Veritas™ Desktop and Laptop Option 9.5 Deployment on Microsoft Azure Cloud

VERITAS

CONTENTS

Veritas Desktop and Laptop Option: Deployment on Microsoft Azure 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 9.5

Legal Notice

Copyright (c) 2021 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. Introduction

Veritas Desktop and Laptop option has been qualified with all DLO server components deployed on both Azure and AWS cloud, while DLO agent remain on the on premises corporate network.

2. Deployment of all DLO Server components on 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.

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

2.2 Steps for deploying all DLO Server components on Azure

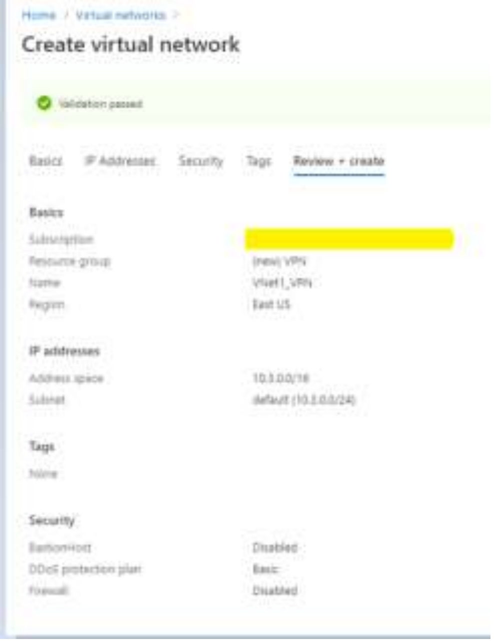
Below steps are followed for deploying all DLO Server components on Azure. All of below steps are detailed in the following sections.

- 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

2.2.1 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



Create virtual network

Validation passed

Basics

Subscription	[redacted]
Resource group	(new) VPN
Name	VNet1_VPN
Region	East US

IP addresses

Address space	10.1.0.0/16
Subnet	default (10.1.0.0/24)

