Arctera™ Desktop and Laptop Option 10.0 Cloud Support

Contents

Documentation Version: 2025

Legal Notice

Arctera US LLC | www.arctera.io

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.

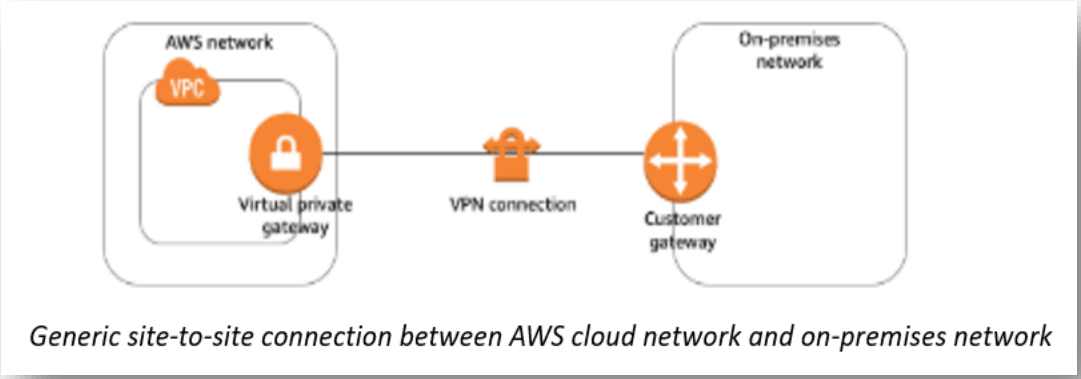
Once the connection between Cloud network and On-Premises network is established, download the configuration file from the AWS Portal and share it to the On-Premises device manager. It is required for enabling the created Virtual network for site-to-site connection.

ii. Configure DLO Server on AWS

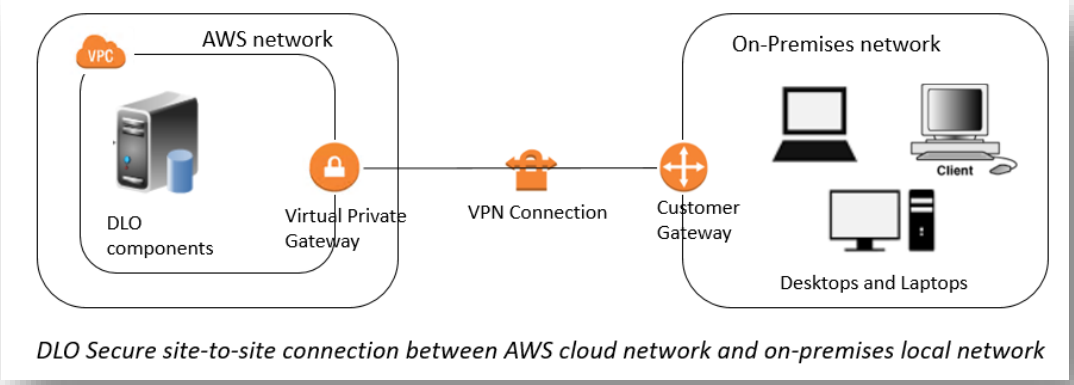
AD DS can exist on either cloud network or On-Premises network. In addition, all DLO components can be installed on one cloud Virtual Machine or multiple Virtual Machines by distributing the DLO components over different servers on cloud. Create both the VM's in same virtual network so that the shared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



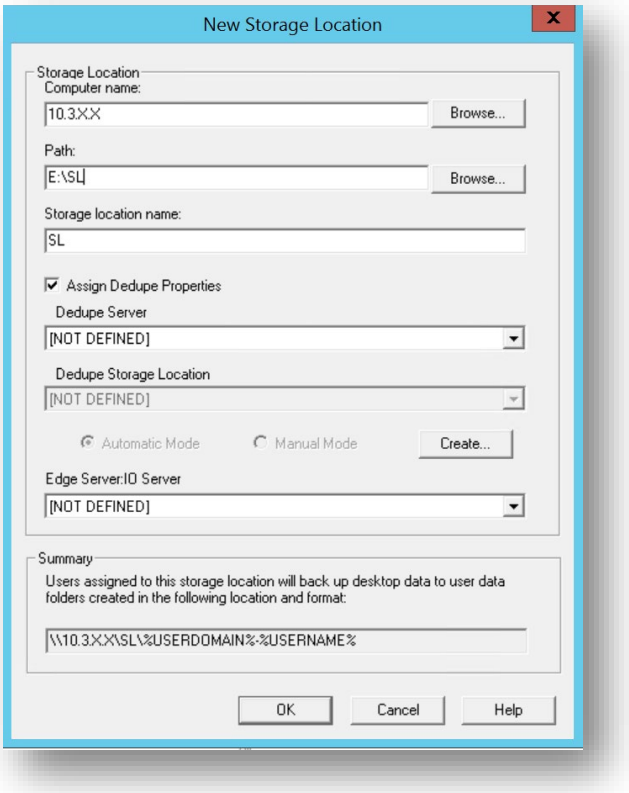
Generic site-to-site connection between AWS cloud network and on-premises network



DLO Secure site-to-site connection between AWS cloud network and on-premises local network

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.



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.

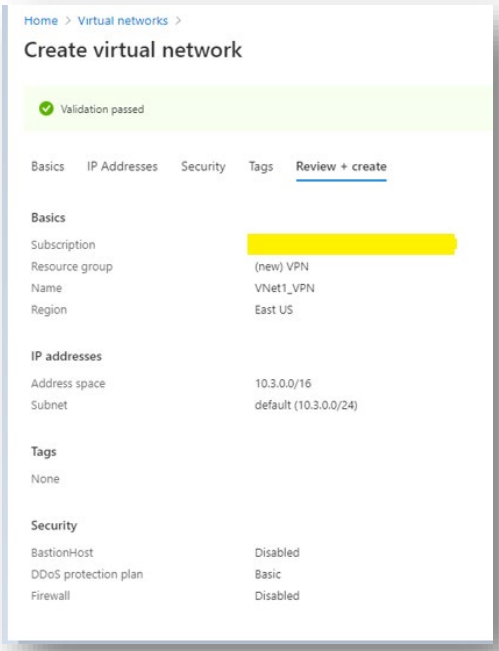
- Creating site-to-site VPN connection
- Configuring Azure disk storage
- Configuring DLO Server and DLO Agent
- Creating DLO Storage Location
- Creating a Dedupe Storage Location

i. Creating site-to-site VPN connection

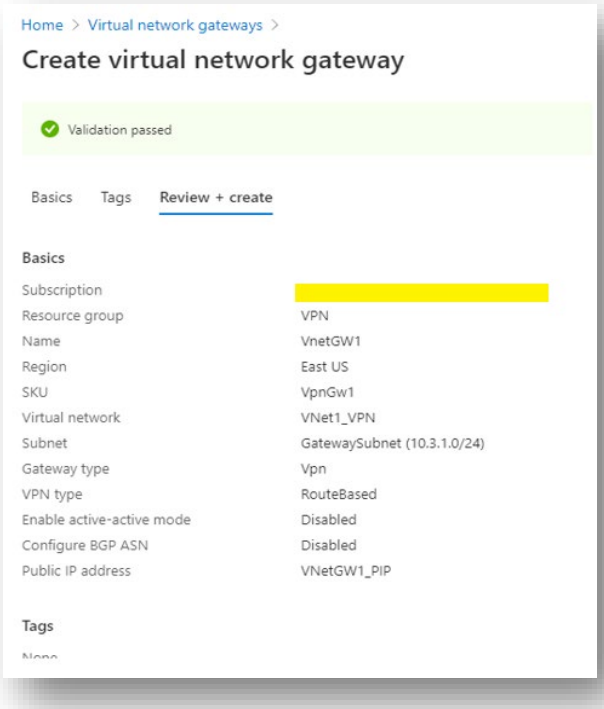
Create a site-to-site VPN connection by establishing Virtual network, VPN gateway, local network gateway and VPN connection as detailed below. For more information on configuring the networks, refer Secure Site-to-Site VPN Connection . It is required to

