Veritas™ Desktop and Laptop Option 9.1

Qualification Details with Cloud Service Providers (Microsoft Azure and Amazon Web Services)

Veritas Desktop and Laptop Option: Qualification Details with Cloud Service Providers (Microsoft Azure and Amazon Web Services)

Note: This document is an updated version of the “Veritas Desktop and Laptop Option: Storage in Cloud” document which was last published in April 2017. The document renaming is in response to the Microsoft Azure and Amazon Web Services qualification that was undertaken for the Veritas Desktop and Laptop Option 9.1 release in November 2017.

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.

Veritas Technologies LLC

500 East Middlefield Road

Mountain View, CA 94043

http://www.Veritas.com/

Contents

Introduction

Veritas Desktop and Laptop Option has been qualified with all DLO Server components deployed on cloud, while the DLO Agents remain on premises in the corporate network.

The qualification has been done with the following Cloud Service Providers

- Microsoft Azure
- Amazon Web Services (AWS)

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

Qualification Details for Microsoft Azure

Below are the qualification details for all DLO Server components deployed on Microsoft Azure.

All DLO Server Components deployed on Microsoft Azure

For this qualification all the DLO Server components have been deployed on virtual machines residing on the Microsoft Azure, with the DLO Storage configured on a Microsoft Azure virtual machine (File Server) as a SMB share (file share) and the DLO Agents deployed on premises in the 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, either through a Virtual Private Network (in case of LAN connectivity) or through Backup Over Internet(BOI).

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.

Qualification Details for Amazon Web Services (AWS)

Below are the qualification details for the DLO components on AWS

- All DLO Server components on AWS
- DLO Storage on AWS

All DLO Server Components deployed on AWS

For this qualification, all DLO Server components have been deployed on virtual machines in AWS EC2 instance, the Storage Gateway on premises, with the DLO Agents deployed on premises in the corporate local network and the DLO Storage configured on Amazon S3.

DLO Agents communicate to the DLO Storage through the Storage Gateway. Organizations where the Storage Gateway is deployed on premises, the communication occurs 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 BOI. DLO Agents communicate to the DLO Server components through VPN tunnel established between the LAN and the Virtual Private Cloud (VPC) network.

Note: DLO Storage can also be configured as a SMB share (File Share) on an AWS EC2 instance (File Server).

DLO Storage Component on AWS

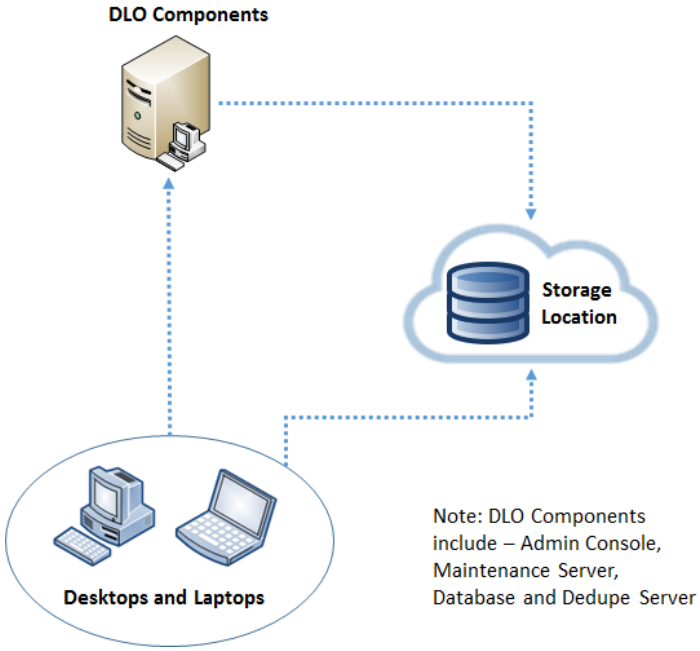
For this qualification, all DLO Server components and the DLO Agents are deployed on premises in the local corporate network, with the DLO Storage that includes the Dedupe Storage configured on AWS Amazon S3 storage.

You can choose to run AWS Storage Gateway either on-premises, as a virtual machine (VM) appliance, or 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 BOI. It is recommended to have AWS Storage Gateway deployed on premises to experience seamless data transfers compared to having it deployed in AWS to avoid perceived latency due to internet connectivity speeds.

Details for deploying DLO Storage on Amazon S3

The following sections provides the details of the qualification and steps for deploying the DLO storage components using AWS Storage Gateway.

