# Veritas<sup>™</sup> Desktop and Laptop Option 9.7 Cloud Support

VERITAS

# Contents

1	All C	DLO server components deployed on cloud platform and DLO agents on premises in the
со	rporate	e network4
	1.1	On Amazon Web Services (AWS)4
	1.1.1	1 Pre-requisites for deployment4
	1.1.2	2 Deployment Steps5
	1.2	On Microsoft Azure
	1.2.2	1 Pre-requisites
	1.2.2	2 Steps for deploying all DLO Server components on Azure8
2	DLO	Storage Component on AWS and DLO Server Component on-premises
	2.1	AWS Storage Gateway running in on-premises machine:
	2.1.2	1 Introduction
	2.1.2	2 Introduction to AWS Volume Storage Gateway17
	2.1.3	3 Pre-Requisites:
	2.1.4	4 Deployment of AWS Volume Storage Gateway:18
	2.2	AWS Storage Gateway running on EC2 machine:

Veritas Desktop and Laptop Option: DLO with Amazon Web Services (AWS) Cloud

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version for Veritas DLO 9.7

#### Legal Notice

Copyright (c) 2022 Veritas Technologies LLC. All rights reserved. Veritas, and the Veritas Logo are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Veritas product may contain third party software for which Veritas is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Veritas product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Veritas Technologies LLC and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. Veritas CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Veritas Technologies LLC 2625 Augustine Drive Santa Clara, California 95054, U.S.A http://www.Veritas.com/

# 1 All DLO server components deployed on cloud platform and DLO agents on premises in the corporate network.

**Benefit** - No restriction on storage size, backup storage can be increased as and when required since storage location is in cloud.

Supported on following cloud service providers -

- Amazon Web Services (AWS)
- Microsoft Azure

DLO server components include DLO Administration server, DLO Dedupe Server, DLO Maintenance Server, DLO Database (DLO and Dedupe Databases), DLO IO Server, DLO Edge Server and DLO Storage

# 1.1 On Amazon Web Services (AWS)

Deploy all DLO Server components on AWS EC2 machine. All DLO Server components can reside on same EC2 machine or can be distributed in different EC2 machine residing in same cloud virtual private network (VPN).

Configure, DLO Storage on a EC2 machine as a SMB share (File Share). Deploy the DLO Agents on the on-premises local corporate network.

**Note:** Organizations can leverage on how the DLO Agents can communicate to the DLO server components residing on cloud. Based on the available network connectivity, this can be achieved either through a Virtual Private Network (in case of LAN connectivity) or through BOI (Backup over Internet).

The BOI setup and configuration remains same for on-premises and above deployment. To refer the BOI configuration steps and details, refer following URL BOI Setup and Configuration Details

For the information related to the DLO Hardware requirements refer Hardware Requirements and for Software compatibility List (SCL) refer SCL.

#### 1.1.1 Pre-requisites for deployment

- An AWS account.
- It is recommend having good connectivity for seamless data transfers, to avoid perceived latency due to internet connectivity issues. Recommended bandwidth should be minimum of one MBPS.

## 1.1.2 Deployment Steps

Below steps are followed for deploying all DLO Server components on AWS. Detailed steps are in the following sections.

- Creating a site-to-site VPN connection.
- Configure DLO Server on AWS.
- Create DLO Storage Location (SL) and Dedupe Storage Location (DSL).
- Install DLO Agent in on-premises desktop machine.
- Test configured environment through DLO Backup and Restore.

#### i. Creating a site-to-site VPN connection

Create a site-to-site VPN connection by establishing Virtual Private Gateway, Transit gateway, Customer gateway device and Customer gateway. For more information on configuring the connections and gateways, refer Site-to-Site VPN Connection. It is required to have a secure site-to-site VPN connection between On-Premises network and cloud network for seamless data transfer.

Once the connection between Cloud network and On-Premises network is established, download the configuration file from the AWS Portal and share it to the On-Premises device manager. It is required for enabling the created Virtual network for site-to-site connection.

#### ii. Configure DLO Server on AWS

AD DS can exist on either cloud network or On-Premises network. In addition, all DLO components can be installed on one cloud Virtual Machine or multiple Virtual Machines by distributing the DLO components over different servers on cloud. Create both the VM's in same virtual network so that the shared resources will be accessible between these Virtual Machines.

