Symantec™ Desktop and Laptop Option

Symantec DLO's Storage in Cloud

(Amazon Web Services)

Symantec

Disclaimer

The information contained in this publication is subject to change without notice. Symantec Corporation makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Symantec Corporation shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual.

Legal Notice

Copyright © 2015 Symantec Corporation. All rights reserved.

Symantec, Backup Exec, NetBackup, the Symantec Logo, and Desktop and Laptop Option are trademarks or registered trademarks of Symantec Software Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

Symantec Software Corporation

350 Ellis Street
Mountain View, CA 94043
www.symantec.com

Third-Party Legal Notices

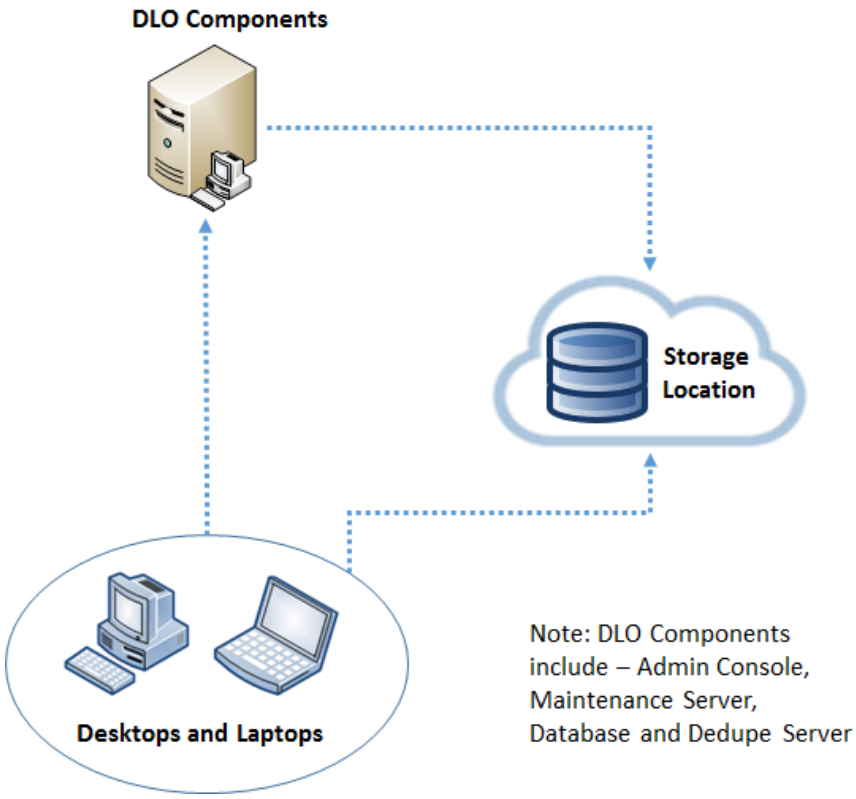
Certain third-party software may be distributed, embedded, or bundled with this Symantec product or recommended for use in connection with its installation and use. Such third-party software is separately licensed by its copyright holder. Licenses that govern the use of the third party software included in the Symantec product and proprietary notices of the copyright holders are listed in the Administrators Guide

Contents

1. Introduction 4
2. AWS Storage Gateway Deployment 5
   2.1 Introduction 5
   2.2 Requirements 5
   2.3 Deployment Configurations 5
      2.3.1 Deployment 1 - Architecture 5
      2.3.2 Deployment 2 - Architecture 6
      2.3.3 Recommended Deployment 6
3. Deployment 1: Deploying on-premises AWS Storage Gateway 7
   3.1 Introduction 7
   3.2 Pre-requisites 7
   3.3 Deployment Steps 7
4. Deployment 2: Deploying new gateway on the EC2 instance 7
   4.1 Introduction 7
   4.2 Deployment Steps 8
5. DLO Configuration 9
   5.1 Creating DLO Storage Locations in the mounted volumes: 10
      5.1.1 Pre-requisites 10
      5.1.2 Creating a Dedupe Storage Location 10
      5.1.3 Creating a DLO Storage Location 11
   5.2 Testing the setup through Backup and Restore from DLO Agent 11
      5.2.1 Pre-requisites 11
      5.2.2 Steps 12

1. Introduction

Symantec DLO 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. So far, the DLO components have all been deployed on premise, but with this recent qualification, the storage components- DLO Storage and Dedupe Storage of DLO 7.6 and above can be hosted on the cloud as illustrated below. The other DLO components will still remain on premise on the corporate network.