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

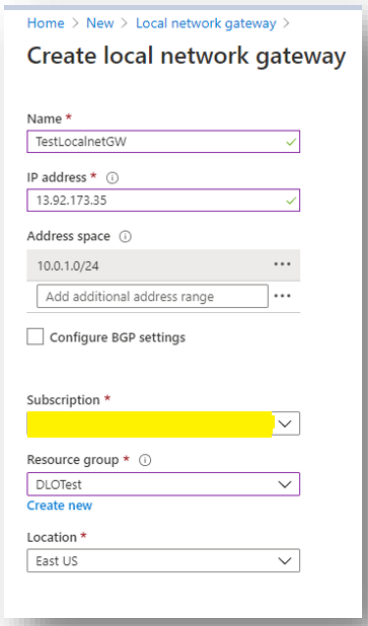
a. Create a Virtual Network



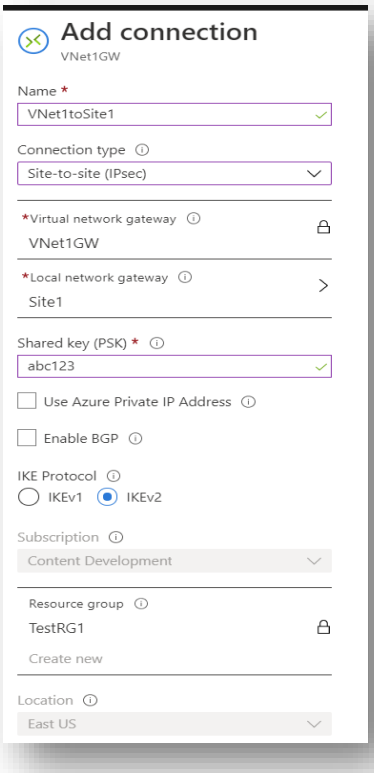
b. Create a Virtual Network Gateway



c. Create a Local Network Gateway



d. Create a Connection:



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

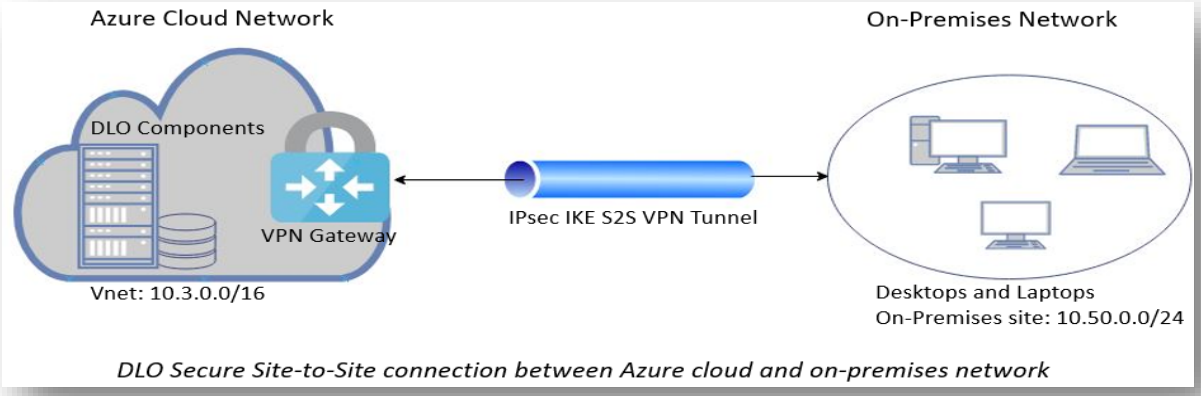
Once the connection between Cloud network and On-Premises network is established, download the configuration file from the Azure Portal and share it to the On-Premises device manager. It is required for enabling the created Virtual network for site-to-site connection.

f. Creating Virtual Machines

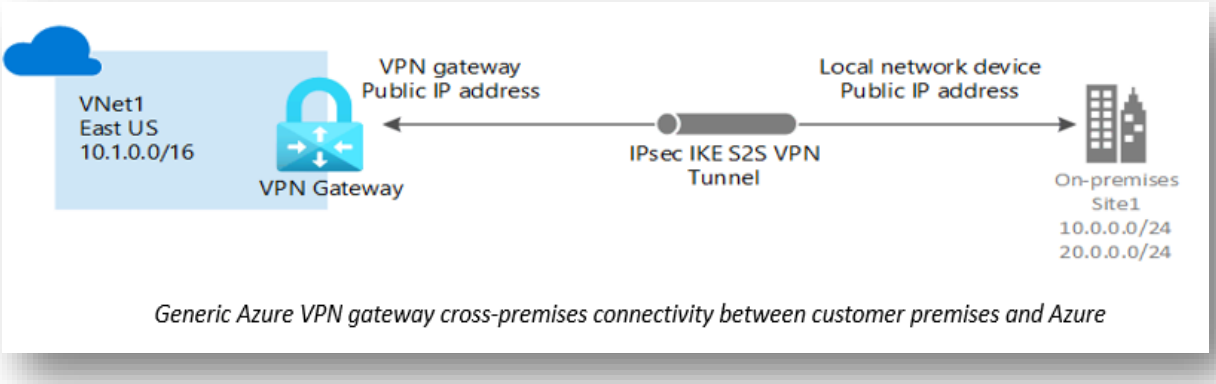
AD DS can exist either on cloud network or On-Premises network. And all DLO components can be installed on one cloud Virtual Machine or multiple Virtual Machines by distributing the DLO components over different servers on cloud. Create both the VM's in same virtual network (created in the previous step) 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