Port requirement: Make sure On-premises device allows all the ports required for the VPN connection. In general, enabling of inbound and outbound TCP ports 135,139, 389, 53, 3389 and 445 are required for seamless site-to-site connectivity.

On EC2 instance install the DLO Server Components i.e. DLO Admin Console, DLO Maintenance server, DLO Database and Dedupe server, DLO Edge and IO Server on the Server. Configure the required settings of Storage Location (SL), Dedupe Storage Location (DSL), Automated User Assignment (AUA), and Profile from the DLO Administration Console.





#### iii. Create DLO Storage Location (SL) and Dedupe Storage Location (DSL)

- a. On the DLO Administrator Console in the Settings Pane, right click Storage Locations and select New Storage Location.
- b. In the New Storage Location wizard, provide the Cloud Server hostname; provide the path of the SMB/CIFS share created using an extra disk as a Storage location, Storage Location Name, Assign Dedupe Storage Location option.

10.3 × ×		Browse
10.3.0.0		D104436
Path:		
E:\SL		Browse
Storage location name:		
SL		
A Assim Dadam Desertion		
Assign Dedupe Properties		
		<u> </u>
Dedupe Storage Location		
[NOT DEFINED]		<b>~</b>
Automatic Mode	C Manual Mode	Create
Edge Server:IO Server		
[NOT DEFINED]		-
ummary		
Users assigned to this storage folders created in the following	location will back up deskto location and format:	p data to user data
INTU.S.X.X\SE\%USERDUMA	AIN%%USEHNAME%	

- c. Create a DSL from the setting pane or create DSL while creating SL. In 'New Storage Location' window, opting automatic mode will create DSL in the same share as SL whereas selecting manual mode allows to assign required DSL from the existing list of drop down to this SL.
- d. Assign the required Edge and IO Server details and click OK to create a Storage Location

#### iv. Install DLO Agents in on-premises desktop machine

Add the desktop machine where DLO Agents will be installed to the network of the same Cloud domain. Install the DLO Agent accessing the Server share located on the Cloud.

Assign the designated DLO Storage Locations for the User from DLO Console.

#### v. Test configured environment through DLO Backup and Restore

Launch the DLO Agent residing in on-premises desktop machine. Verify the backup of the files required, either by adding them to the Backup Selection or providing the path of the backup selection in the Profile of DLO Administrator console.

Restore the backed up files from DLO Agent and verify the restoration of all the files along with their revisions.

# 1.2 On Microsoft Azure

For this deployment, all DLO Server components are deployed on Virtual machine(s) residing on Microsoft Azure. The DLO storage is configured on a Microsoft Azure Virtual machine (File Server) as a SMB share (File Share). The DLO agents are deployed on the on-premises local corporate network.

Organizations can leverage on how the DLO Agents can communicate to the DLO server components residing on cloud. Based on the available network connectivity, this can be achieved either through a Virtual Private Network (in case of LAN connectivity) or through BOI (Backup over Internet).

The BOI setup and configuration remains same for on-premises and cloud deployment. To refer the BOI configuration steps and details, refer following URL BOI Setup and Configuration Details.

For the information related to the DLO Hardware requirements refer Hardware Requirements and for Software compatibility List (SCL) refer SCL.

## 1.2.1 Pre-requisites

- An Azure account with active subscription.
- For the generic purpose hardware and the compatible Virtual machine sizes for CPU to memory ratio which are ideal for testing and development, refer article Requirements
- It is recommend having good connectivity for seamless data transfers, to avoid perceived latency due to internet connectivity issues. Recommended bandwidth should be minimum of one MBPS.
- For details regarding to the Hardware requirements and compatible configuration of VPN devices refer VPN Device Requirements

## 1.2.2 Steps for deploying all DLO Server components on Azure

Below steps are followed for deploying all DLO Server components on Azure. All of below steps are detailed in the following sections.

- Creating site-to-site VPN connection
- Configuring Azure disk storage
- Configuring DLO Server and DLO Agent
- Creating DLO Storage Location
- Creating a Dedupe Storage Location

#### i. Creating site-to-site VPN connection

Create a site-to-site VPN connection by establishing Virtual network, VPN gateway, local network gateway and VPN connection as detailed below. For more information on configuring the networks, refer Secure Site-to-Site VPN Connection . It is required to

have a secure site-to-site VPN connection between On-Premises network and cloud network for seamless data transfer.