Veritas Desktop and Laptop Option has been qualified to write data to the Amazon Storage Gateway, which is an AWS service that provides cloud based storage to an on premise software appliance.



AWS Storage Gateway Deployment

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 to the AWS cloud for scalable and cost-effective storage.

The Gateway-Cached Volume configuration supported by AWS Gateway has been considered and discussed in this document. In this configuration, the primary data is stored in Amazon Simple Storage Service (Amazon S3) while the frequently accessed data is retained locally on premise. This configuration provides low-latency access to your frequently accessed data, minimizes the need to scale your storage on-premises and provides substantial cost savings on primary storage.

Requirements

Refer the link Requirements for information on the Supported Hypervisors, Supported iSCSI Initiators, Hardware, Storage and Network before deploying AWS Storage Gateway.

Note: The above requirements are common for both the deployments.

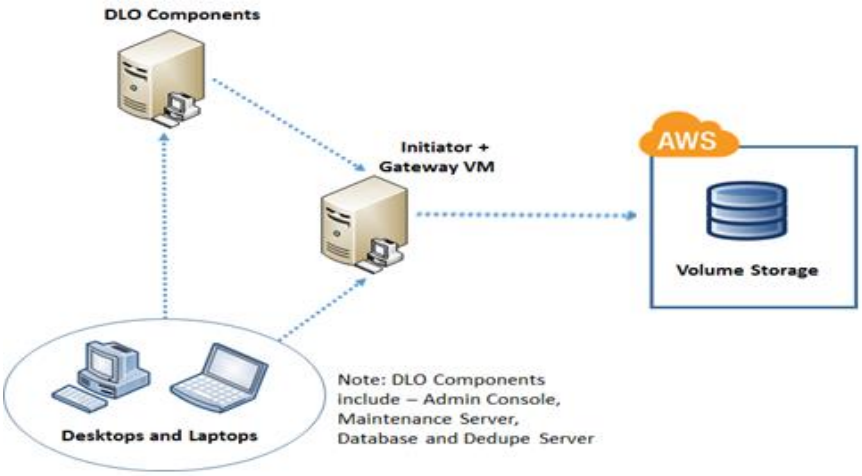
Deployment Configurations

You can choose to run AWS Storage Gateway either on-premises, as a virtual machine (VM) appliance, or in AWS, as an Amazon Elastic Compute Cloud (EC2) instance. Two possible deployments of AWS Storage Gateway have been discussed below.

Deployment 1 - Architecture

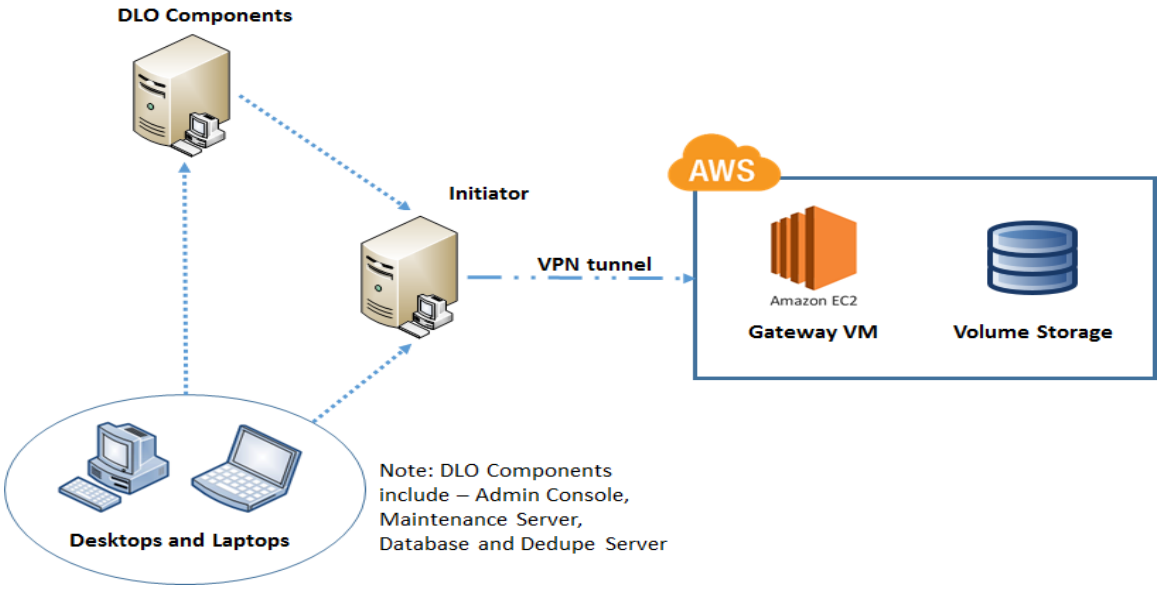
You can deploy your gateway on a host in your on-premises data center. The hypervisors that AWS Storage Gateway supports is mentioned in the Requirements link.