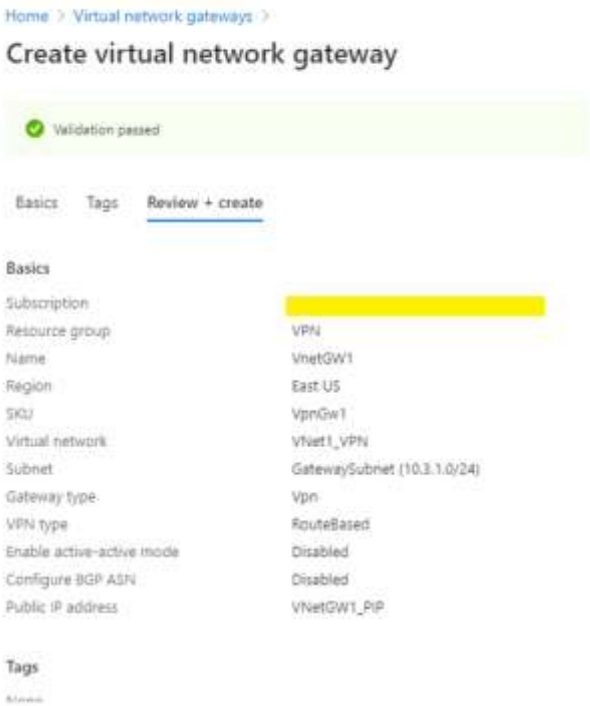
Tags

None

Security

BastionHost	Disabled
DDoS protection plan	Basic
Firewall	Disabled

b. Create a Virtual Network Gateway



Home > Virtual network gateways >

Create virtual network gateway

Validation passed

Basics Tags **Review + create**

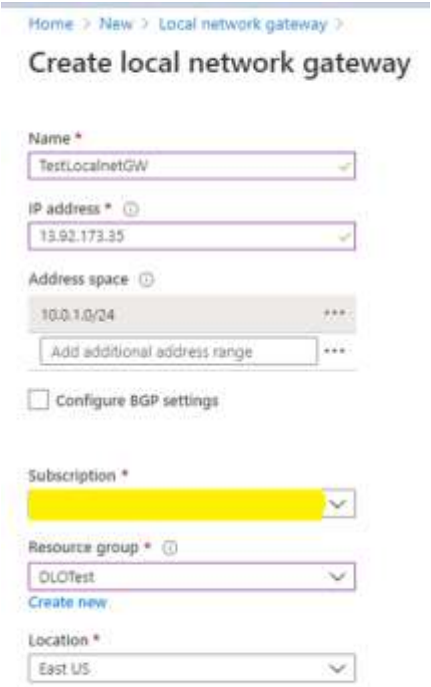
Basics

Subscription	[redacted]
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

None

c. Create a Local Network Gateway



Home > New > Local network gateway >

Create local network gateway

Name *
TestLocalnetGW

IP address *
13.92.173.35

Address space
10.0.1.0/24
Add additional address range

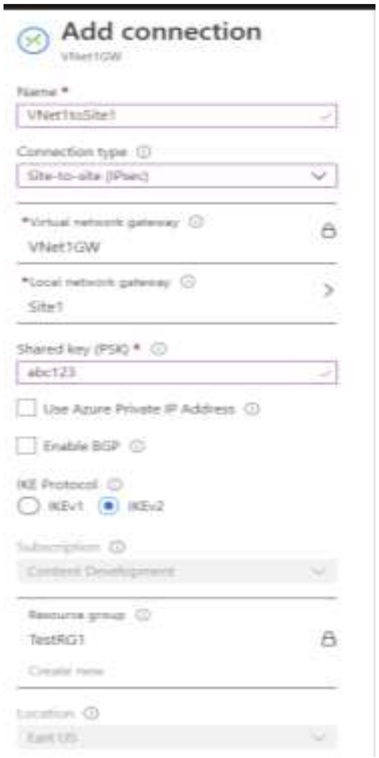
□ Configure BGP settings

Subscription *
[redacted]

Resource group *
DLOTest
Create new

Location *
East US

d. Create a Connection:



Add connection
VNet1GW

Name *
VNet1toSite1

Connection type
Site-to-site (IPsec)

*Virtual network gateway
VNet1GW

*Local network gateway
Site1

Shared key (PSK) *
abc123

□ Use Azure Private IP Address

□ Enable BGP

IKE Protocol
○ IKEv1 ● IKEv2

Subscription
Content Development

Resource group
TestRG1
Create new

Location
East US

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

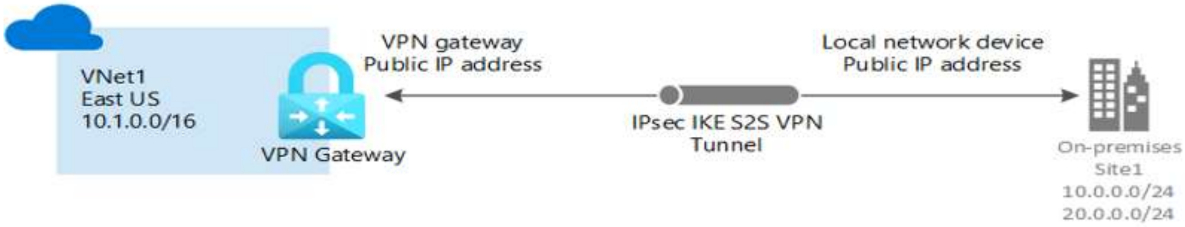
Once the connection between Cloud network and On-Premises network is established, download the configuration file from the Azure Portal and share it to the On-Premises device manager. It is required for enabling the created Virtual network for site-to-site connection.

f. Creating Virtual Machines

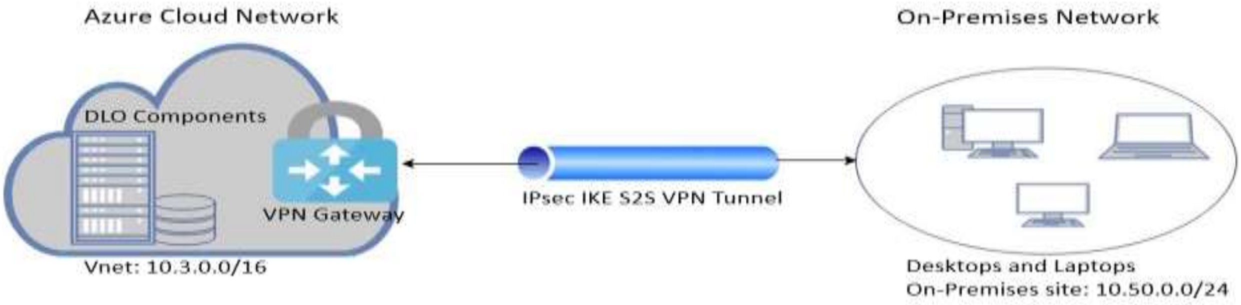
AD DS can exist either on cloud network or On-Premises network. And all DLO components can be installed on one cloud Virtual Machine or multiple Virtual Machines by distributing the DLO components over different servers on cloud. Create both the VM's in same virtual network (created in the previous step)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



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



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

> DLO components Include: DLO Admin Console, Maintenance server, Database and Dedupe server, Edge and IO Server