#### a. Create a Virtual Network

🕑 Vali	dation passed				
Basics	IP Addresses	Security	Tags	Review + create	
Basics					
Subscript	tion				
Resource	group		(new)	VPN	
Name			VNet	L_VPN	
Region			East L	IS	
IP addre	sses				
Address	space		10.3.0	.0/16	
Subnet			defau	lt (10.3.0.0/24)	
Tags					
None					
Security					
BastionH	ost		Disab	led	
DDoS pro	ptection plan		Basic		
Firewall			Disab	led	_

# b. Create a Virtual Network Gateway

✓ Validation passed		
Basics Tags Review + create		
Basics		
Subscription		
Resource group	VPN	
Name	VnetGW1	
Region	East US	
SKU	VpnGw1	
Virtual network	VNet1_VPN	
Subnet	GatewaySubnet (10.3.1.0/24)	
Gateway type	Vpn	
VPN type	RouteBased	
Enable active-active mode	Disabled	
Configure BGP ASN	Disabled	
Public IP address	VNetGW1_PIP	
Tags		
N		

# c. Create a Local Network Gateway

			in guit	Juna
Testi	ocalnetGW		~	
ID add	rocc * 🕕			I
13.9	2.173.35		~	
Addre	a anaca (i)			
10.0	1.0/24			
Ad	d additional ad	dress range		
	onfigure RGD se	ottings		
	inigure bor se	rungs		
c	intina *			
Subsc	ription ~		$\sim$	
Bacau	rea group + C	\ \		
DLO	lest	)	~	
Create	new			
Locati	on *			
			~	

# d. Create a Connection:

Name *	
VNet1toSite1	~
Connection type 🕕	
Site-to-site (IPsec)	$\sim$
*Virtual network gateway ①	A
VNet1GW	
*Local network gateway ① Site1	>
Shared key (PSK) * 🔅	
abc123	~
Use Azure Private IP Address 🕕	
Enable BGP ①	
KE Protocol 🔅	
Subscription ①	
Content Development	$\sim$
Resource group (i)	
TestRG1	8
Create new	
ocation (i)	
East US	$\sim$

#### e. Enabling the VPN for site-to-site connection

Once the connection between Cloud network and On-Premises network is established, download the configuration file from the Azure Portal and share it to the On-Premises device manager. It is required for enabling the created Virtual network for site-to-site connection.

#### f. Creating Virtual Machines

AD DS can exist either on cloud network or On-Premises network. And all DLO components can be installed on one cloud Virtual Machine or multiple Virtual Machines by distributing the DLO components over different servers on cloud. Create both the VM's in same virtual network (created in the previous step) by maintaining them in the same resource group, same Availability Set and same region, so that the shared resources will be accessible between these Virtual Machines.

#### g. Port requirement

Make sure On-premises device allows all the ports required for the VPN connection. In general, enabling of inbound and outbound TCP ports 135,139, 389 and 445 are required for seamless site-to-site connectivity. For more information, refer Ports Requirement





#### ii. Configuring Azure disk storage

Microsoft Azure cloud offers several types of scalable and with High-Availability storage. Azure offers two types of Storage Accounts, five types of storage, four levels of redundancy and three tiers for storing the data in cloud.

DLO supports Azure managed data disk for creating SMB/CIFS share. The SMB/CIFS share of the volume will be created by adding the required number of disks to the Azure Server VM. DLO can use the above-created volume as a Storage location.

**Note**: DLO Storage configured using Azure File Storage Services has some limitations as it does not support Active Directory based authentication and Access Control List (ACL). Hence DLO Storage configured using Azure File Storage Services is not supported.

#### To add the Storage disk to Server, below steps should be followed.

1. Go to **Disks** tab in **Azure Server** machine and click on **"+Add data disk**" to add an extra premium disk with required size for SMB/CIFS File share to use it for DLO Storage Location option.