Note: The on premises deployment considered in this document is in VMware ESXi Hypervisor.



Deployment 2 - Architecture

You can deploy your gateway on an Amazon EC2 instance to provision iSCSI storage volumes on AWS. AWS Storage Gateway provides an Amazon Machine Image (AMI) that contains the gateway VM image.



Recommended Deployment

It is recommended to have AWS Storage Gateway deployed on premises (Deployment 1) to experience seamless data transfers compared to having it deployed in AWS (Deployment 2) to avoid perceived latency due to internet connectivity speeds.

Note: Deployment 2 requires establishment of VPN connection between iSCSI initiator and AWS VPC network.

For more information on the deployment of Gateway Cached Volume refer Gateway-Cached Volume Architecture, this will give a detailed explanation of the Gateway cached Volume architecture and the two different deployments in it.

Deployment 1: Deploying on-premises AWS Storage Gateway

Introduction

This section contains details about the deployment of an on-premises AWS gateway cached volume as a VM appliance in VMWare ESXi server.

Pre-requisites

Refer Configuring a VMware ESXi Host for AWS Storage Gateway for basic information on setting up the virtualization host before deploying the gateway.

Deployment Steps

Refer Deploy a VM and Activate the Gateway for deploying on-premises Gateway Cached Volume. This covers activation of the hosted VM image, further configuration with respect to adding local disks (cache and buffer), storage volumes in AWS and finally connecting to these volumes from an iSCSI Initiator.

Note: You can connect to AWS storage volumes that is, iSCSI targets, directly by providing the IP address of the Storage gateway while connecting from iSCSI initiators. AWS storage gateway securely transfers the data to AWS over SSL and securely stores the data in Amazon S3. You can also establish VPN tunnel between iSCSI initiator and AWS VPC network and connect to these iSCSI targets. VPN connectivity for deployment1 is not mandatory.

Refer to the link Troubleshooting On-Premises Gateway Issues for issues that you might encounter while working on-premises gateways.

Having deployed the AWS storage gateway, refer to the section on DLO Configuration for creating DLO storage locations and testing the setup.

Note: The DLO Configuration steps are the same for both the deployments.

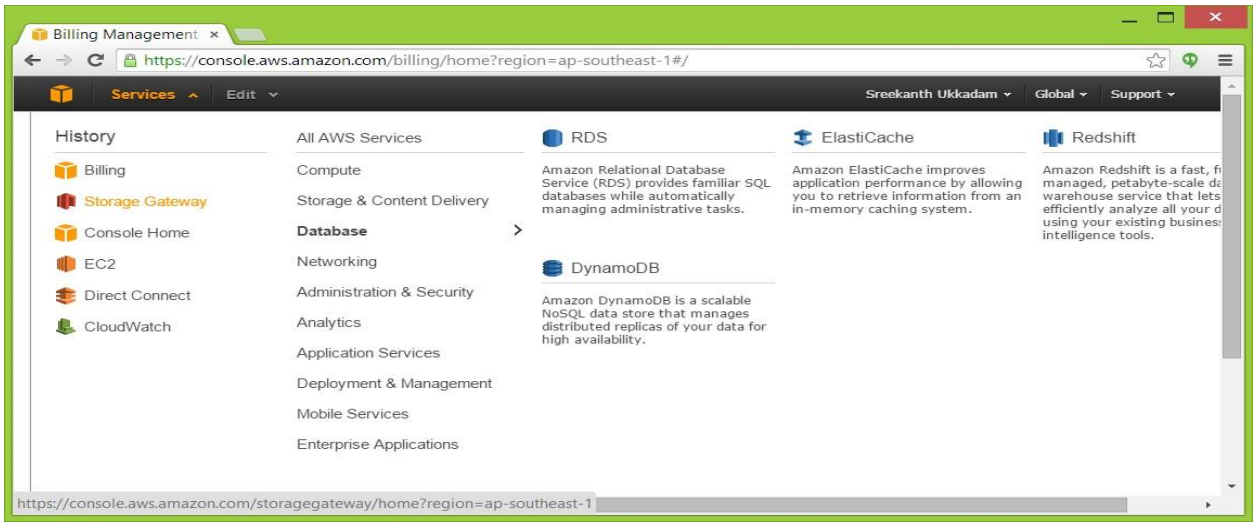
Deployment 2: Deploying new gateway on the EC2 instance

