Veritas™ Desktop and Laptop Option 9.0

Best Practices

VERITAS

Veritas Desktop and Laptop Option: Best Practices

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 9.0

Legal Notice

Veritas Technologies LLC

500 East Middlefield Road

Mountain View, CA 94043

http://www.Veritas.com/

Contents

Introduction

The Veritas Desktop and Laptop Option (DLO) is an easy to use application which provides automated file protection for desktops and laptops (collectively referred to as end-points). Protection is provided regardless of whether the computer is connected to the network (corporate or public) or offline.

Veritas DLO provides continuous, non-intrusive backup of files in both, the corporate and public networks. When the desktop is not connected to the corporate network, files are backed up using the available internet connection. In case there is no available internet connection, files are backed up to a user data folder on the desktop. When the computer reconnects to the network, files are backed up from the local desktop user data folder to the designated network user data folder.

This Best Practices Guide summarizes Veritas's recommendations for planning and deploying Veritas DLO. For detailed information on using DLO, refer to the *Veritas Desktop and Laptop Option Administrator's Guide* available at https://www.veritas.com/support/en_US/article.000116797

To take full advantage of all the benefits that the application can bring to your organization, Veritas recommends that you perform the following tasks before implementing DLO:

1. Determine the end-point backup requirements.
2. Determine the most effective hardware configuration and storage requirements based on the size of your enterprise, the current network environment, IT resources, and backup requirements as well as the needs of the end users.
3. Create Profiles to meet the different needs of particular user subgroups. For example, mobile users who back up their laptops or computers through internet connections usually have different needs than their colleagues on LAN-connected workstations.
4. Roll out the Desktop Agents gradually. A gradual rollout normalizes the impact of the first backup over a greater period, while providing an opportunity to identify and resolve any issues that arise.

Consider the following for effective DLO usage:

1. Network capacity
2. Number of users, and their mode of connectivity to the corporate network
3. Frequency of backup
4. Backup selection
5. End user privileges on the Agent

DLO uses a policy-based configuration mechanism called a Profile to manage backups for groups of similar users. Desktop and Laptop users are assigned to a Profile in which the DLO administrator grants or restricts user rights to control data protection for an end-point. DLO provides default Profiles that can be customized to meet the needs of various user groups.

The best practices provided in the following sections will ensure smooth operations when using Veritas DLO:

- Determining Deployment Topology
- Determining Hardware Requirements
- Determining Software Requirements

Determining Deployment Topology

To arrive at a deployment topology, the following factors must be considered:

1. Total number of sites (Data Centers, Head Quarters, Branch Offices, etc.)
2. Total number of end-points in each site and physical location of the Agents in relation to the servers
3. Connectivity of the end-points (LAN, WAN, Link Speed, and so on.)

Different types of topologies

Depending on the above factors, we can deduce the following topologies.

1. Single Site with Single Administration Server
2. Single Site with Multiple Administration Server
3. Multiple Sites with Centralized Administration Server
4. Multiple Sites with Independent Administration Server

Single Site with Single Administration Server

This topology is applicable when 'all or most of the end-points' and 'DLO Servers' can be co-located in-terms of high speed connectivity between them, preferably in a LAN.

Single Site Administration and Storage

Administration Server + Dedupe Server + DLO and Dedupe Database+ Dedupe Storage Location + DLO Storage Location + Maintenance Server+ Edge Server+ IO Servers(s)
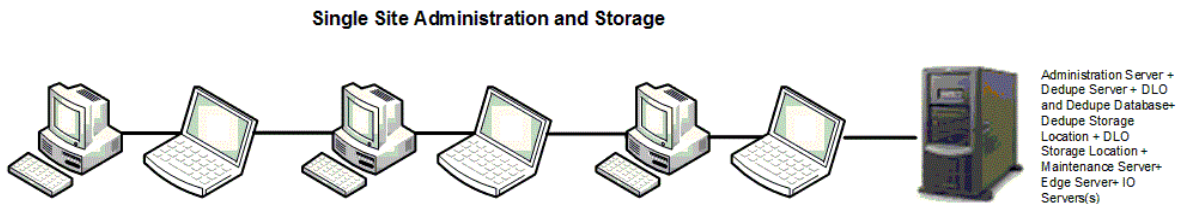
In this topology, a single DLO Administration Server will handle all the end-points in the site with all other Servers (Administration Server, Maintenance Server, Dedupe Server, Edge Server, IO Server) including the file servers in one place. This topology is easy for administration. Only one maintenance server is required, but in large installations it may be more efficient to have one maintenance server for each Storage Location host (that is File Server).