DLO Secure Site-to-Site connection between Azure cloud and on-premises network



Generic Azure VPN gateway cross-premises connectivity between customer premises and Azure

ii. Configuring Azure disk storage

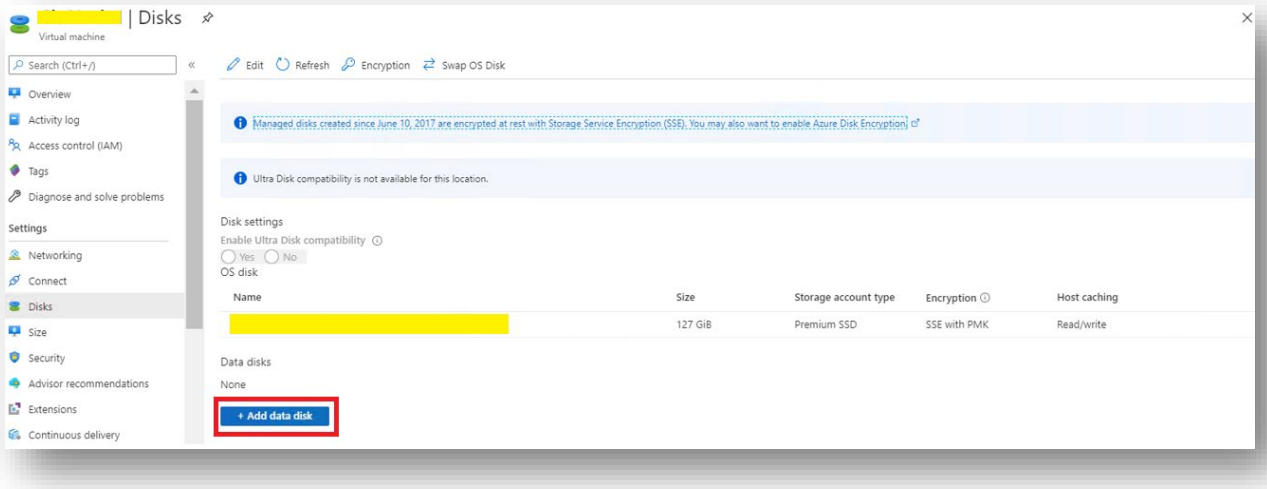
Microsoft Azure cloud offers several types of scalable and with High-Availability storage. Azure offers two types of Storage Accounts, five types of storage, four levels of redundancy and three tiers for storing the data in cloud.

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.

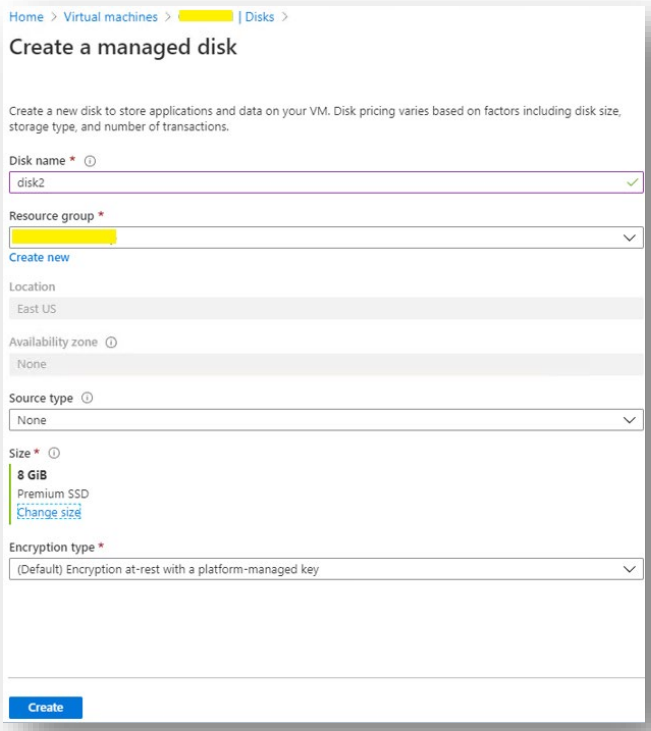
Note: DLO Storage configured using Azure File Storage Services has some limitations as it does not support Active Directory based authentication and Access Control List (ACL). Hence DLO Storage configured using Azure File Storage Services is not supported.

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

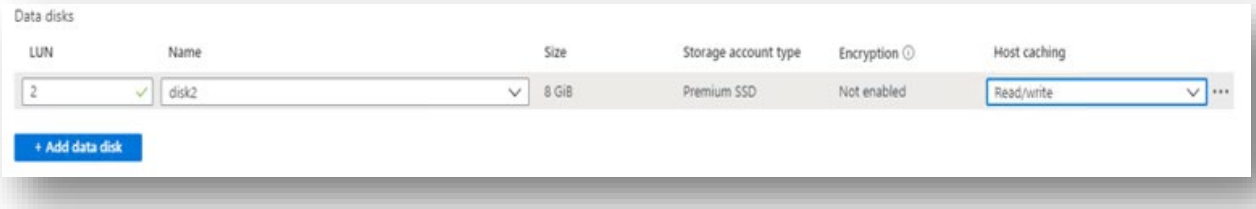
1. Go to **Disks** tab in **Azure Server** machine and click on **"+Add data disk**" to add an extra premium disk with required size for SMB/CIFS File share to use it for DLO Storage Location option.



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



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



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

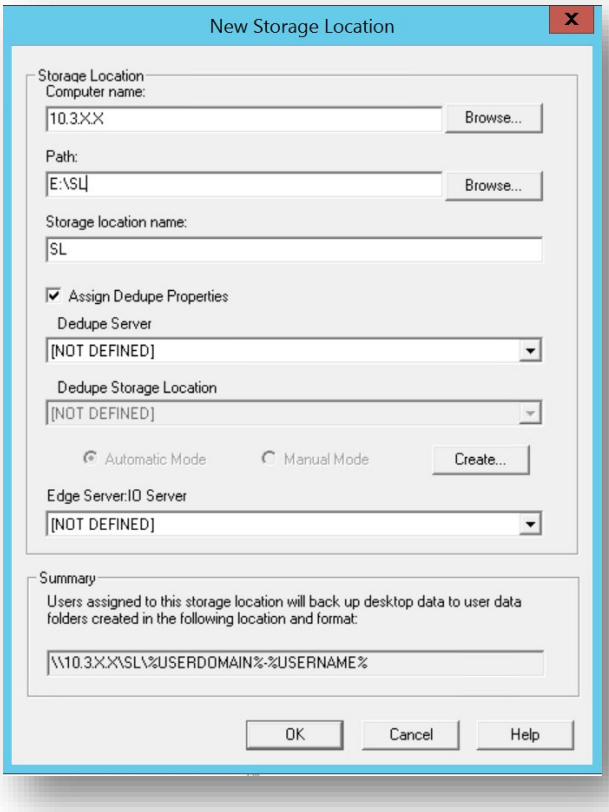
- For more information about creating a storage account suitable for configuration, refer Storage Account Creation

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.
2. 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

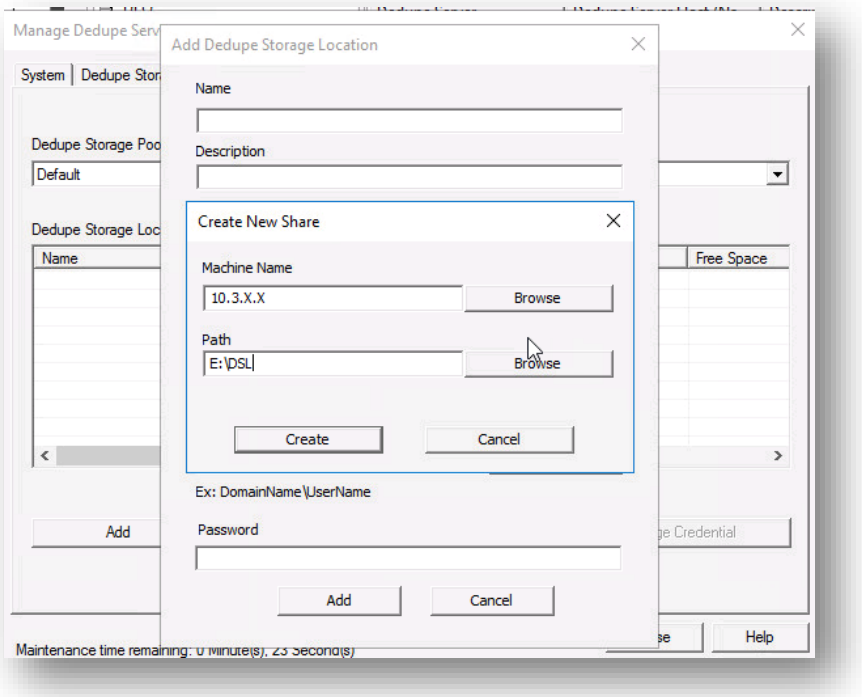
1. On the DLO Administrator Console in the Settings Pane, right click Storage Locations and select New Storage Location.
2. In the New Storage Location wizard, provide the Cloud Server hostname; provide the path of the SMB/CIFS share created using an extra disk as a Storage location, Storage Location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



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.