This document provides the details of this recent qualification and provides the steps of deploying the storage components using AWS Storage Gateway.

2. AWS Storage Gateway Deployment

2.1 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 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.

2.2 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.

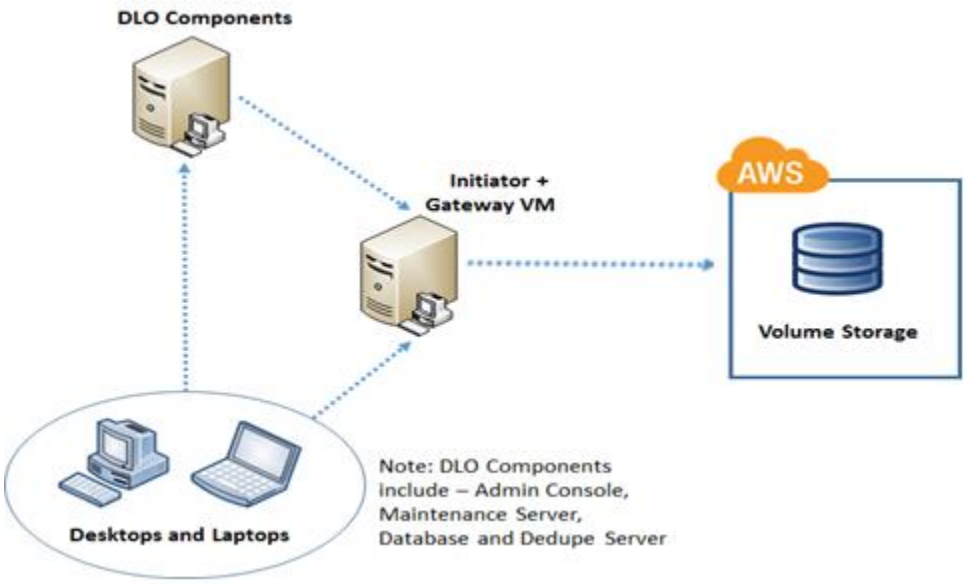
2.3 Deployment Configurations

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.

2.3.1 Deployment 1 - Architecture

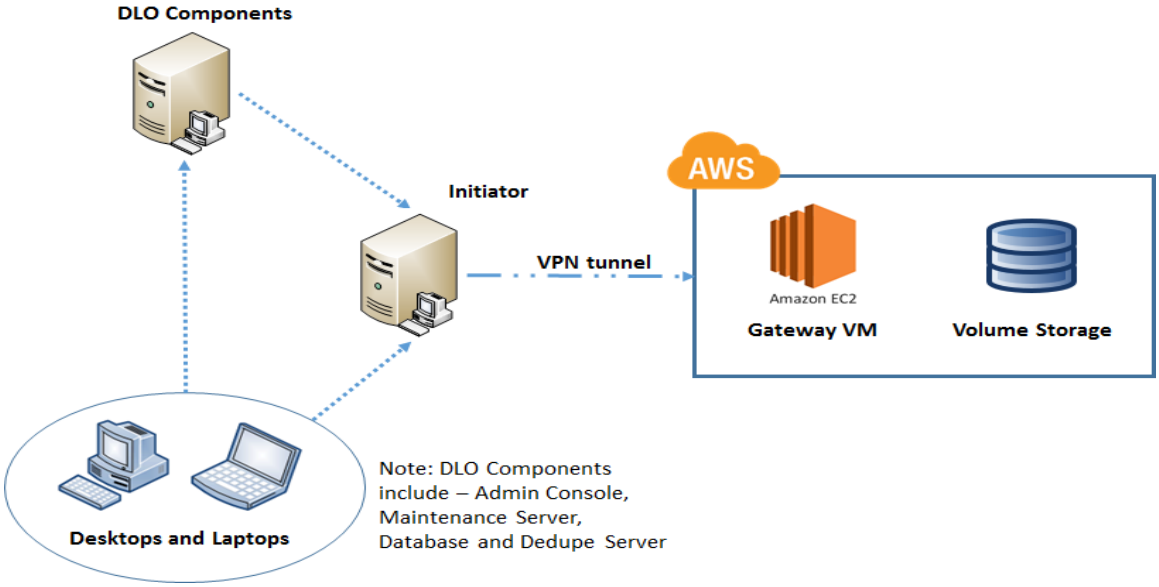
You can deploy your gateway on a host in your on-premises data center. The hypervisors that AWS Storage Gateway supports is mentioned in the Requirements link.

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



2.3.2 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.



2.3.3 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: Only deployment 2 requires establishment of VPN connection between iSCSI initiator and AWS VPC network whereas VPN connectivity for deployment1 is optional.