Single Site with Multiple Administration Servers

One DLO Administration Server will be able to handle around 100,000 users. If there is a requirement to support more than the supported number of users, then the users should be grouped into logical sites handled by independent DLO Administration Servers.

Multiple Sites with Centralized Administration Server

This topology is applicable when users are spread across multiple sites. This topology can be classified into two categories based on the network connectivity speed between the "centrally located servers" and the sites.

1. **Category 1:** All sites are connected to the central office by high-speed connectivity that matches or exceeds the speed of a LAN.
2. **Category 2:** One or more sites are connected to the central office by low-speed connectivity links.

In the first category, all DLO servers including the storage can be kept safely and managed at the central site. The only concern with this setup would be the amount of traffic that goes through WAN.

Category 1 - Multiple Sites with Centralized Administration Server
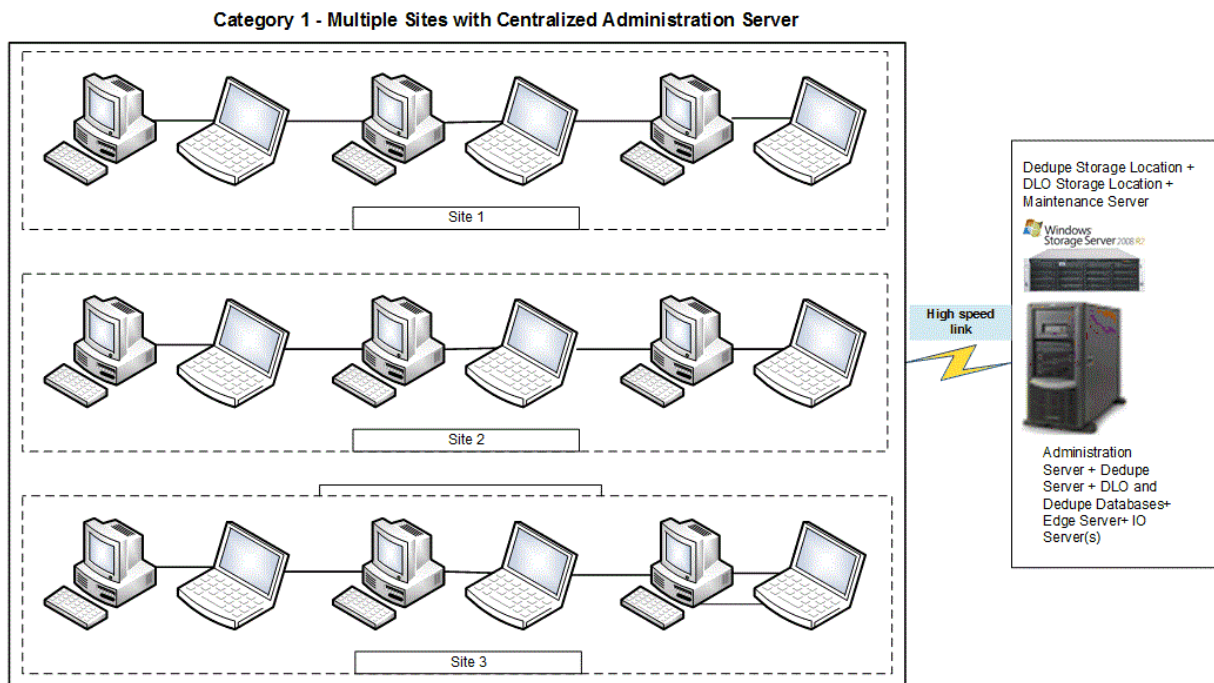
In the second category, all DLO servers can be kept in the central office, except for the storage. Since there is going to be a lot of IO involved during the backup process, it is advised to keep the storage local to each site. Since the storage is kept in each site, the Dedupe Storage Location(s) configured to a site specific Dedupe Storage Pool should also be configured in each site. Only site level deduplication can be achieved using this configuration, because of the site specific Dedupe Storage Pool.