Search (Ctrl+/)	<ul> <li>K Edit O Refresh P Encryption Z Swap OS Disk</li> </ul>					
Overview	A					
Activity log	Managed disks created since June 10, 2017 are encrypted at res	st with Storage Service Encryption (SSE). You may also v	vant to enable Azure Disk Encryption,	ď		
Access control (IAM)						
Tags	Illera Dick compatibility is not available for this location					
Diagnose and solve problems						
ttings	Disk settings					
Networking	Enable Ultra Disk compatibility ③					
Connect	OS disk					
Disks	Name	Size	Storage account type	Encryption ③	Host caching	
Size		127 GiB	Premium SSD	SSE with PMK	Read/write	
Security	Data disks					
Advisor recommendations	None					
Extensions	A Add dots diek					
Continuous delivery	+ Add data disk					

2. Provide the required details and make sure that the disk created in the same resource group where server exists.

me > Virtual machines > Disks >	
reate a managed disk	
5	
ante a new diek to store applications and data on your VM. Diek pricing varies based on fact	tors including disk size
rage type, and number of transactions.	tors including disk size,
k name * 🕕	
isk2	~
source group *	
	$\sim$
ate new	
ation	
ast US	
ailability zone ①	
lone	
Irre type ①	
ione	~
- * 0	
GiB	
remium SSD	
hange size	
cryption type *	
Default) Encryption at-rest with a platform-managed key	~
Create	

3. Make sure the Read/write permissions exists to the disk for having seamless data transfer.

Data disks						
LUN	Name	Size	Storage account type	Encryption 🛈	Host caching	
2	✓ disk2	V 8 GiB	Premium SSD	Not enabled	Read/write	× ···
+ Add data disk						
						_

To know more about the Azure storage types for when to use which types of storage and their services, refer Azure Storage types

• For more information about creating a storage account suitable for configuration, refer <u>Storage</u> <u>Account Creation</u>

#### iii. Configuring DLO Server and DLO Agent

- 1. Both the Azure VM's created in one virtual network should be added to the same cloud domain, ensuring that the private IP address of both the machines are in same subnet.
- Once the Server VM added to the Cloud domain, install the DLO Server Components i.e. DLO Admin Console, Maintenance server, Database and Dedupe server, Edge and IO Server on the Server. Configure the required settings of Storage Location (SL), Dedupe Storage Location (DSL), Automated User Assignment (AUA), and Profile from the DLO Administrator Console.
- 3. Add the Agent machine residing on the On-Premises network to the same Cloud domain. Install the DLO Agent accessing the Server share located on the Cloud. Assign the designated DLO Storage Locations for the User.

#### iv. Creating DLO Storage Location

- 1. On the DLO Administrator Console in the Settings Pane, right click Storage Locations and select New Storage Location.
- 2. In the New Storage Location wizard, provide the Cloud Server hostname; provide the path of the SMB/CIFS share created using an extra disk as a Storage location, Storage Location Name, Assign Dedupe Storage Location option.

orage Location		
0.3.X.X		Browse
ath:		
e <b>ss</b> ų		Browse
torage location name:		
ίL		
Assign Dedupe Properties		
Dedupe Server		
NUT DEFINED]		•
Dedupe Storage Location		
NOT DEFINED]		7
Automatic Mode	C Manual Mode	Create
dge Server:10 Server		
NOT DEFINED]		•
mmary		
sers assigned to this storage	location will back up desk	top data to user data
liders created in the following	location and format:	
\10.3.X.X\SL\%USERDOM	AIN%-%USERNAME%	
	OK C	Cancel Help

- 3. Dedupe Storage Location can be assigned manually or automatically. Opting Automatic mode will create DSL in the same share as SL. Selecting Manual mode allows to assign required DSL from the existing list of drop down to this SL.
- 4. Assign the required Edge and IO Server details and click OK to create a Storage Location

#### v. Creating a Dedupe Storage Location

- 1. On the DLO Administrator Console in the Settings Pane, right-click on the Dedupe Server and select Manage.
- 2. In the Manage Dedupe Server wizard, click the Dedupe Storage Pool tab and click Add
- 3. Now, click Dedupe Storage Location Tab, select the created Storage Location Pool, and click Add to add a Storage location to that Pool.
- 4. In Dedupe Storage Location wizard, select "+" button to add a new share.
- 5. In the Create New Share wizard, either browse and select the machine name or manually enter the Hostname/IP of the Cloud Server SMB share path. In the Path field, enter a DSL path to create and click Create.

ystem Dedupe Stor	Name	
Dedupe Storage Poo	Description	
Default		•
Dedupe Storage Loc	Create New Share X	
Name	Machine Name	Free Space
	10.3.X.X Browse	
	Path	
	E: \DSL Browse	
	Create Cancel	
<		<b>`</b>
	Ex: Domainivame (Userivame	
Add	Password	pe Credential
	Add Cancel	
		16

6. Provide relevant domain username and password and click ok to create a DSL.

#### vi. Test the Configured environment through Backup and Restore

Launch the DLO Agent residing in on-premises network. Verify the backup of the files required, either adding them to the Backup Selection or mentioning the path of the backup Selection in the Profile of DLO Administrator console.