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

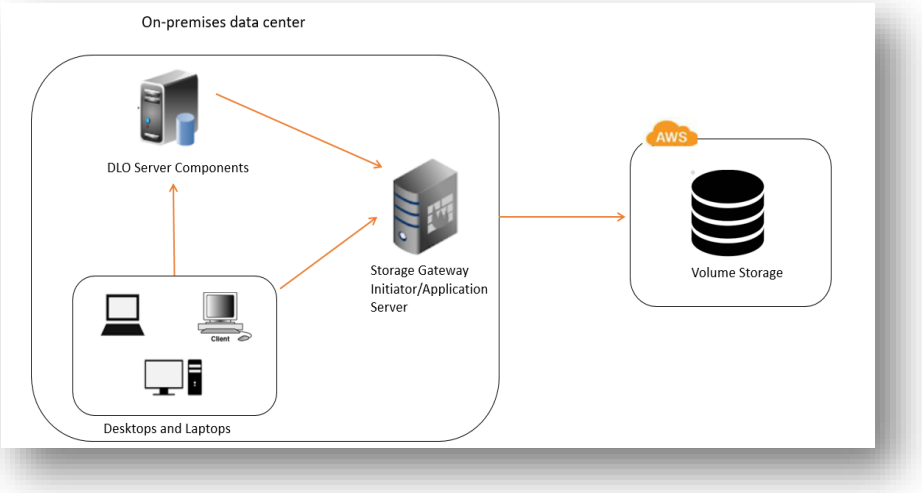
DLO Server components include the DLO Administration Server, DLO Dedupe Server, DLO Maintenance Server, DLO Database (DLO and Dedupe databases), DLO IO Server, DLO Edge Server and DLO Storage (DLO and Dedupe Storage)

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 on-premises 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.

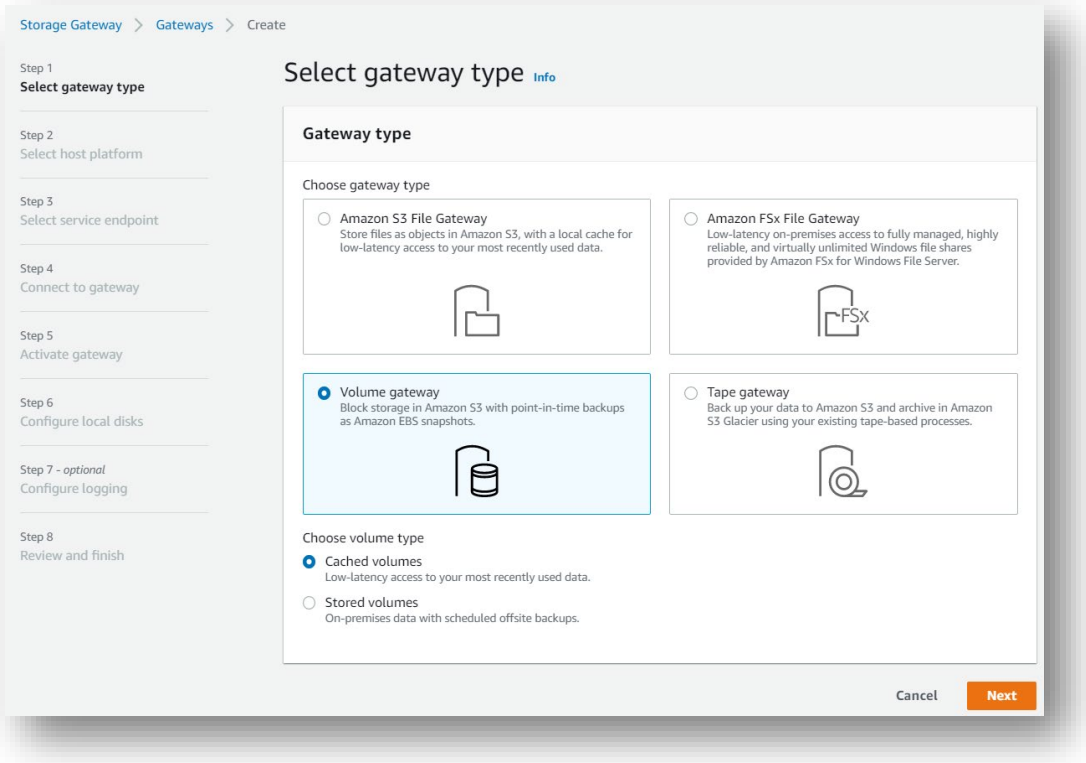
c. For hardware and required support of the host platform, please refer Requirements
d. For using or managing the AWS Storage gateway hardware appliance, please refer Using Hardware Appliance

2.1.4 Deployment of AWS Volume Storage Gateway:

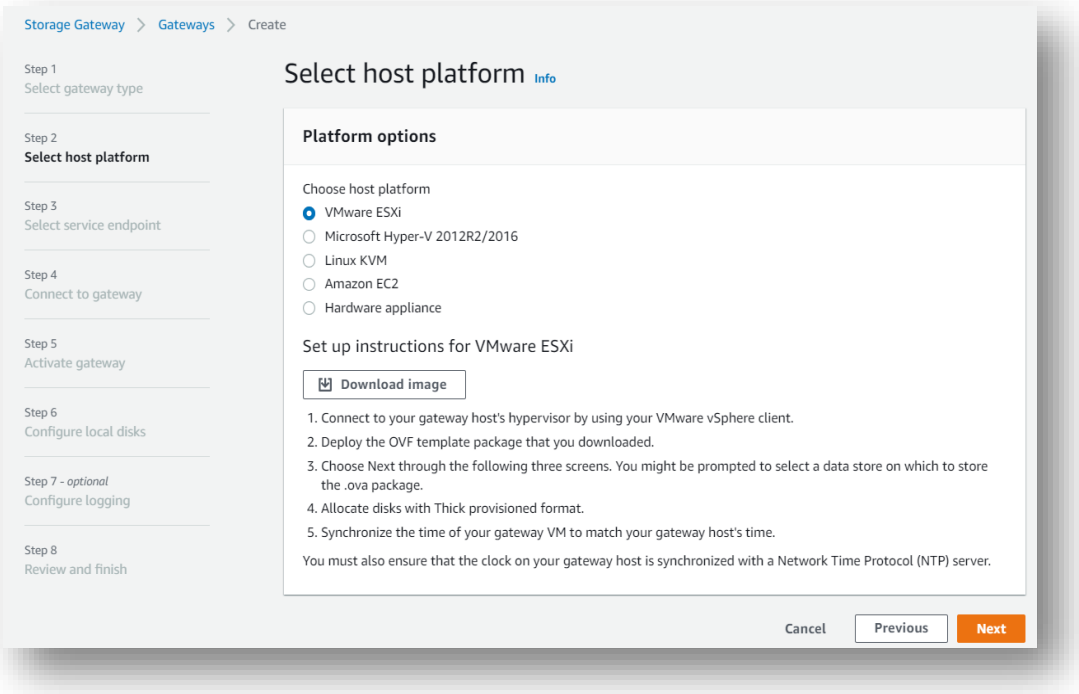
Deployment of on-premises AWS gateway volumes in VMWare ESXi Server.