Category 2 - Multiple Sites with Centralized Administration Server
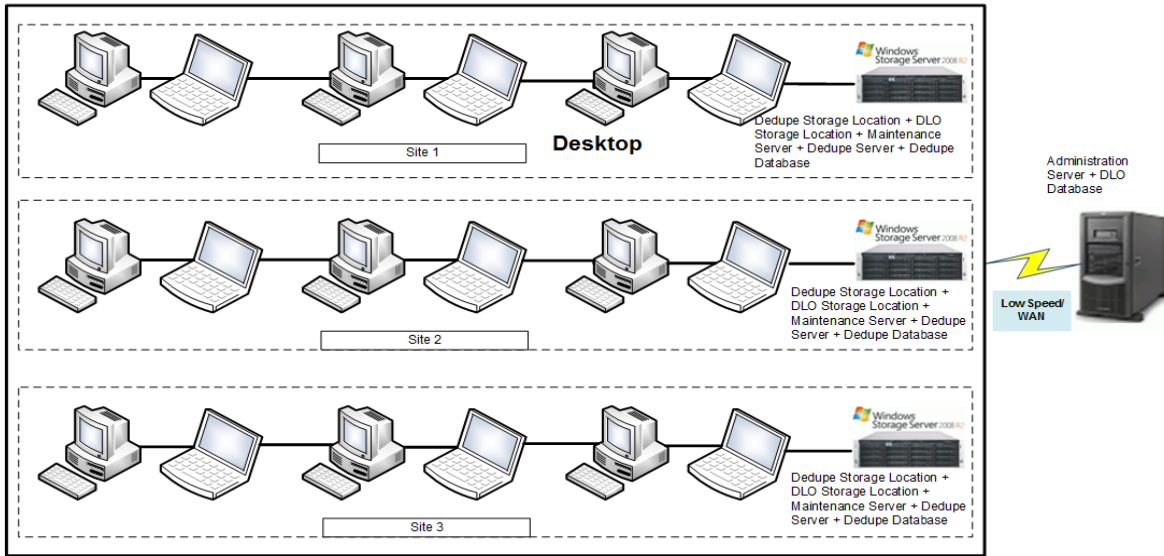
Note: Sites connected to central office with high speed links could be configured similar to the first option.

Multiple Sites with Independent Administration

This topology is applicable when the users are spread across multiple sites, with each site having relatively more number of users.

In this case, each independent site can be configured in the same manner as "Single Site with Single Administration   Server."