Restore the backed up files from DLO Agent and verify whether the restoration of all files along with their revisions is successfully.

# 2 DLO Storage Component on AWS and DLO Server Component on-premises

DLO Server components include the DLO Administration Server, DLO Dedupe Server, DLO Maintenance Server, DLO Database (DLO and Dedupe databases), DLO IO Server, DLO Edge Server and DLO Storage (DLO and Dedupe Storage)

In this deployment, all DLO Server components and the DLO Agents resides in on-premises local corporate network and the DLO Storage that includes the Dedupe Storage configured on AWS cloud volume.

**Benefit:** Cost affective as DLO Server stays in on-premises machine and only Storage location resides in cloud.

You can choose to either run a) AWS Storage Gateway on-premises, as a virtual machine (VM) appliance, or b) In AWS, as an Amazon Elastic Compute Cloud (EC2) instance. Organizations where the Storage Gateway is deployed on premises, the communication is through AWS Storage Gateway, where as if the Storage Gateway is deployed on cloud, the communication is through VPN (in case of LAN connectivity) or through DLO BOI mode.

# 2.1 AWS Storage Gateway running in on-premises machine:



#### 2.1.1 Introduction

The AWS Storage Gateway is a service connecting an on-premises software appliance with cloud-based storage to provide seamless and secure integration between an organization's on-premises IT environment and AWS's Storage infrastructure. The service enables you to securely-store data on AWS cloud for scalable and cost-effective storage.

AWS Storage Gateway offers file-based file gateway, volume-based (Cached and Stored), and tape-based storage solutions. For more information related to AWS Storage Gateway, please refer AWS Storage Gateway

#### 2.1.2 Introduction to AWS Volume Storage Gateway

A Storage volume gateway provides cloud-backed storage volumes that can be mount as Internet Small Computer System Interface (iSCSI) devices from the on-premises application servers. The software appliance, or gateway, is deployed into your onpremises environment as a virtual machine (VM) running on VMware ESXi, Microsoft Hyper-V, or Linux Kernel-based Virtual Machine (KVM) hypervisor.

This Volume gateway supports two types of volume configurations, Cache volume and Stored Volume. DLO supports both of the volume types for configuration of the storage volume in the AWS cloud.

With **cached volumes**, you store volume data in AWS, with a small portion of recently accessed data in the cache on-premises. This approach enables low-latency access to your frequently accessed dataset. It also provides seamless access to your entire dataset stored in AWS. By using cached volumes, you can scale your storage resource without having to provision additional hardware. For the architecture and details for creating disks for cache storage and upload buffer, please refer Cached Volume Concepts

With **stored volumes**, you store the entire set of volume data on-premises and store periodic point-in-time backups (snapshots) in AWS. In this model, your on-premises storage is primary, delivering low-latency access to your entire dataset. AWS storage is the backup that you can restore in the event of a disaster in your data center. For more details regarding stored volume, please refer Stored Volume Concepts

## 2.1.3 Pre-Requisites:

- a. An AWS account.
- b. Before deploying and activating storage gateway, select the respective AWS region where the file, volume, snapshot data has to be stored. For more details regarding the supported AWS Regions for the service endpoints and for the use of hardware appliances, please refer AWS Region support.

- c. For hardware and required support of the host platform, please refer Requirements
- d. For using or managing the AWS Storage gateway hardware appliance, please refer Using Hardware Appliance

#### 2.1.4 Deployment of AWS Volume Storage Gateway:

Deployment of on-premises AWS gateway volumes in VMWare ESXi Server.

- i) Steps for configuring AWS Volume gateway on VM:
- a. Choose a Gateway type. Once we create a volume gateway, we should be creat storage volume(s) in AWS cloud. This cloud storage volume will be accessed using its iSCSI targets.