i) Steps for configuring AWS Volume gateway on VM:

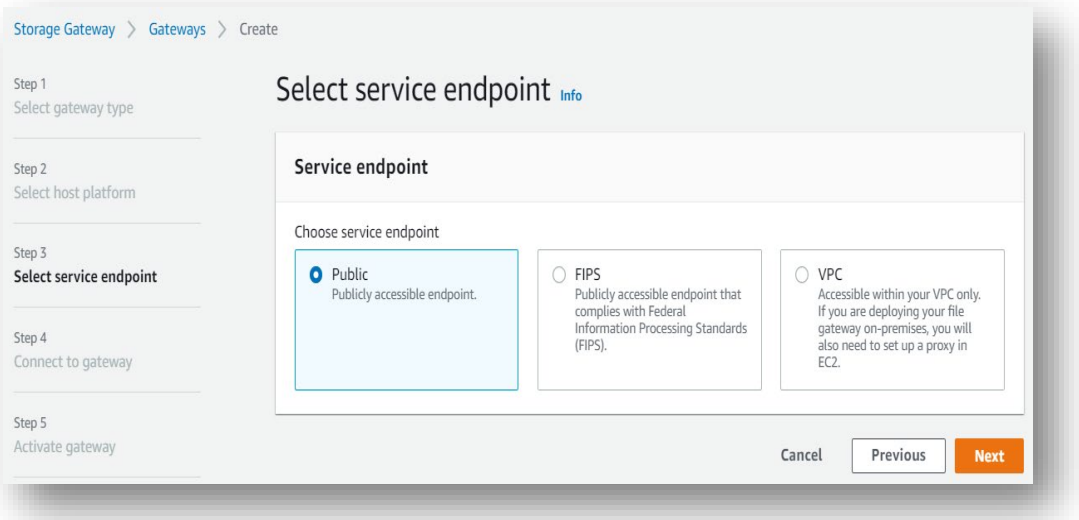
a. Choose a Gateway type. Once we create a volume gateway, we should be creat storage volume(s) in AWS cloud. This cloud storage volume will be accessed using its iSCSI targets.



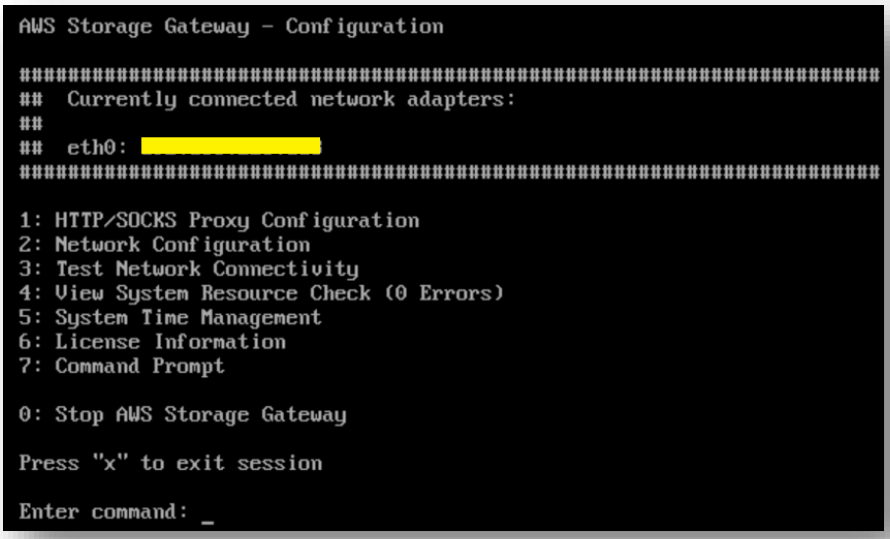
b. Choose a host platform and download the respective VM image from AWS console to deploy the downloaded gateway VM on the host hypervisor. For more information related to the supported host platform for downloading the Gateway VM, please refer Supported Hypervisor and host requirements



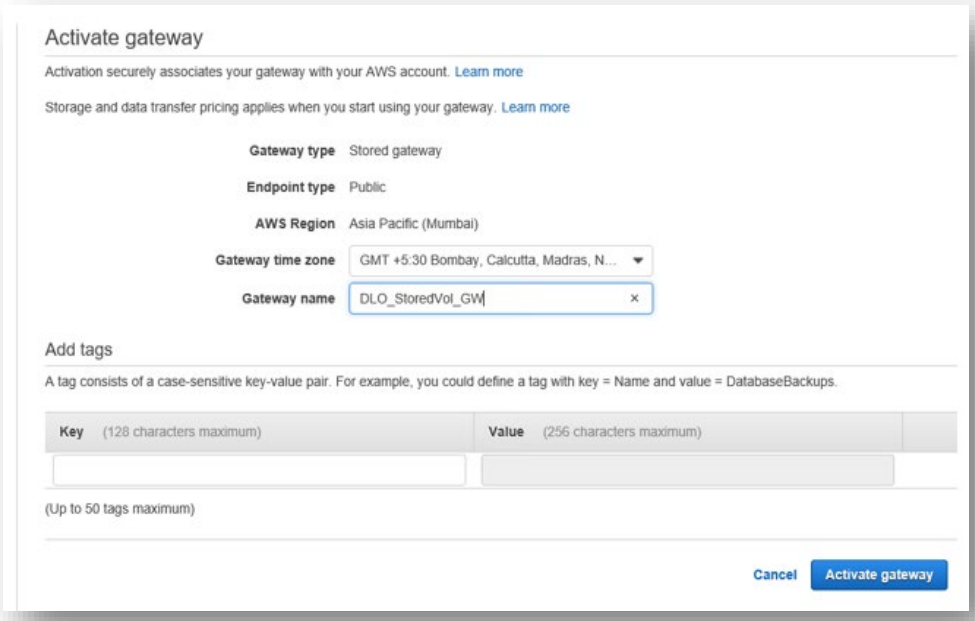
c. Choose a service endpoint to have the required gateway access to AWS services.