Multiple Sites with Independent Administration
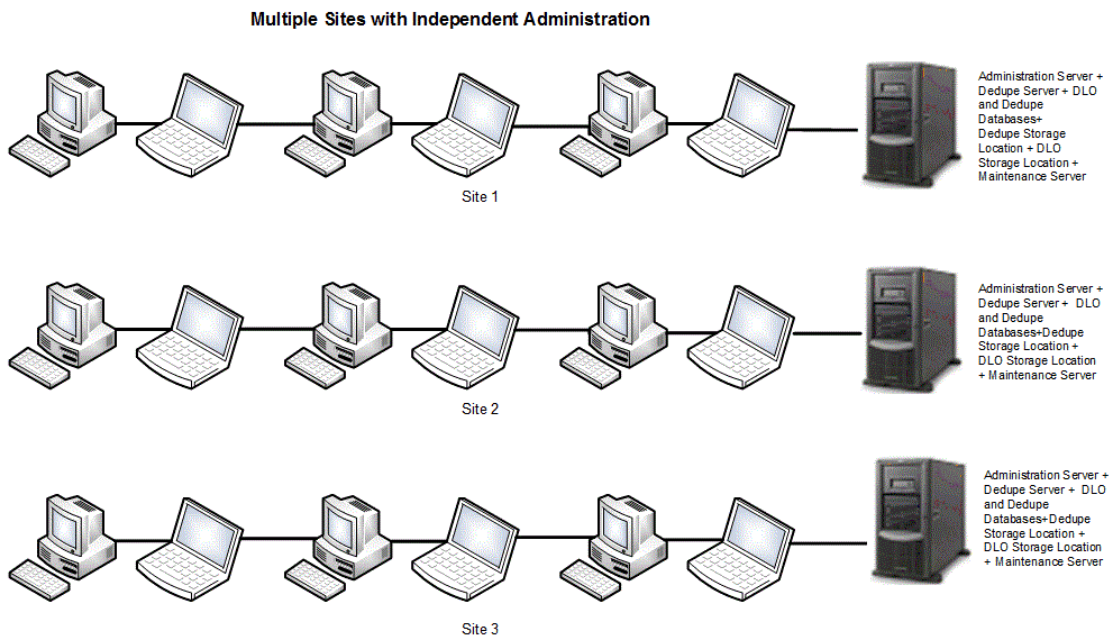
Recommendations:

User Count	Deployment Topology
Users<5000	All in one setup
Users>5000	Distributed Server Setups. **Note:** Recommended to deploy the Maintenance Server and File Servers on same machine, Dedupe Server and SQL Server (Dedupe Database) on one machine and other components (Administration Server, Edge Server, IO Server) on one machine.

Centralized vs. Distributed Administration Server

The following table provides additional information:

	Pros	Cons
Centralized	Single point of management and configuration. Single DLO database for backup and disaster recovery purposes Global Deduplication when Dedupe Server is centralized.	May require traffic over WANs for agent updates, loading and saving configuration settings, periodic Agent status updates, and alert data
Distributed	Isolates administrative traffic to the local network Provides local, independent control	No centralized management of DLO users and Profiles No Global Deduplication

Centralized Dedupe Server vs. Site level Dedupe Server

The following table provides additional information:

	Pros	Cons
Centralized	Global Deduplication Greater Deduplication savings	Data traffic from all remote clients to the central Dedupe Server
Site level	Data traffic is within the sites. As Dedupe Server is local on the site, the backups, restores and maintenance activities are considerably faster depending on the available bandwidth.	No Global Deduplication Lesser Deduplication savings

Determining Hardware Requirements

Veritas DLO is designed with the flexibility to operate on networks with a variety of structures. However, some factors that affect DLO efficiency and performance should be considered in the planning process for DLO.

Veritas DLO has the following components:

1. **Administration Server**: Moderately loaded component
2. **Administration Console**: On demand GUI
3. **Maintenance Server**: IO and CPU intensive
4. **Database**: IO and CPU intensive
5. **Dedupe Server**: CPU intensive and can leverage on multiple cores/processors.
6. **File Server**: IO intensive, CPU load is based on the Network Speed.
7. **Edge Server**: Apache Web server used for Front-Ending Application Servers
8. **IO Server**: Service hosted on Tomcat Web server

All these components can be installed independently in individual server machines or they can be installed in the same server as well. Installing all the components in one server is easy to administer. Having the Dedupe Server and the Dedupe Database in the same server machine is surely advantageous for the DLO performance.

Server hardware budgeting should be done considering the IO and CPU requirements of each of the components in each logical site controlled by the Administration Server.