Step 1 Select gateway type	Select gateway type Info	
Step 2 Select host platform	Gateway type	
	Choose gateway type	
Step 3 Select service endpoint Step 4 Connect to gateway	Amazon S3 File Gateway     Store files as objects in Amazon S3, with a local cache for     low-latency access to your most recently used data.	Amazon FSx File Gateway Low-Jatency on-premises access to fully managed, highly reliable, and virtually unlimited Windows file shares provided by Amazon FSx for Windows File Server.
Step 5 Activate gateway		L_EF\$X
Step 6 Configure local disks	<ul> <li>Volume gateway Block storage in Amazon S3 with point-in-time backups as Amazon EBS snapshots.</li> </ul>	Tape gateway Back up your data to Amazon S3 and archive in Amazon S3 Glacier using your existing tape-based processes.
Step 7 - <i>optional</i> Configure logging		<u>o</u>
Step 8 Review and finish	Choose volume type Cached volumes Low-latency access to your most recently used data.	
	<ul> <li>Stored volumes</li> <li>On-premises data with scheduled offsite backups.</li> </ul>	
		Cancel Next

b. Choose a host platform and download the respective VM image from AWS console to deploy the downloaded gateway VM on the host hypervisor. For more information related to the supported host platform for downloading the Gateway VM, please refer Supported Hypervisor and host requirements

Step 1 Select gateway type	Select host platform Info
Step 2 Select host platform	Platform options
Step 3 Select service endpoint	Choose host platform VMware ESXi Microsoft Hyper-V 2012R2/2016
Step 4 Connect to gateway	<ul> <li>Linux KVM</li> <li>Amazon EC2</li> <li>Hardware appliance</li> </ul>
Step 5 Activate gateway	Set up instructions for VMware ESXi 땐 Download image
Step 6 Configure local disks	<ol> <li>Connect to your gateway host's hypervisor by using your VMware vSphere client.</li> <li>Deploy the OVF template package that you downloaded.</li> </ol>
Step 7 - <i>optional</i> Configure logging	<ol> <li>Choose Next through the following three screens. You might be prompted to select a data store on which to store the .ova package.</li> <li>Allocate disks with Thick provisioned format.</li> </ol>
Step 8 Review and finish	<ol> <li>Synchronize the time of your gateway VM to match your gateway host's time.</li> <li>You must also ensure that the clock on your gateway host is synchronized with a Network Time Protocol (NTP) server.</li> </ol>
	Cancel Previous Next

c. Choose a service endpoint to have the required gateway access to AWS services.

Step 1 Select gateway type	Select service endpo	Dint Info	
Step 2 Select host platform	Service endpoint		
Step 3 Select service endpoint Step 4	Choose service endpoint <ul> <li>Public</li> <li>Publicly accessible endpoint.</li> </ul>	<ul> <li>FIPS</li> <li>Publicly accessible endpoint that complies with Federal Information Processing Standards (FIPS)</li> </ul>	VPC Accessible within your VPC only. If you are deploying your file gateway on-premises, you will also need to set un a provv in
Connect to gateway Step 5			EC2.

d. Once gateway VM is deployed on to the host hypervisor, note down the IP address this will be used to activate the storage gateway from AWS console.

AWS Storage Gateway - Configuration
######################################
1: HTTP/SOCKS Proxy Configuration 2: Network Configuration 3: Test Network Connectivity 4: View System Resource Check (0 Errors) 5: System Time Management 6: License Information 7: Command Prompt
0: Stop AWS Storage Gateway Press "x" to exit session
Enter command:

e. Activate the Gateway by providing the required details on the AWS console.

· · · · · · · · · · · · · · · · · · ·	rour AWS account. Learn more
Storage and data transfer pricing applies when you	u start using your gateway. Learn more
Gateway type	Stored gateway
Endpoint type	Public
AWS Region	Asia Pacific (Mumbai)
Gateway time zone	GMT +5:30 Bombay, Calcutta, Madras, N 🔻
Gateway name	DLO_StoredVol_GW ×
Add tags A tag consists of a case-sensitive key-value pair. F	For example, you could define a tag with key = Name and value = DatabaseBackups.
Key (128 characters maximum)	Value (256 characters maximum)
(Up to 50 tags maximum)	
(Up to 50 tags maximum)	

f. Once Gateway is activated, provision a cloud local disk in AWS Console. Provide respective disks for Cache and Upload buffer. For more information related to the recommended disks and their size please refer Disks and their recommended Sizes and Managing Local Disks

Select galeway type	Gateway is now active	/e.		×
Select host platform				
Select service endpoint	Configure local disks			
Connect to gateway	Choose the local disks on your gatewa	ay VM to use for upload buffer.		
Activate gateway	Learn more			
Picifiate galenay				C 0
Configure local disks				
Configure logging	Disk ID	Capacity	Allocated to	
		(2) Preparing local	disks	

