network name	Scheduled Scan Scan method not defined	File Server	
<b>A</b>	AD_CPA	Local 102 168 112 126	3/13/2024 11:0	17:0 Please select comp	onent(s) and the server(s) to be scanned			Scan Once Only School and Scan	Active Directory	
19	CPA_F5239	192.168.112.126	3/15/2024 4:16	136			to and Store the tree sector of the sector	Scheduled Scan	File Server	
<u> </u>	CPA_F5112146 CPA_F5112126	192.168.112.126	12/13/2023 1:5	7:4 Component Name:	AWS S3	-	ne pari ((192.100.112.140 prare 3_140 year fo	Scan method not defined	File Server	
•	CPA_dttojan-16	192.168.112.126	12/20/2023 4:2	10:3	2002	12		Scan method not defined	He server	
				Server Name:	anso					
				AWS Access Key:	AKIAJMUY2UJH07U2Q30Q					
0				AWS Secret Key	IgVN1kWLp7SGGD7wvAbWDP/OBgoNP2v/H	72378				
• I										
					×	date information				
				-	0 120					
				() In	nformation validated successfully.					
				~						
					OK					
										~
					< Back	Next > C	lencel			
< >>	<									>

Figure 14: Component and Server Information

- Click **Ok**
- Click Next

The Scan Options dialog box will be displayed:

Settings			_						
- A Idsp5.com	Current Permission	Scan Settings							
Iepsoftpvtltd-admin.sharepoir     Im Im AWS3-IAM(AWS S3)	Primary Database Configure primary database t	to store common information	1	Secondary Database(s) Secondary database will store NTFS and Share permission	or files and folders selected in the datasets			c	• × 41
CODA_NEW	SOL Server : DR251			File Server(s) Sol s	iver name	Detabase			-
General Settings				PP		P			P
Current Permission Scan Settings	Database : CPA_Primary	OB1@10.239		192.168.112.126 DB25		CPA_Secondary	DB1@239_192.168.112.126		
Message Delivery Settings     Default SQL Server Settings				DB251 DB251	1	CPA_Secondary	DB1@239_DB251		-1
G UEBA	Stale Object Settings :	90 Days -	Jooh	Find All Shares		(881 B )			
🔂 LDSP Web Console	Date Cat Name	Area	Last Care				Core Tax	Constant Tors	· · ^ +/
Archive & Import	CPA_SVM97	Local	3/19/2024 4:17	112	*	d.\\\$\M97\dept_share\$The network name	Scheduled Scan	File Server	
	CPA_NPCNF5183	Local	12/20/2023 3:59	Scan Options			Scan method not defined	File Server	
	CPA_FSD8251	192.168.112.125	3/18/2024 1:19	35 Please select the scanning method.			Scheduled Scan	File Server	
	OPA_F5239 OPA_F5112140 OPA_F5112126	192.168.112.126 192.168.112.126 192.168.112.126	3/15/2024 4:16 3/18/2024 1:27 12/13/2023 1:5	136 113 7;4 Scan Now		he path '\\192.168.112.140\Share 3_140\Wew fol	Scheduled Scan Scheduled Scan Scan method not defined	File Server File Server File Server	
	Cry2nn-Jan te	192.000.112.020	12/20/2023 4:0	Schedule Scan			Scan method not delined	He server	
				Run every day at 12:24:16 PM, Schedule start from 3/26/2024	Change Schedule				
					1974				
									^
4				5					
					< Back Finish Caroel				
(I									
N									· · · ·



Choose the option you require:

-	Scan Now	to run a scan immediately
-	Schedule Scan	to specify when the scan should be run. Click Change Schedule
		to set the date and time for running the scan

Click Finish

This will return to the Current Permission Scan Settings screen and the newly added Data Set will be listed:

Settings	_									
-St Idso5.com	Current Permission	Scan Settings								
lepsoftpvtltd-admin.sharepoir     B    B    File Servers     AWS3-iAM(AWS S3)	Primary Database Configure primary database to	1	Second Secondar	<b>lary Database(s)</b> ry database will store NTFS ar	d Share permission for files and folders selected in the	datasets			tt X 🔪 🕻	
CODA_NEW	SQL Server : DB251				File Server(s)	Sd server name	Detabase			
see General Settings	Database : CPA_PrimaryD			192 168 112 126 192 168 112 140 DB251	08251 08251 08251 08251	لکر CPA_Seconday CPA_Seconday CPA_Seconday	DB1@239_192.168.112.126 DB1@239_192.168.112.140 DB1@239_DB251		_ م •	
- 🔂 UEBA - 🙀 Agent Settings	Stale Object Settings :	90 Days -	🖌 Apply	Fi	nd All Shares					
🔯 LDSP Web Console 🔯 Archive & Import	Data Set Name CPA_SVM97 CPA_NPCMP5183	Agent Local Local	Last Scan 3/19/2024 4: 12/20/2023 3	17:12 PM	Next Scan 4/2/2024 4:15:00 PM Never	Statue Pailed to scan : \\SVM97\dept_share\$The network nam Success	re cannot be found. \\\$VM97\dept_share\$The network name	Scan Type Scheduled Scan Scan method not defined	Component Type File Server File Server	
	50:53 AD_CPA CPA_FSDB251 CPA_FSDB251 CPA_FS112190 CPA_FS112126 CPA_stnc-jsn-16	Local 192.168.112.125 192.168.112.125 192.168.112.125 192.168.112.125 192.168.112.125	3/13/2024 11 3/18/2024 1: 3/15/2024 4: 3/15/2024 4: 12/13/2023 1 12/20/2023 4	:07:02 AM 19:35 PM 16:36 PM 27:13 PM :57:43 PM :20:38 PM	Nover 3/26/2024 1:00:00 PM 3/26/2024 4: 15:00 PM 3/26/2024 1: 15:00 PM Nover Nover	In Progress Success Success Pailed to scan : \\192.168.112.140\Share 3_140\New Success	folder Access to the path 1/192, 168, 112, 140/Share 3_14074ew fol	Scan Circe Only Scheduled Scan Scheduled Scan Scheduled Scan Scheduled Scan Scan method not defined Scan method not defined	AWS 53 Active Directory File Server File Server File Server File Server File Server File Server	
	Data Set Information Data Set Name Description Component Type Status	: aws3 : : AWS 53 : In Progress								je j
< >	¢									, v

Figure 16: Data Set Added

• If Scan Now was selected, the scan will start immediately

Once the scan has run successfully, you can generate the Open AWS S3 Buckets Report

#### 4.2.2 Running the Open AWS S3 Buckets Report

- From the Lepide Web Console Home screen, select Lepide Trust
- From the Lepide Trust menu, select Reports
- Expand Risk Analysis from the list of reports on the left-hand side
- Select Open AWS S3 Buckets
- Click Generate Report

## The example below shows the Open AWS S3 Buckets Report:

Report Name - Open AWS S3 Buckets												
Filters : Server Name(s) : [Equals [All]]												
Home / Lepide Trust / Reports / Open AWS S3 Buckets Generate Report												
Server Name(s)	Copen Bucket Name	Owner 1	Permissions	Scan Time								
Q	Q	Q	Q	Q								
AWSBucket	abcdeft	tarunkumar456	Everyone: READ; READ PERMISSIONS; , AWS Authentic	05-06-2025 15:49:35								
AWSBucket	awssanitybucket01	tarunkumar456	Everyone: READ; READ PERMISSIONS; , AWS Authentic	05-06-2025 15:49:35								
AWSBucket	bucketsanity	tarunkumar456	Everyone: READ; READ PERMISSIONS; , AWS Authentic	05-06-2025 15:49:35								
AWSBucket	sanity4	tarunkumar456	Everyone: READ; READ PERMISSIONS; , AWS Authentic	05-06-2025 15:49:35								
AW5Bucket	sanity5	tarunkumar456	Everyone: READ; , AWS Authenticated Users: READ; RE	05-06-2025 15:49:35								
AWSBucket	sanity7	tarunkumar456	Everyone: READ: READ PERMISSIONS: , AWS Authentic	05-06-2025 15:49:35								
AWSBucket	sanitytesting	tarunkumar456	Everyone: READ; READ PERMISSIONS; , AWS Authentic	05-06-2025 15:49:35								
AWSBucket	sanitytesting1	tarunkumar456	Everyone: READ: READ PERMISSIONS: , AWS Authentic	05-06-2025 15:49:35								
AWSBucket	sanitytesting2	tarunkumar456	Everyone: READ; READ PERMISSIONS; , AWS Authentic	05-06-2025 15:49:35								
AWSBucket	spawsbuck26	tarunkumar456	Everyone: READ: READ PERMISSIONS: , AWS Authentic	05-06-2025 15:49:35								
	Total Records - 10 First	Previous 1 /1 Next	Last 200 / Page 👻									

Figure 17: Open AWS S3 Buckets Report



## 5 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 https://www.lepide.com/data-security-platform/.

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

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