Hardware Specification for All-In-One Setup (Administration Server, Maintenance Server, Database, Dedupe Server) (Excludes Edge Server and IO Server):

Users	<=1000	<=4000	<=8000	<=16000	<=32000	<=64000	~100000
CPU	64 Bit Quad Core Xeon	64 Bit 6 Core Xeon	64 Bit 8 Core Xeon	64 Bit 16 Core Xeon	64 Bit 16 Core Xeon	64 Bit 16 Core Xeon	64 Bit 16 Core Xeon
RAM	8 GB	12 GB	16 GB	32 GB	32 GB	48 GB	64 GB

Hardware Specification for All-In-One Setup (Administration Server, Maintenance Server, Database, Dedupe Server, Edge Server, IO Server):

Users	<=1000	<=4000	<=8000	<=16000	<=32000	<=64000	~100000
CPU	64 Bit Quad Core Xeon	64 Bit 8 Core Xeon	64 Bit 16 Core Xeon	64 Bit 16 Core Xeon	64 Bit 16 Core Xeon	64 Bit 16 Core Xeon	64 Bit 16 Core Xeon
RAM	12 GB	32 GB	32 GB	48 GB	48 GB	64 GB	96 GB

Hardware Specification for Administration Server/Maintenance Server:

Users	<=1000	<=4000	<=8000	<=16000	<=32000	<=64000	~100000
CPU	32/64 Bit Dual Core Xeon	32/64 Bit Dual Core Xeon	32/64 Bit Dual Core Xeon	32/64 Bit Dual Core Xeon	32/64 Bit Dual Core Xeon	32/64 Bit Dual Core Xeon	32/64 Bit Dual Core Xeon
RAM	8 GB	8 GB	8 GB	8 GB	12 GB	16 GB	32 GB

Hardware Specification for Dedupe Server:

Users	<=1000	<=4000	<=8000	<=16000	<=32000	<=64000	~100000
CPU	64 Bit Dual Core Xeon	64 Bit Quad Core Xeon	64 Bit 8 Core Xeon	64 Bit 16 Core Xeon	64 Bit 16 Core Xeon	64 Bit 16 Core Xeon	64 Bit 16 Core Xeon
RAM	4 GB	4 GB	8 GB	8 GB	12 GB	16 GB	16 GB

Hardware Specification for Database Server:

Users	<=1000	<=4000	<=8000	<=16000	<=32000	<=64000	~100000
CPU	64 Bit Dual Core Xeon	64 Bit Quad Core Xeon	64 Bit 8 Core Xeon	64 Bit 16 Core Xeon	64 Bit 16 Core Xeon	64 Bit 16 Core Xeon	64 Bit 16 Core Xeon
RAM	4 GB	4 GB	4 GB	8 GB	12 GB	16 GB	16 GB

Hardware Specification for Edge Server:

Users	<=1000	<=4000	<=8000	<=16000	<=32000	<=64000	~100000
CPU	64 Bit Quad Core Xeon	64 Bit Quad Core Xeon	64 Bit Quad Core Xeon	64 Bit 8 Core Xeon	64 Bit 16 Core Xeon	64 Bit 16 Core Xeon	64 Bit 16 Core Xeon
RAM	4 GB	4 GB	4 GB	8 GB	8 GB	8 GB	8 GB

Hardware Specification for IO Server:

Users	<=1000	<=4000	<=8000	<=16000
CPU	64 Bit Quad Core Xeon	64 Bit Quad Core Xeon	64 Bit 8 Core Xeon	64 Bit 16 Core Xeon
RAM	4 GB	4 GB	8 GB	12 GB

Note:

1. Multiple IO Servers can be configured based on the Number of roaming Users and Hardware availability. Single IO Server can handle 16,000 users. So for supporting more than 16,000 users, multiple IO Servers will be required.

2. The user count mentioned for Edge and IO servers are the expected number of roaming users.

3. File server(s) configuration and count should be decided based on the number of users, amount of storage space required, and the concurrent access supported. For more information, refer to the section Choosing File Server.

Configurations for Higher Scale

In case more than 16,000 users need to be supported by the DLO deployment, then some of the configuration parameters of Edge Server, IO Server(s) and Dedupe Server(s) need to get updated. These updates depend on the number of users to be supported by DLO say **maxUsers**.