- g. Continue Logging and configure the storage volume gateway.
- h. Once Gateway is established, create a volume from AWS console. Note down iSCSI target name. For more information regarding the creation of volume, please refer Creating a volume

<b>r</b> Fi	iter by ID, type, or other vol	ume at	tributes.										
	Volume ID		Status		Туре	•	Used	-	Size		Gateway		
	vol-0020a0ecea492c714		Gateway offlin	ne	Cached		4		50 GiB				
	vol-013c985f1fa00a284		Available		Cached			0%	30 GiB				
	vol-0ba4f299e5a12f9b1		Available		Cached			3%	100 GiB				
	vol-0e0eb15a2996b3094		Available		Cached			74%	20 GiB		ē		
2	vol-0518ba25750e1ddb6		Working stor.		Stored		- 1	4.895 GIB	150 GiB		0		
Deta	ills Tags												
	Volume ID	vol-0	e0eb15a2996b	309	4 (Cached)						Status	Available	
	Gateway			•	1						Used	14.895 GiB	
	CHAP authentication	ion 1	007.05								Size	20 GIB Cloudwatch	
	Initiator	-0.0	0 40.40400	-	anna ann an a						Host IP	Choudhand	
											Host port	3260	
										Snaps	hot schedule	-	
											Created	£100/00/00/00/00	Infradout

i. After creating a cloud volume, go to on-premises machine and install iSCSI initiator. Use local machine iSCSI initiator to connect to AWS storage volume created in previous step using iSCSI Target name. For more details refer Using the Volume

argets	Discovery	Favorite Targets	Volumes and Devices	RADIUS	Configuration
Quick (	Connect				
To disc DNS na	over and log ame of the ta	on to a target usin arget and then dick	ng a basic connection, t Quick Connect.	ype the IP	address or
Target	:			Qu	uick Connect
~					
uick C	onnect				$\times$
Targe provid to eac Conne to res	ts that are an led are listed In target indiv ections made tore them wil	vailable for connect below. If multiple vidually. here will be added II be made every tin	ion at the IP address or targets are available, y to the list of Favorite Ta he this computer restart	r DNS name ou need to argets and ts.	e that you connect an attempt
Targei provid to eac Conne to res Disco	ts that are an ed are listed h target indiv ections made tore them wil vered <u>t</u> arget	vailable for connect below. If multiple t vidually. here will be added Il be made every tin s	ion at the IP address or targets are available, y to the list of Favorite Ta to the list computer restart	DNS name ou need to argets and ts.	e that you connect an attempt
Targe provid to eac Conne to res Disco Nam	ts that are a led are listed th target indivi- ections made tore them will vered <u>t</u> arget e 1997.	vailable for connect below. If multiple ! vidually. here will be added II be made every tin s	ion at the IP address or targets are available, yu to the list of Favorite Ti ne this computer restart Sta	r DNS name ou need to argets and ts.	e that you connect
Targei provid to eac Conne to res Disco Nam	ts that are are ed are listed h target indi- ections made tore them wil vered <u>t</u> arget e 1997.	vailable for connect below. If multiple f vidually. here will be added II be made every tin s	ion at the IP address or targets are available, yi to the list of Favorite Ti ne this computer restart Sta Co	r DNS name ou need to argets and is.	e that you connect an attempt
Targe provid to eac Conne to res Disco Nam iqn,	ts that are an ed are listed h target indi- sctions made tore them wil vered target e 1997: ess report	vailable for connect below. If multiple ! vidually. In be added Il be made every tin s	ion at the IP address or targets are available, y to the list of Favorite Ti ne this computer restart Sta Cor	DNS name ou need to argets and ts.	e that you connect an attempt

- j. For more information related to managing a gateway or volume (Cache and Stored), please refer Managing Volume Gateway
- k. Refer Monitor gateway to know more about how to monitor a gateway in a cached volumes or stored volumes setup, including monitoring the volumes associated with the gateway and monitoring the upload buffer.
- I. Refer troubleshooting your Gateway issues for issues that might encounter working with the gateway.

#### ii) DLO Configuration

There are two parts to be considered in the DLO configuration, as mentioned below.

- 1. Create required DLO Storage Locations by providing the path of the local mounted AWS storage volumes (iSCSI initiator)
- 2. Backing up and restoring the data to and from these volumes, through the DLO Agent.