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.

3. Deployment 1: Deploying on-premises AWS Storage Gateway

3.1 Introduction

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

3.2 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.

3.3 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.

4. Deployment 2: Deploying new gateway on the EC2 instance

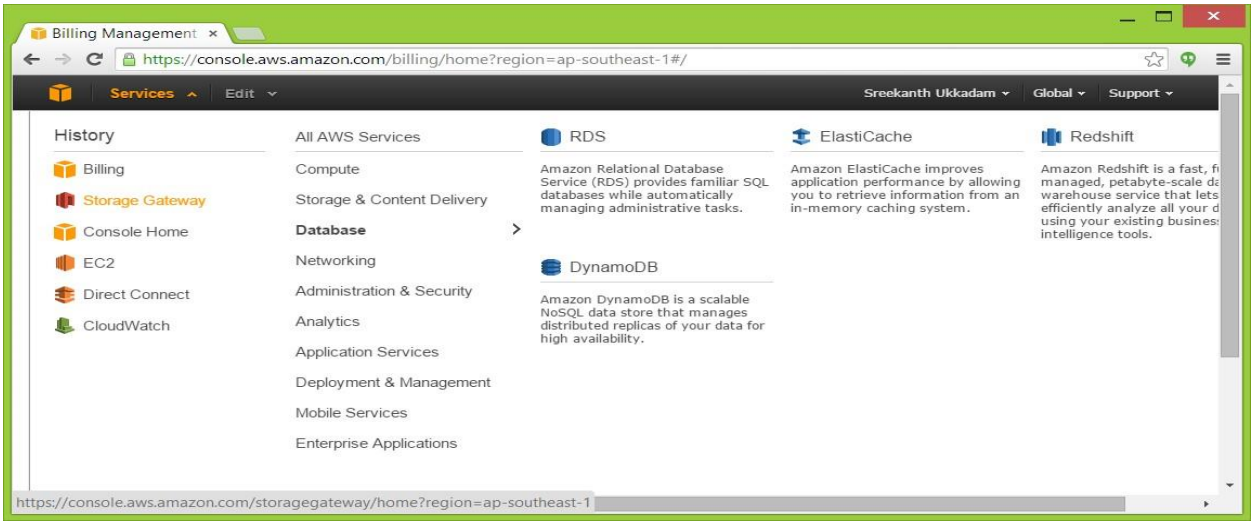
4.1 Introduction

This section contains details about deploying Gateway Cached Volume as an EC2 instance. AWS

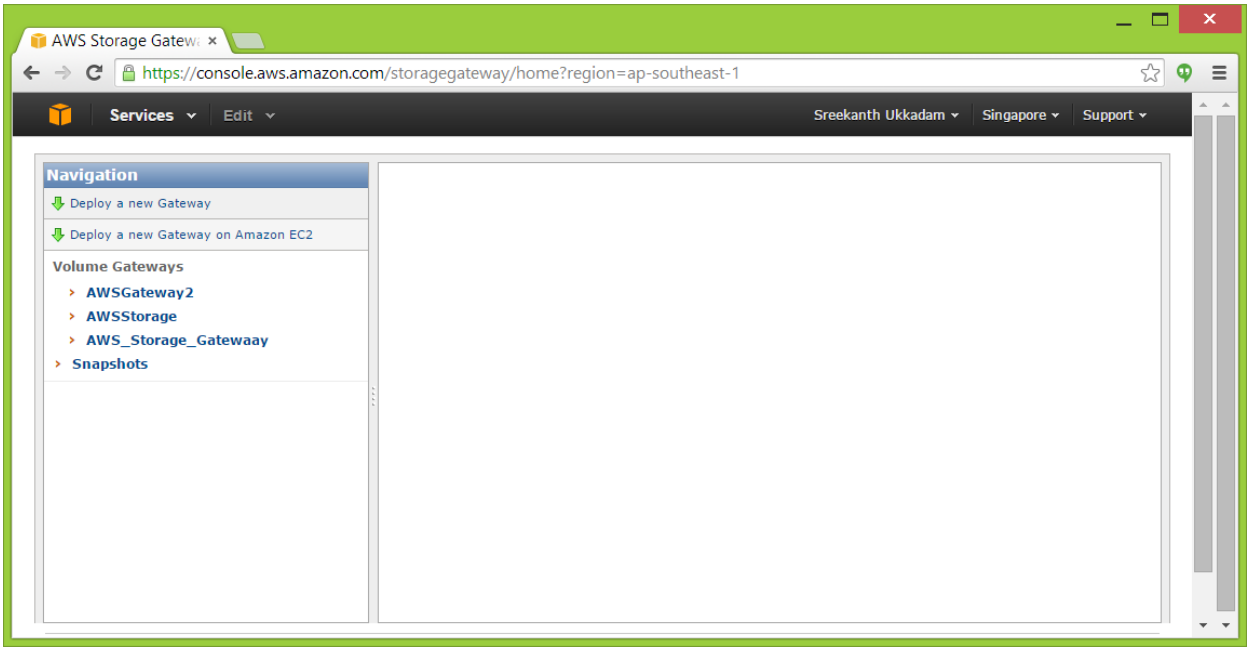
Storage Gateway provides an Amazon Machine Image (AMI) that contains the gateway VM image.