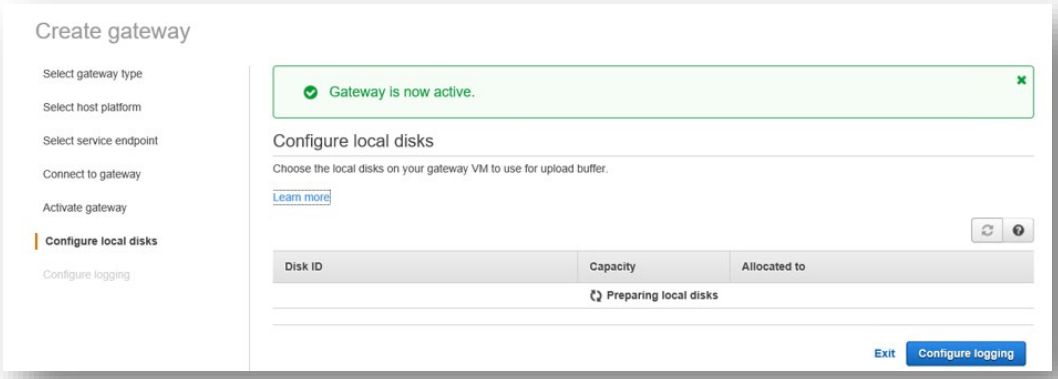
d. Once gateway VM is deployed on to the host hypervisor, note down the IP address this will be used to activate the storage gateway from AWS console.



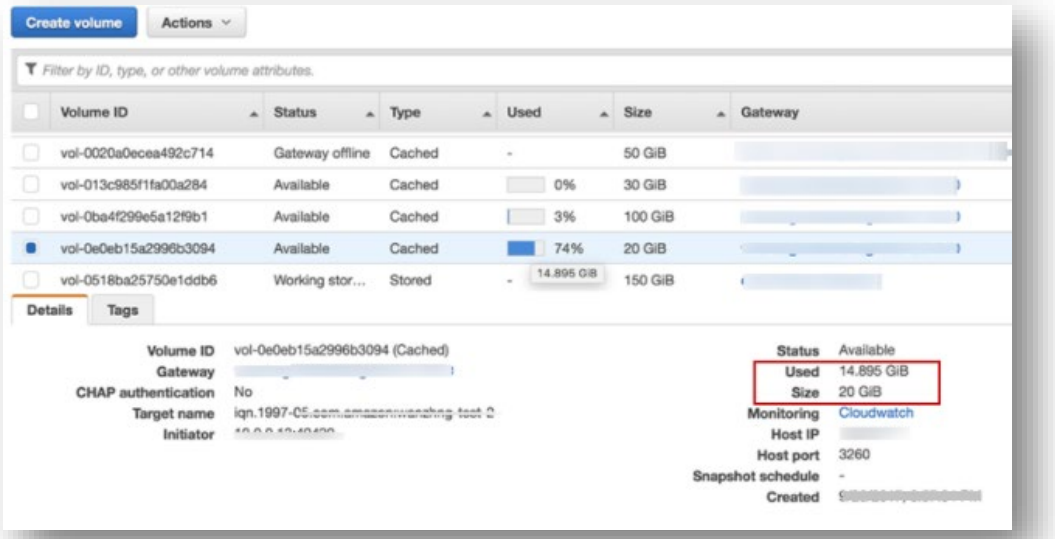
e. Activate the Gateway by providing the required details on the AWS console.



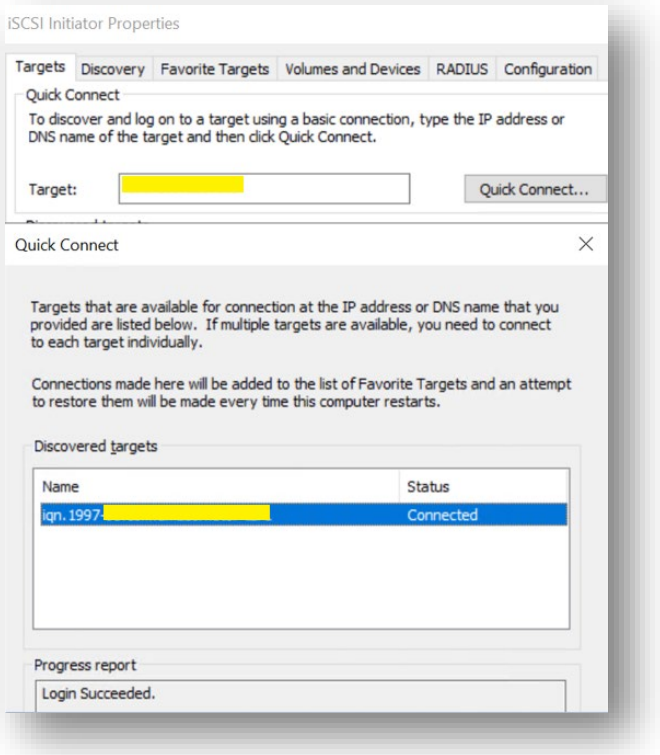
f. Once Gateway is activated, provision a cloud local disk in AWS Console. Provide respective disks for Cache and Upload buffer. For more information related to the recommended disks and their size please refer Disks and their recommended Sizes and Managing Local Disks



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



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



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.
l. 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.

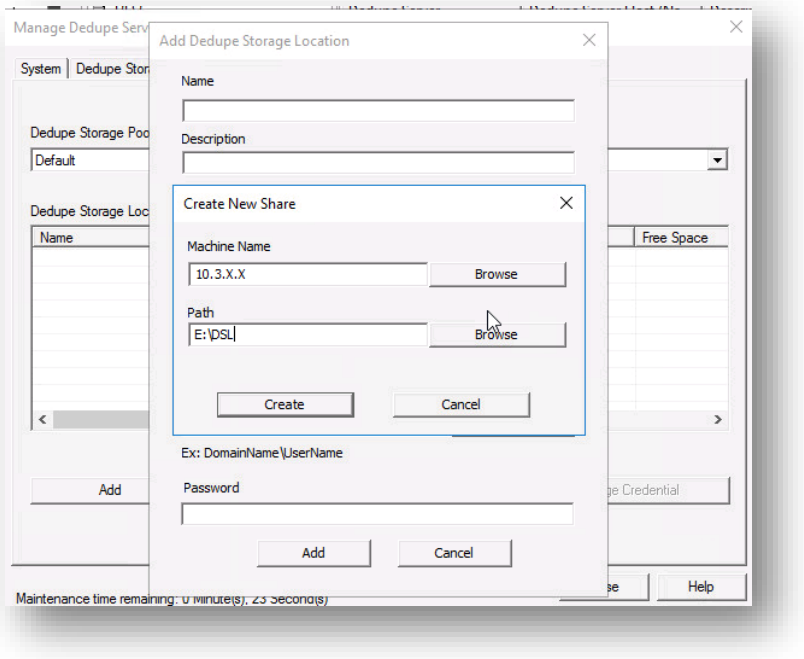
1. Create required DLO Storage Locations by providing the path of the local mounted AWS storage volumes (iSCSI initiator)
2. Backing up and restoring the data to and from these volumes, through the DLO Agent.

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.
2. 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.