#### iv) Configuring DLO Server and DLO Agent

- 1. Ensure AWS storage gateway appliance Server, DLO server and DLO client are in same network and domain.
- Install the DLO Server Components i.e. DLO Admin Console, Maintenance server, Database and Dedupe server, Edge and IO Server on the Server. Configure the required settings of Storage Location (SL), Dedupe Storage Location (DSL), Automated User Assignment (AUA), and Profile from the DLO Administration Console.
- 3. Install the DLO Agent accessing the Server share. Assign the designated DLO Storage Locations for the User.

#### v) Creating a Dedupe Storage Location

- 1. On the DLO Administrator Console in the Settings Pane, right-click on the Dedupe Server and select Manage.
- 2. In the Manage Dedupe Server wizard, click the Dedupe Storage Pool tab and click Add
- 3. Now, click Dedupe Storage Location Tab, select the created Storage Location Pool, and click Add to add a Storage location (locally mounted drive through iSCSI target) to that Pool.
- 4. In Dedupe Storage Location wizard, select "+" button to add a new share.
- 5. In the Create New Share wizard, either browse and select the machine name or manually enter the Hostname/IP of the Cloud Server SMB share path. In the Path field, enter a DSL path to create and click Create.

System Dedupe Sto	Name	_	
Dedupe Storage Poo	Description		
Default			-
Dedupe Storage Loc	Create New Share	<	~
Name	Machine Name		Free Space
	10.3.X.X Browse		5
			)
	Path		
	E: \DSL Browse		
		6	
	Create Cancel	-	
<			>
	Ex: DomainName\UserName		
Add	Password	te Crei	dential
		-	
	Add Cancel		
	ARAMIN'S AND ARE AND ARAMIN'S AND AR	se	Help

#### vi) Creating DLO Storage Location

- 1. On the DLO Administrator Console in the Settings Pane, right click Storage Locations and select New Storage Location.
- 2. In the New Storage Location wizard, provide the Server hostname; provide the path of the SMB/CIFS share created using an extra disk as a Storage location (locally mounted drive through iSCSI target), Storage Location Name, Assign Dedupe Storage Location option.

Computer name:		
0.3.X.X		Browse
'ath:		
E:\SL		Browse
itorage location name:		
δL		
Assime Deduce Propertie		
Dedune Server	2	
		•
Dedupe Storage Location		
[NUT DEFINED]		+
Automatic Mode	C Manual Mode	Create
dge Server:10 Server		
[NOT DEFINED]		-
ummary		
Isers assigned to this storag olders created in the followi	je location will back up desktop ( ng location and format:	data to user data
V10.3.X.XVSLV&USERDO	MAIN%-%USERNAME%	

- 3. Dedupe Storage Location can be assigned manually or automatically. Opting Automatic mode will create DSL in the same share as SL. Selecting Manual mode allows to assign required DSL from the existing list of drop down to this SL.
- 4. Assign the required Edge and IO Server details and click OK to create a Storage Location

#### vii) Testing the Configured environment through Backup and Restore

- 1. Launch the DLO Agent. Verify file backup, either adding them to the Backup Selection or providing the path of the backup Selection in the Profile of DLO Administrator console.
- 2. Ensure the backup of the data is getting stored in the AWS Storage volume.
- 3. In the case of Cache volume, ensure the data backed up to the local cache volume is being uploaded to the cloud on regular basis based on size of storage gateway cache volume. Here upload of data from Storage Gateway happens synchronously. Monitor the progress of the uploaded data through the AWS CloudWatch. For more information about AWS CloudWatch, refer Amazon CloudWatch Metrics
- 4. In case of Stored Volume, ensure the data is backed up to local mounted drive of on-premises machine and getting uploaded to the AWS. Here upload of data from Storage Gateway happens asynchronously. Monitor the progress of the uploaded data through the AWS CloudWatch
- 5. Restore the backed up files to the Cloud Storage Volume from DLO Agent and verify file restoration with along their revisions.

# 2.2 AWS Storage Gateway running on EC2 machine:



Note: If EC2 machine is used to host AWS Storage Gateway then a secure VPN connection between iSCSI initiator (residing in on-premises machine) and EC2 machine is needed.

For more information related to creation, deployment and activation of gateway, refer Configuring Gateway and Types

Steps for configuring and running Storage Gateway in EC2 machine remains the same as described in section **2.1.4**. While selecting host platform, select 'Amazon EC2', rest all steps remains the same.