4.2 Deployment Steps

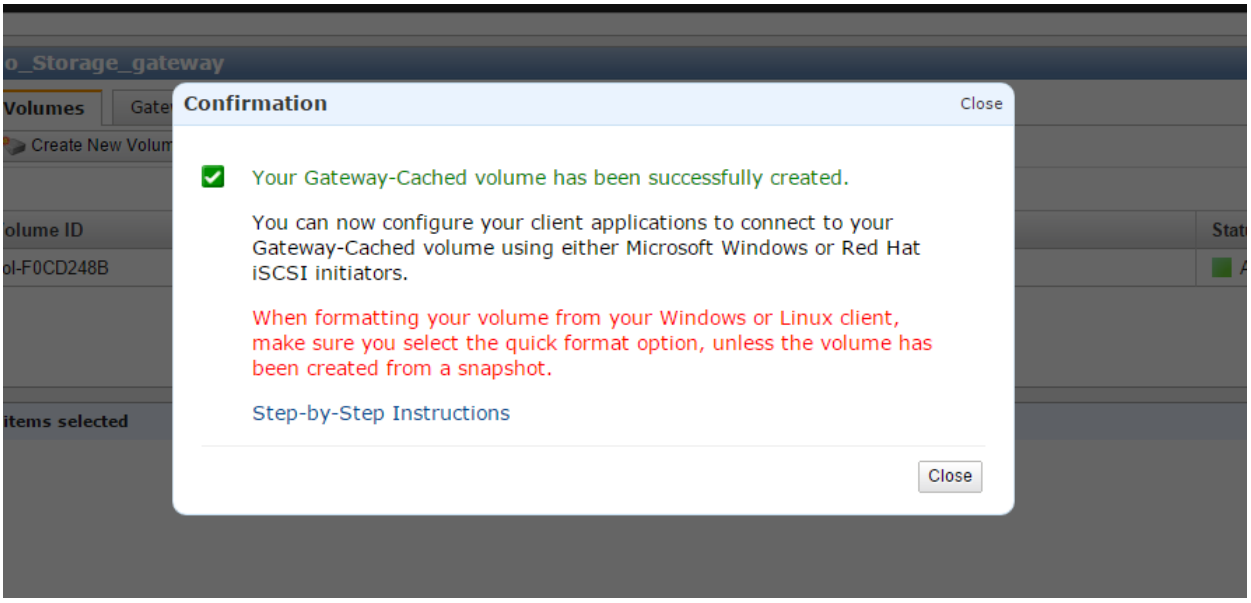
1. Open the **AWS management Console**, click on the **Services** and select **Storage Gateway** option.



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.

5. 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.

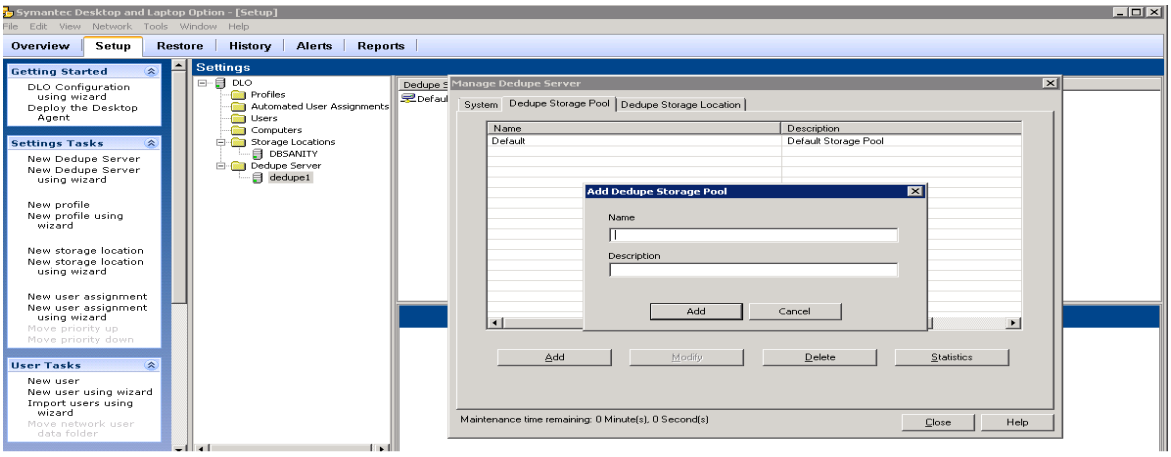
5.1 Creating DLO Storage Locations in the mounted volumes:

5.1.1 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.

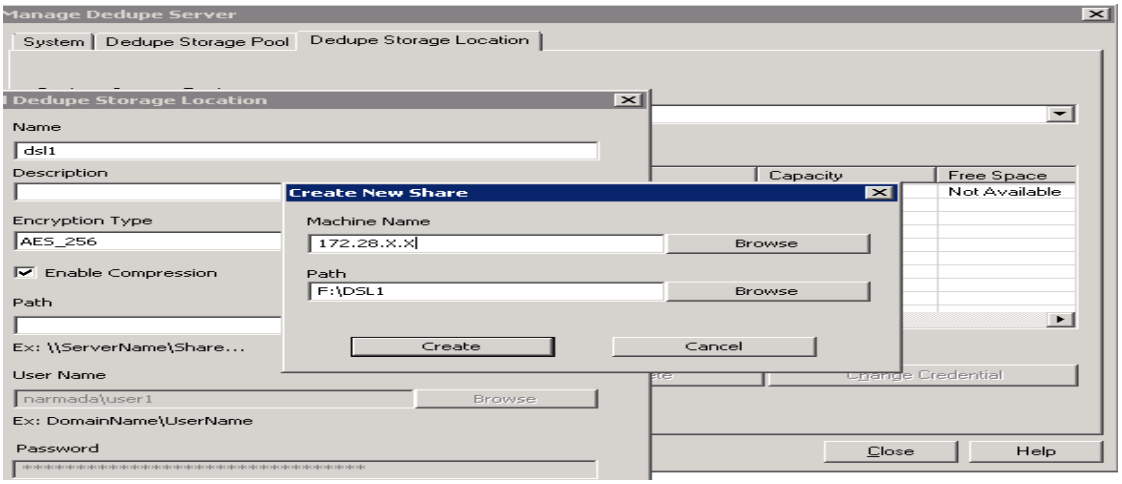
5.1.2 Creating a Dedupe Storage Location

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



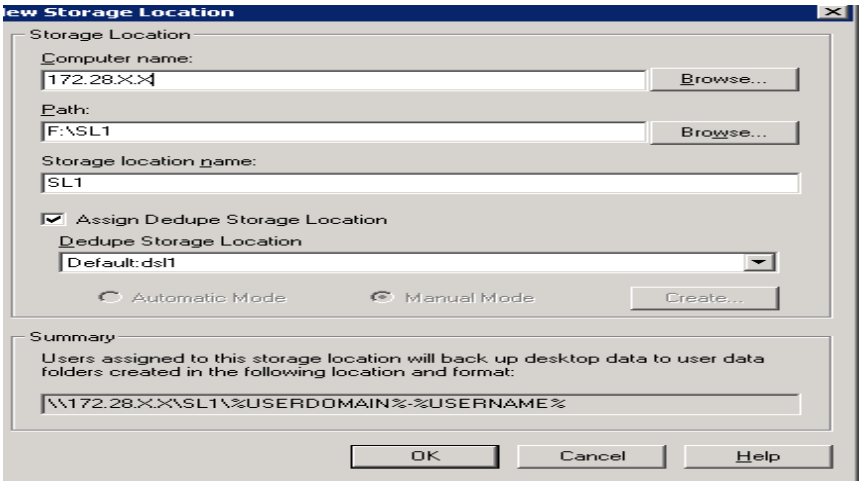
3. Now, click **Dedupe Storage Location tab** and select the created **Dedupe Storage Pool** from the list and click **Add** to add a **Dedupe Storage Location** to the pool.
4. In the **Dedupe Storage Location wizard,** create a new share by clicking **'+' button** next to the path field.
5. In the **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.**



5.1.3 Creating a 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 either assigned 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**.



5.2 Testing the setup through Backup and Restore from DLO Agent

5.2.1 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.

5.2.2 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.