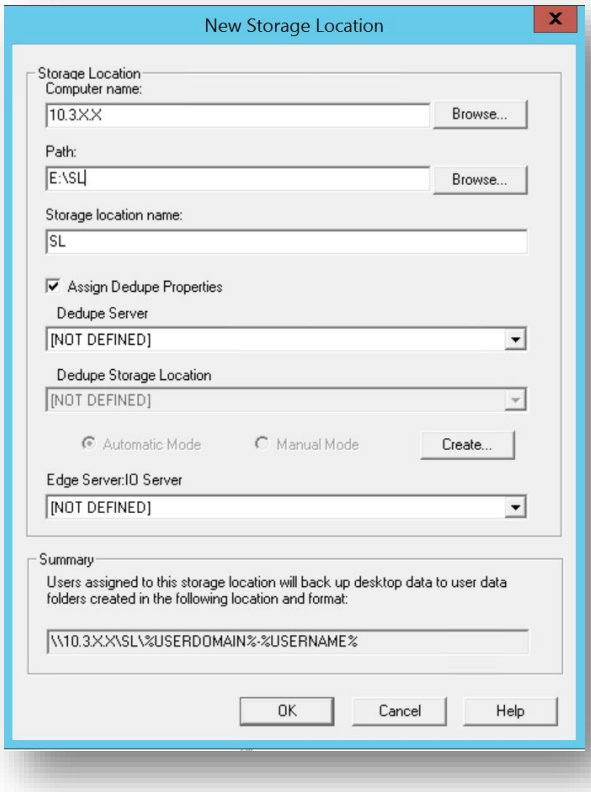
v) Creating a Dedupe Storage Location

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.



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.

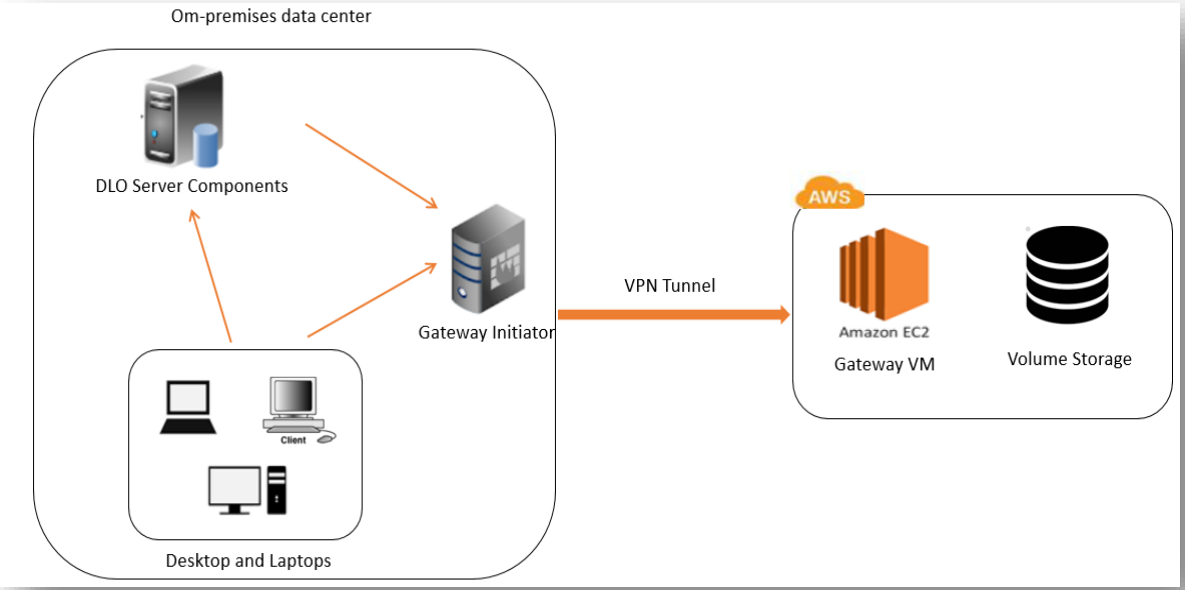


3. Dedupe Storage Location can be assigned manually or automatically. Opting Automatic mode will create DSL in the same share as SL. Selecting Manual mode allows to assign required DSL from the existing list of drop down to this SL.
4. Assign the required Edge and IO Server details and click OK to create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

3 Supported deployment of Arctera Desktop and Laptop Option (DLO) using Azure AD

Deployment Type – 1

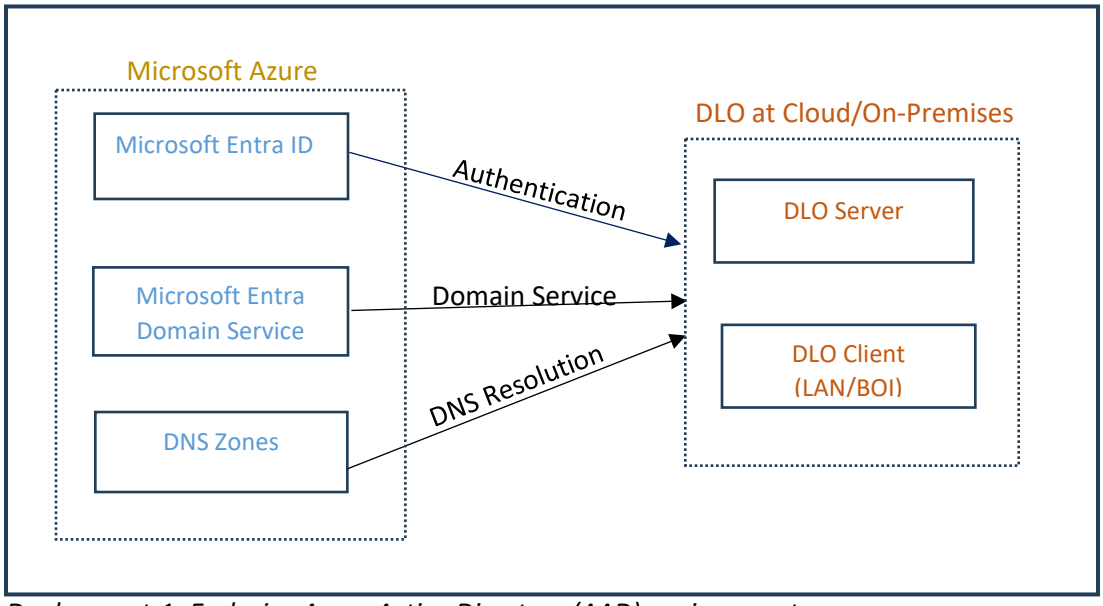
1. AD Service:

Exclusive Azure Active Directory (AAD) environment, where

Microsoft Entra ID for identity management, **Microsoft Entra Domain Services** and Azure **DNS Zones** records are used for domain resolution.

2. Domain Joined Machine:

- Arctera DLO Server machines are either on Cloud or On-Premises.
- Arctera DLO Client machines are either on Cloud or On-Premises.