IO Server

For each IO Server, execute below request in the browser. Here maxUsers is the number of users given IO Server will handle. DLO supports multiple IO Servers. In case of more than 16,000 maxUsers multiple IO Servers should be deployed for better performance.

```
http://<IOServer_IP>:<http_port>/DLOServer/rest1/operations/configureRequestS
cale/{maxUsers}/
```

```
Ex:
http://172.28.16.10:7080/DLOServer/rest1/operations/configureRequestScale/160
00/
```

Note: This request is restricted to work within LAN network over http port.

Dedupe Server

For each Dedupe Server, execute below request in the browser. Here maxUsers is the number of users given DedupeServer will handle.

```
http://<DedupeServer_IP>:<http_port>/DedupeServer/rest/dedupeManager/configur
eRequestScale/{maxUsers}/
```

```
Ex:
http://172.28.16.10:8080/DedupeServer/rest/dedupeManager/configureRequestScal
e/16000/
```

Note: This request is restricted to work within LAN network over http port.

Edge Server

1. Calculate the **ThreadLimit** as below.

set ThreadLimit = maxUsers*0.16

if ThreadLimit is greater than 15,000 then set ThreadLimit = 15,000

2. Update the file "C:\Program Files\Apache Software Foundation\Apache24\Conf\extra\httpd-mpm.conf" for below highlighted parameters (ThreadLimit and ThreadsPerChild).
The value for ThreadLimit and ThreadsPerChild is same as calculated in step 1.
\# WinNT MPM
\# ThreadsPerChild: constant number of worker threads in the server process
\# MaxConnectionsPerChild: maximum number of connections a server process serves
<IfModule mpm_winnt_module>
   ThreadLimit   2000
   ThreadsPerChild   2000
   MaxConnectionsPerChild   0
   AcceptFilter http none
   AcceptFilter https none
</IfModule>

3. Restart the DLO Edge Server Service.

Determining Software Requirements

We recommend that you take a mandatory decision to select the SQL Server Database Edition.

By default, DLO uses its own SQL Server Express instance. However, DLO can be manually configured to use other editions of SQL Server. The reason why you need to manually configure a non-express edition of database can be inferred from the following comparison chart.

Comparing SQL Express and SQL Server

	Pros	Cons
SQL Express	Free	The number of concurrent connections to the database is limited, resulting in slower I/O to the database under load. Maximum database size supported is 10 GB and is sufficient only for 8 TB of deduped backups. Cannot take advantage of the given hardware resources and scale.
SQL Server Non Express	Can scale for the given hardware and supported any amount of deduped backups.	Requires some manual configuration for DLO to work with SQL Server Cost. Also, if the customer has opted for a Server and Client Access licensing (CAL) model then, in addition to the Server license, CALs are required for each DLO client.

Regarding Server Certificates - The default installation of Edge Server comes with self-signed SSL certificate. However it is recommended to use SSL certificate issued by a trusted Certificate Authority. For more details on Server certificates, refer to *Veritas Desktop and Laptop Option Administrator's Guide* available at https://www.veritas.com/support/en_US/article.000116797.

In case of any certificate push from admin server, it is recommended to push the certificate before installing the clients. If the admin wants to push the certificate (any new CA cert. or Self signed cert.) after installing the clients, then ensure that the certificate is pushed when the clients are operating in LAN as certificate changes won't get reflected on the clients which are operating outside corporate network.

For those clients operating in BOI the user has to manually download the Edgeserver.ini and server certificate by using 'Server Certificate' option from web restore page. They can then replace the downloaded files in the DLO Agent install path for clients to work in BOI.

Storage Sizing

You can calculate the storage sizing requirements for Dedupe Storage Location, NUDF, Dedupe database, and the total data that these components can back up.

To calculate the storage sizing requirements, please use the spreadsheet **Veritas_DLO_9.0_Sizing_Calculator.xlsx** and the **Storage Estimation Tool User Guide** available at

https://www.veritas.com/support/en_US/article.000125463.