2.2.2 Configuring Azure disk storage

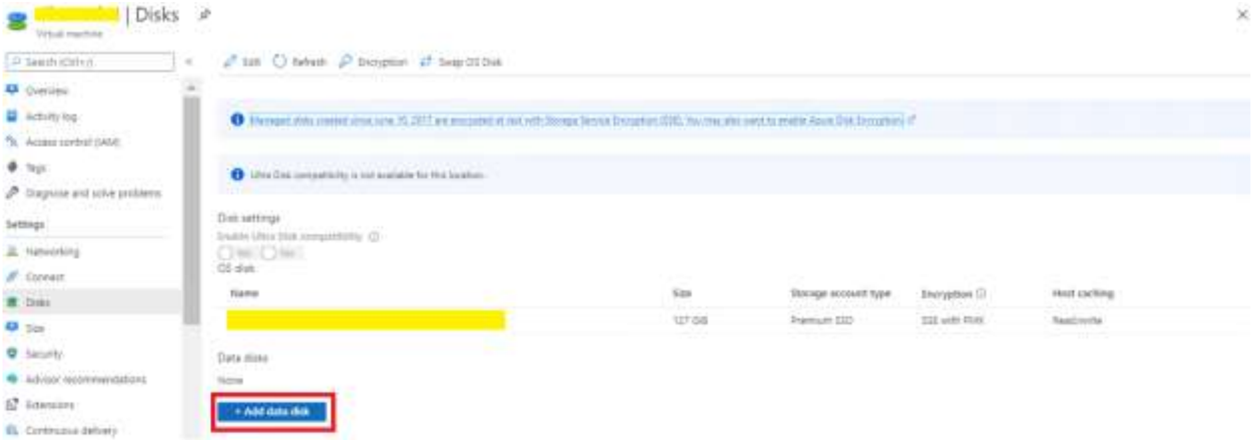
Microsoft Azure cloud offers several types of scalable and with High-Availability storage. Azure offers two types of Storage Accounts, five types of storage, four levels of redundancy and three tiers for storing the data in cloud.

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.



[redacted] | Disks

Virtual machine

Search (Ctrl+/)

Managed disks created since June 10, 2017 are encrypted at rest with Storage Service Encryption (SSE). You may also want to enable Azure Disk Encryption

Ultra Disk compatibility is not available for this location.

Disk settings

Enable Ultra Disk compatibility ⓘ

○ Yes ○ No

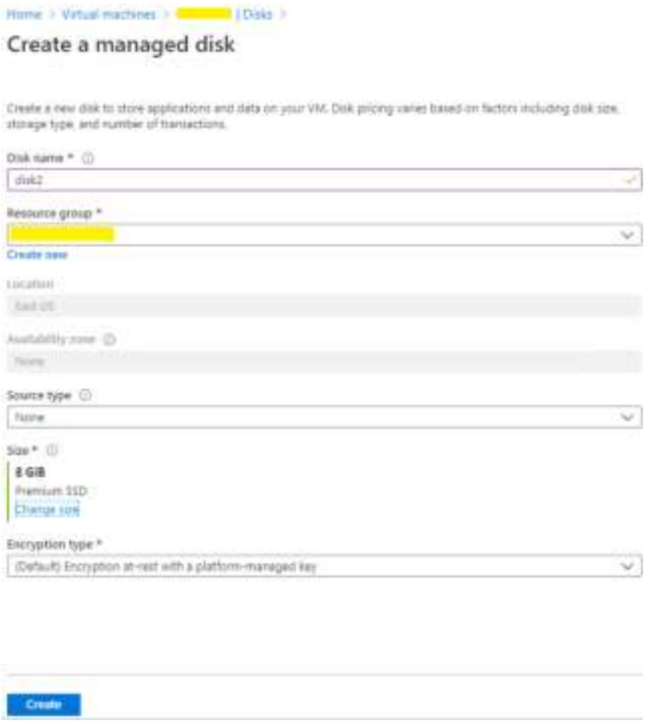
OS disk

Name	Size	Storage account type	Encryption ⓘ	Host caching
[redacted]	127 GiB	Premium SSD	SSE with PMK	ReadWrite

Data disks

None

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



Create a managed disk

Create a new disk to store applications and data on your VM. Disk pricing varies based on factors including disk size, storage type, and number of transactions.