Deployment-1: Exclusive Azure Active Directory (AAD) environment

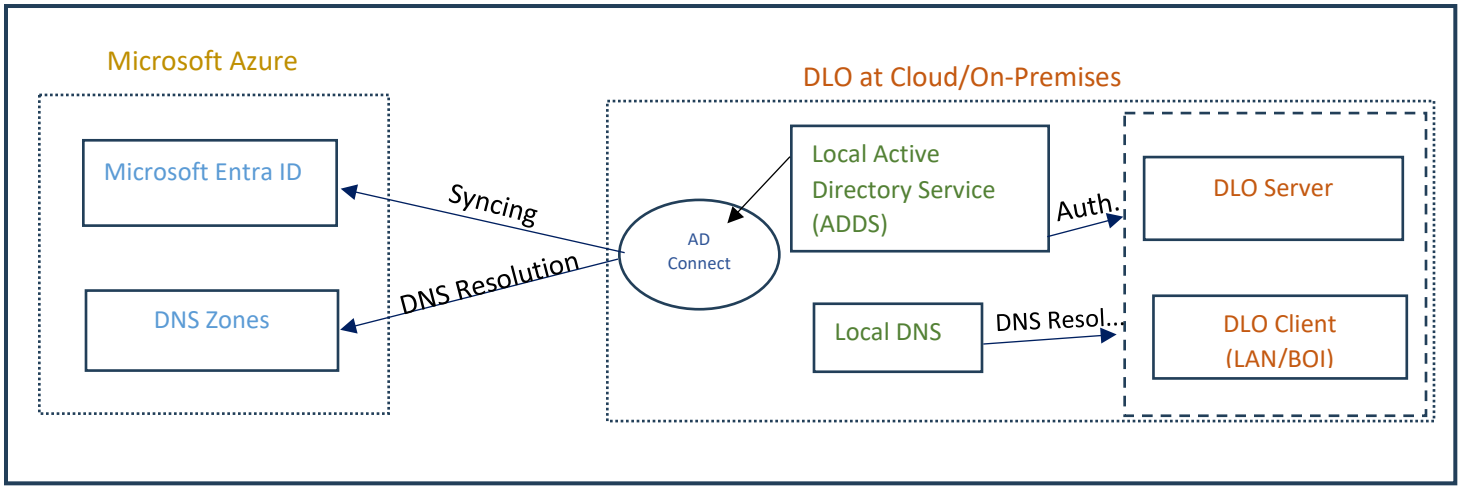
Deployment Type – 2

1. AD Service:

Hybrid identity environment where your on-premises **Active Directory Domain Services (AD DS)** is synchronized with **Microsoft Entra ID (Azure AD)** using **Azure AD Connect**, and **Azure DNS Zones** records are used for domain resolution

2. Domain Joined Machine:

    - Arctera DLO Server machines are On-Premises
    - Arctera DLO Client machines are On-Premises



Deployment-2: Hybrid identity environment

Note:

1. Arctera DLO does not support 'only AD-Joined' configuration. At present, only 'Domain Joined' machines are supported.
2. Exclusive BOI and LAN, both modes are supported by DLO Agent for backup and restore operation.
3. In deployment type-2, the Arctera DLO Webrestore login will be authenticated using local active directory.

For the deployment of Microsoft Azure AD service, consult the Azure documentation. The following steps provide a general high-level overview of the process.

Exclusive Azure Active Directory (AAD) environment:

Step-by-Step Setup

- **Step 1: Create a Microsoft Entra ID (Azure AD) Tenant**

1. Go to the Azure Portal.
2. Search for **"Microsoft Entra ID"**.
3. Click **"Create a tenant"**.
4. Choose **Azure Active Directory**.
5. Fill in:
    - Organization name
    - Initial domain name (e.g., yourorg.onmicrosoft.com)
    - Country/region
6. Click **Review + Create** → **Create**.

- **Step 2: Add a Custom Domain (Optional but Recommended)**

1. In Entra ID, go to **Custom domain names**.
2. Click **+ Add custom domain**.
3. Enter your domain (e.g., yourorg.com).
4. Verify ownership by adding a **TXT record** in your domain registrar's DNS settings.
5. Once verified, set it as **primary domain** if needed.

- **Step 3: Create an Azure DNS Zone**

1. In Azure Portal, search for **"DNS Zones"**.
2. Click **+ Create**.
3. Select your subscription and resource group.

4. Enter your domain name (e.g., yourorg.com).
5. Click **Review + Create** → **Create**.
6. Add **DNS records** as needed (A, CNAME, MX, etc.).

- **Step 4: Deploy Microsoft Entra Domain Services**

1. In Azure Portal, search for **"Microsoft Entra Domain Services"**.
2. Click **+ Create**.
3. Choose:
    - Subscription and resource group
    - DNS domain name (e.g., corp.yourorg.com)
    - Virtual network (create or select an existing one)
4. Configure **IP address range** and **replica set**.
5. Enable **secure LDAP** if needed.
6. Click **Review + Create** → **Create**.

- **Step 5: Link Azure DNS with Entra Domain Services (Optional)**

- If you want to resolve names for your Entra Domain Services domain:
    - Add **A records** in your Azure DNS Zone pointing to the **Domain Services IPs**.
    - Configure **custom DNS servers** in your virtual network to point to the Domain Services IPs.

- **Step 6: Create and Manage Users**

- In **Microsoft Entra ID**, go to **Users** → **+ New user**.
- Assign roles, licenses (e.g., Microsoft 365), and group memberships.

- **Step 7: Join VMs to Entra Domain Services**

- Deploy a VM in the same virtual network.
- Set the VM's DNS to the **Domain Services IPs**.
- Join the VM to the domain (e.g., corp.yourorg.com) using domain credentials.

Hybrid identity environment:

Step-by-Step Setup

- **Step 1: Set Up On-Premises Active Directory (AD DS)**

1. Install **Windows Server** and promote it to a **Domain Controller**.
2. Create a **domain** (e.g., corp.yourorg.com).
3. Add users, groups, and organizational units (OUs) as needed.

- **Step 2: Prepare Azure Environment**

1. Create a **Microsoft Entra ID (Azure AD)** tenant if not already available.
2. Optionally, add and verify your **custom domain** (e.g., yourorg.com) in Entra ID.
3. Create an **Azure DNS Zone** for your domain:
    - Go to **DNS Zones** in Azure Portal.
    - Create a zone for yourorg.com.
    - Add necessary records (A, CNAME, MX, etc.).

- **Step 3: Install and Configure Azure AD Connect**

1. Download **Azure AD Connect** from Microsoft's official site.
2. Install it on a **domain-joined Windows Server** (not a DC, ideally).
3. During setup:
    - Choose **"Express Settings"** for simple sync or **"Custom"** for granular control.
    - Connect to your **on-prem AD DS** and **Microsoft Entra ID**.
    - Select **OU filtering** if needed.
    - Choose **Password Hash Sync** or **Pass-through Authentication**.

- Enable **Hybrid Azure AD Join** if you want devices to be joined to both AD and Entra ID.

- **Step 4: Verify Synchronization**

1. Open **Synchronization Service Manager** on the AD Connect server.
2. Confirm that sync cycles are running successfully.
3. In **Microsoft Entra ID**, verify that users and groups from on-prem AD appear.

- **Step 5: Configure Azure DNS Zones (Optional)**

- If you're using **Azure DNS Zones** for public resolution:
  - Add **A records** for services (e.g., vpn.yourorg.com, mail.yourorg.com).
- If using for **internal resolution**:
  - Use **Azure Private DNS Zones** and link them to your virtual networks.
  - Add **custom DNS servers** in your Azure VNet to point to on-prem DNS or Azure DNS forwarders.

- **Step 6: Test the Setup**

- Log in to Microsoft 365 or Azure using an on-prem synced user.
- Test SSO, password sync, and device join scenarios.
- Use dsregcmd /status on a Windows client to verify hybrid join.