Choosing File Server

The server configuration will be in part, based on the number of users as well as the amount and type of data backed up.

The number of desktop computers backing up to the server at a time affects the efficiency of backup. In an environment where there are very large numbers of desktop computers in one location, it is important to size the file server appropriately, and it may be advantageous to install more than one file server.

Bus Architecture

High I/O throughput is a key factor in designing a DLO file server. A server with PCI/X or PCI-Express bus is recommended. The network controller and disk controller should be on this bus and not on the legacy PCI bus.

RAID

DLO puts very high file write demands on the file server, which can significantly affect a RAID controller. The RAID controller should be an intelligent controller with parity generation on the controller and not a host based controller with the server CPU used for parity generation. Parity RAID levels (3, 4, 5) are not recommended for write-intensive applications, but may be selected due to cost. RAID 10 will give significantly better performance.

Memory (Windows File Servers) recovery

More memory is always better. A minimum of 4GB should be considered.

Determine Backup Requirements

To determine organizational and user requirements for desktop and laptop backups, consider the following:

Profile Configuration

- How can users be grouped to take advantage of common characteristics? For example, users working with vital technical or regulatory information that is constantly changing may require more frequent backups than users who do not work with critical data.

- What is the quantity of data to be stored?

- What type of data do you want to protect? Will it be specific file type such as .doc or .pdf, specific folders, or a combination of both?

- What data should be excluded from backups?

- How many versions of each file should be retained?

- How frequently do you want to back up user data? Will backups be scheduled or will they be performed as files change?

- How do you want to backup (full backup/delta backups)?

- Do you want separate profile settings for BOI Enabled Users?

- Do you want the users to download the data through Web/Mobile App restore?

The answers to the questions above will guide decisions regarding hardware and network configuration as well as determining how Profiles will be designed to customize backups. The most successful large deployments of DLO use a pilot process to determine backup requirements.

Profile Setup

DLO uses Profiles to configure the settings of a group of similar users. The DLO administrator can customize the backup environment of the Profiles. The DLO administrator can assign users to Profiles automatically based on their domain and group, or can assign individual end-point users to Profiles.

- Modifications to a Profile or a backup selection will enable users of that Profile or backup selection to cancel jobs, load settings, restart backup engines, and scan their backup selection tree.

- The Profile should be configured to only back up user documents and not the entire machine.

- To minimize network bandwidth issues, define the Backup and Restore Throttling settings.

Determining What to Back up

- DLO uses backup selections in each Profile to specify which folders will be backed up. Include and exclude filters are added to further categorize which files and subfolders within the specified folder will be backed up.

   The following are the two types of excludes:

   - Global Excludes are specified by the administrator in the DLO Administration Console and apply to every backup selection. Files and folders specified in a Global Exclude are never backed up.

   - "Backup Selection Excludes" applies only to the specific Backup Selection in which they are created.

Note: DLO performance is directly related to the speed of the network and disk attached to the media servers. For more information on the recommended bandwidth and number of clients that can be backed up in parallel, refer to the *Veritas_DLO_9.0_Sizing_Calculator* mentioned in section on Storage Sizing.

Backup Strategies

Two options are available for Includes and Excludes in each Backup Selection: the "*include-only*" strategy and "*everything-but*" strategy.

Include-only strategy (recommended)

When you select the "*Include and exclude only the items listed below*" option in the backup selection, you create a custom list of file types that will be included or excluded. If no includes are specified when the backup selection is created, a "*" include is added, and all files that are not specifically excluded are backed up. If a specific include is later specified, the default "*" selection is removed, and only those files or folders specifically included are backed up.

For example, if you create a backup selection for `C:\Data` and select the "*Include and exclude only the items listed below*" option, but you do not provide any specific includes, all files not specifically excluded by the backup selection or Global Excludes will be backed up. If you later add an "*include*," such as *.doc, then only the *.doc files will be backed up.