Introduction

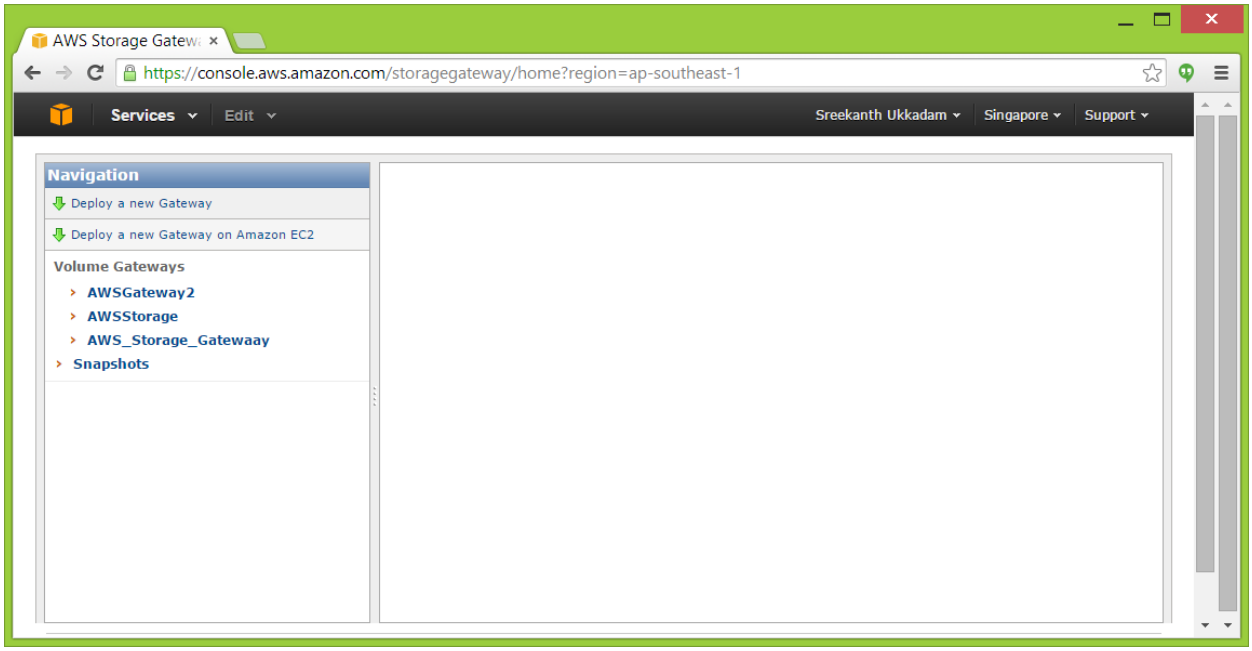
This section contains details about deploying Gateway Cached Volume as an EC2 instance. AWS Storage Gateway provides an Amazon Machine Image (AMI) that contains the gateway VM image.