Disk name * ⓘ
disk2

Resource group *
[redacted]

Location
East US

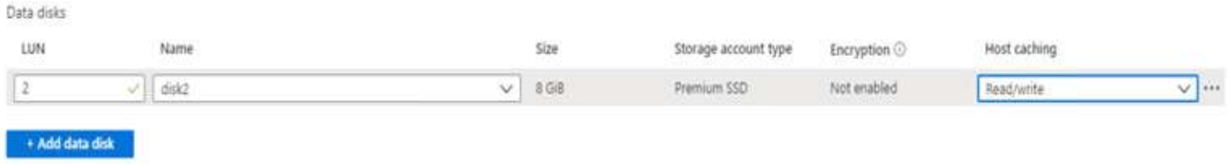
Availability zone ⓘ
None

Source type ⓘ
None

Size * ⓘ
8 GiB
Premium SSD

Encryption type *
(Default) Encryption at-rest with a platform-managed key

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	8 GiB	Premium SSD	Not enabled	Read/write

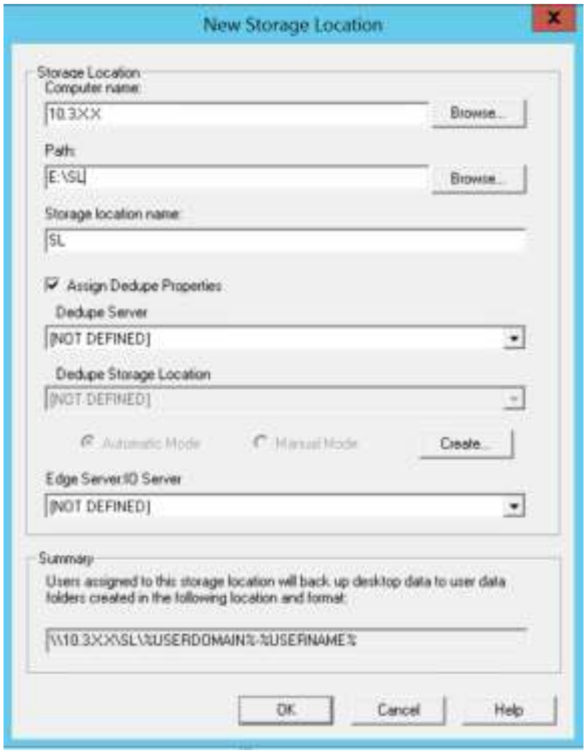
- To know more about the Azure storage types for when to use which types of storage and their services, refer Azure Storage types
- For more information about creating a storage account suitable for configuration, refer Storage Account Creation

2.2.3 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.

2.2.4 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.



New Storage Location

Storage Location

Computer name: 10.3XX

Path: E:\SL

Storage location name: SL

☑ Assign Dedupe Properties

Dedupe Server: [NOT DEFINED]

Dedupe Storage Location: [NOT DEFINED]

● Automatic Mode ○ Manual Mode

Edge Server/IO Server: [NOT DEFINED]

Summary

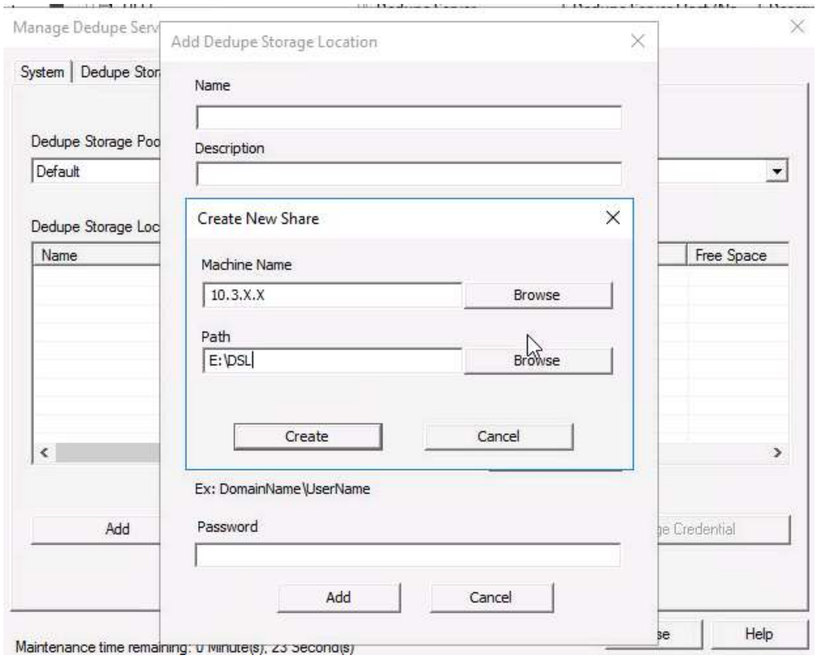
Users assigned to this storage location will back up desktop data to user data folders created in the following location and format:

\\10.3XX\SL\%USERDOMAIN%-%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

2.2.5 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.



Dedupe Storage Poo: Default

Machine Name: 10.3.X.X

Path: E:\DSL

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

2.2.6 Testing the Configured environment through Backup and Restore

1. 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.
2. Restore the backed up files from DLO Agent and verify whether the restoration of all files along with their revisions is successfully.