Deployment Steps

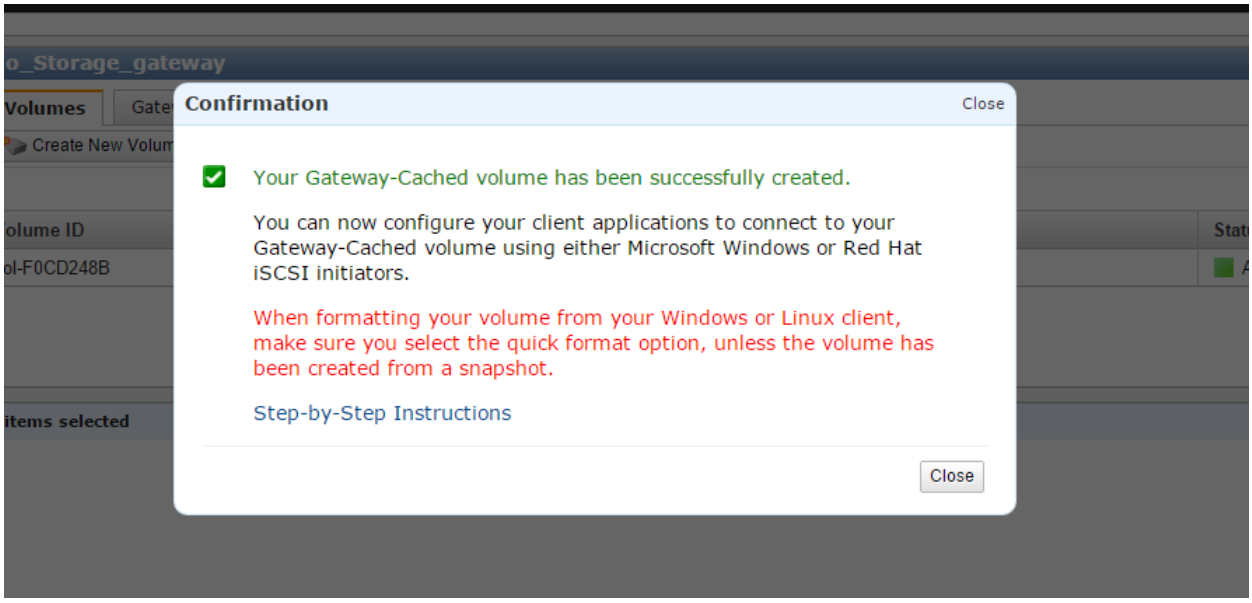
1. Open the **AWS management Console**, click on the **Services** and select **Storage Gateway** option.



2. Select the second option deploy a new Gateway on the Amazon EC2.



3. Refer Amazon EC2 Gateway for activation of gateway and further deployment steps.
4. Once the deployment is done, a confirmation message of successful creation of Gateway Cached Volume will be displayed as below.



5. After the creation of storage gateway, next we mount the storage volumes created in AWS from an on-premises machine configured as iSCSI Initiator.
6. Refer to the below pre-requisites before configuring an iSCSI Initiator.
   - Have a VPN client installed in the initiator to connect to a VPN server installed in VPC network.
   - Ensure that VPN connectivity is established between on-premises iSCSI Initiator and VPC network.
7. Refer Connect Your Volumes to Your Windows Client to configure and mount the required storage volumes via the iSCSI Initiator.

Refer to the link Troubleshooting Amazon EC2 Gateway Issues for issues that you might encounter working with your gateway deployed on Amazon EC2.

Having deployed the AWS storage gateway, refer to the section on DLO Configuration for creating DLO storage locations and testing the setup.

Note: The DLO Configuration steps are the same for both the deployments.

DLO Configuration

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

1. Create the required DLO storage locations by providing the path of locally mounted storage volumes (iSCSI Initiator)
2. Write/Read data to and from these volumes by backing up and restoring the data from DLO Agent. Both of the parts have been discussed in detail below.

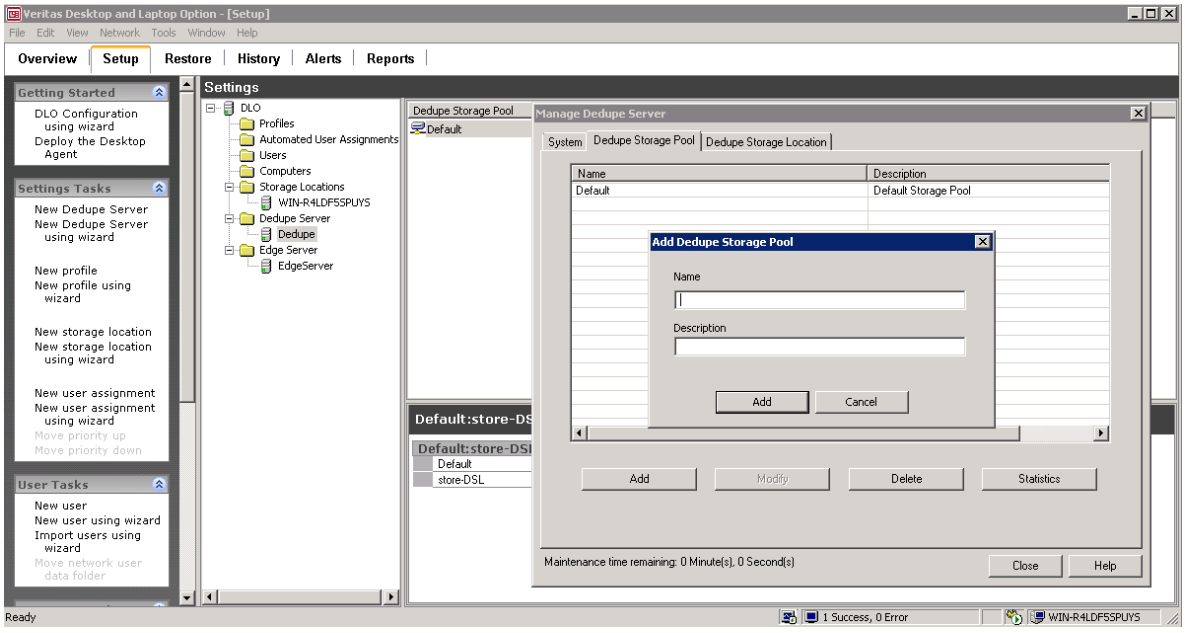
Creating DLO Storage Locations in the mounted volumes

Pre-requisites

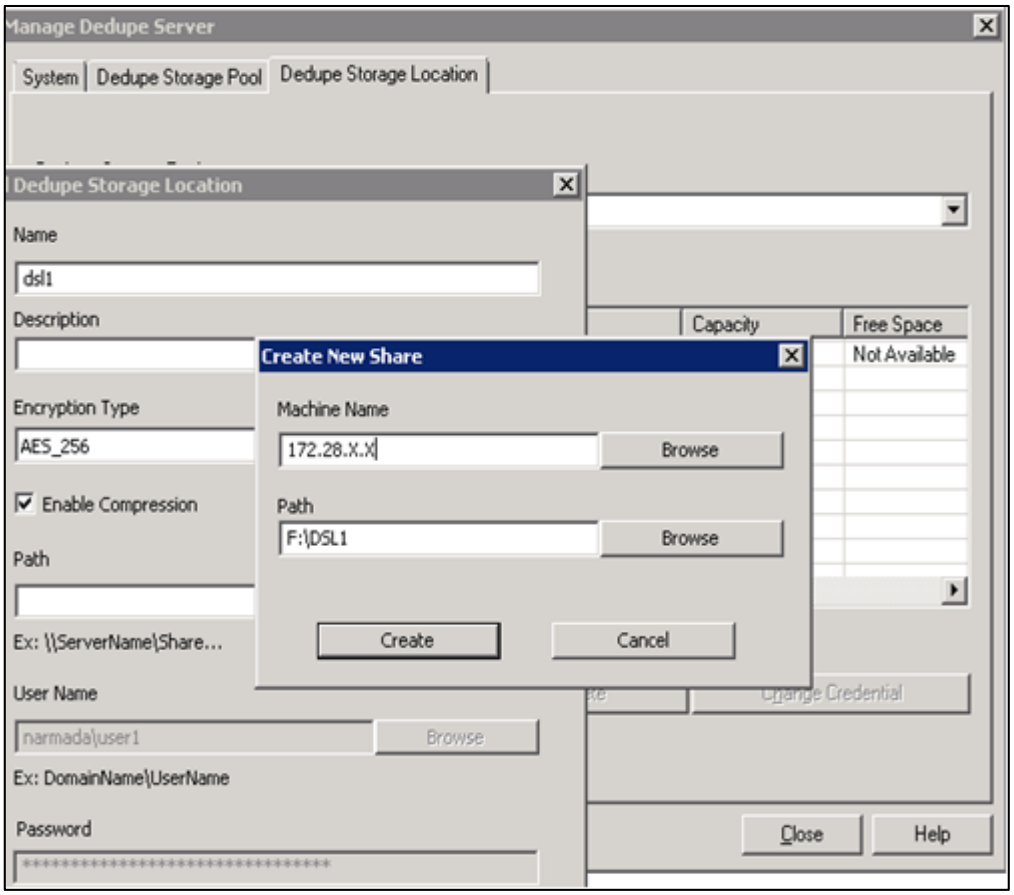
- Test the Gateway Cached Volume setup. Refer Test the Setup for a Gateway-Cached Volume to confirm whether the created Gateway Cached Volume setup is proper.
- Make sure all the DLO components are installed prior to creating these storage locations.

Creating a Dedupe Storage Location

1. On the **DLO Administration Console**, right-click the Dedupe Server name and select **Manage**.
2. In the **Manage Dedupe Server** wizard, click the **Dedupe Storage Pool** tab and click **Add** as shown in the figure below.



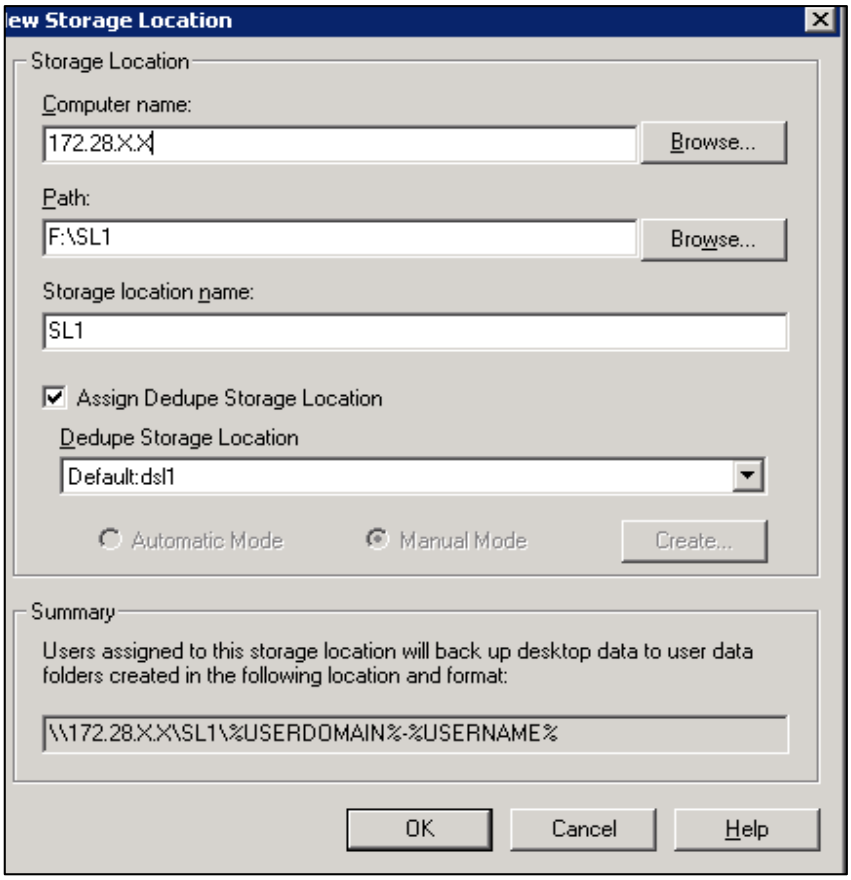
3. Now, click **Dedupe Storage Location tab** and select the created **Dedupe Storage Pool** from the list and click **Add** to add a **Dedupe Storage Location** to the pool.
4. In the **Dedupe Storage Location wizard,** create a new share by clicking **'+' button** next to the path field.
5. In the **Create New Share** wizard, either browse and select the machine name or manually enter the hostname/IP of the **iSCSI Initiator Client** machine. In the **path** field enter a **DSL** path to be created and click **Create.**
6. Provide a relevant domain user name and password and click **OK** to create a **DSL**.



Creating DLO Storage Location

1. On the **DLO Administration Console**, in the **Settings** pane, right-click **Storage locations** and select **New Storage Location**.
2. In the **New Storage Location** wizard, browse and select the Computer (**iSCSI Initiator**), provide the path of the storage location (you can provide a new path or any existing shared path in the iSCSI local volume), **storage location name**, check the **Assign Dedupe Storage Location** option.

3. Here **Dedupe Storage Location** can be assigned either automatically or manually. Selecting **Automatic Mode** will create a SL in the same share as the DSL. Selecting **Manual Mode** will allow one to associate a required DSL from the drop down to this SL.
4. Click **OK** to create a Storage Location.



Testing the setup through Backup and Restore from DLO Agent

Pre-requisites

- Configure DSL, SL, Profile, AUA settings in the DLO Administration Console.
- Install the DLO Agent prior to performing read/write tasks to the designated DLO Storage Locations.

Steps

1. Launch the DLO Agent and verify the backup of few files (as present in Backup Selection).
2. Restore them from DLO Agent and verify if all the backed up files have been successfully restored.