Use this option in the following scenarios:

- You want to tailor the scope of backups to meet specific organizational needs

- You need to specifically target the backup scope to reduce the amount of data backed up

Users may store data in nonstandard locations or outside the selected backup area. This option may be considered when the data is adequately protected by the defined backup scope.

Everything-but strategy

When you select the "*Include all file types*" option in the backup selection, all files in the selected folder are backed up unless the file type is specifically excluded in the global exclude list.

Use this option in the following scenarios:

- File types and locations will vary across your environment.

- You have little control over the desktop environment.

- You want to protect all data, even if it increases costs and storage requirements.

The broad scope of backups may require significant storage space. To determine what files to exclude, look at the pending files during backup, or evaluate what is taking up space in the network and desktop user data folders, which can help refine the "*excludes*." For determining when to back up, Veritas recommends you use a continuous backup schedule. This keeps your files protected as they change and provides the maximum level of protection. This schedule also reduces the load on your network and media server by spreading out backups throughout the workday. However, if you choose to use a scheduled backup mode, make sure to consider the amount of changed data that will be sent to your backup destinations simultaneously. Creating several Profiles with staggered scheduled backup times will help reduce the load on your media server.

Determine When to Back up Data

Veritas recommends you use a continuous backup schedule. This ensures your files are protected as they change and provides the maximum level of protection. This schedule also reduces load on your network and Administration servers by spreading out backups throughout the workday.

However, if you choose to use a scheduled backup mode, be sure to consider the amount of changed data that will be sent to your Backup Destinations at or near the same time. Creating several Profiles with staggered scheduled backup times will help reduce load on your administration server.

BOI Backup Strategy

In cases where the existing profile is MAPI/Non MAPI enabled in earlier versions of DLO, and if you are enabling BOI for those profiles, then it is advised to back up the PST's when the clients are connected to LAN, because if the profile is BOI enabled, VSS PST backups will be enabled by Default and as a result full PST backups would get re-triggered for PST's which were already backed up. This will lead to significant amount of data transfers over the internet.

Due to the huge size of files during the Initial full backup, it is recommended to be over the corporate network than using BOI. For seamless backups over the internet, apart from the hardware configuration, the administrator may also need to take into consideration the bandwidth that is available on the server side.

Default Global Excludes

By default, the following file types and folders are excluded from all backups through the Global Excludes feature.

Default Global Excludes

Filter	Applies to
*.dat.log	Files
*.ost	Files
~.tmp	Files
System Volume Information	Folders
thumbs.db	Files
~*.doc	Files
~*.tmp	Files

Desktop Agent Rollout

When DLO needs to be provided to a large number of desktop users, it is best to roll out the Desktop Agent incrementally to reduce the impact on network and file servers. A small pilot deployment can accomplish this task while also providing an opportunity to refine the backup strategy and Profile settings.

For example, if you are deploying 1000 Desktop Agents, start with 15 users. Analyze the backup results and customize the Backup Selections if required. Deploy 100 users per week to reduce the impact of initial backups on the network.

Installing the Desktop Agent

The Desktop Agent is installed on each desktop computer by running the Desktop Agent install set. You can deploy the software in several ways. The following table lists the deployment options.

Desktop Agent Deployment Methods

Deployment Method	Description
Push Install	A push install is available for Veritas DLO using the Veritas DLO installer. This option is not available for NetBackup DLO.
Logon scripts	Create a logon script to automatically install the Desktop Agent on selected computers.
Microsoft Systems Management Server (SMS)	Use this automated system to distribute the Desktop Agent install set to the desktop computers, which then initiate the installation. For more information about SMS, refer to your Microsoft documentation.
Command Line Upgrade	Administrator has option to Upgrade the clients through Command line or Select all the users from Users tab in DLO Console and choose Upgrade User.
Right Click Upgrade	Administrator can select all the users from Users tab in DLO Console and choose Upgrade User.
Roaming Users	First time users who are not in Corporate network or the users who haven't upgraded to the Latest versions, can download and install the DLO Agent folder by logging into DLO Web Restore URL.

Note: Desktop Agent users are assigned to a specific server during the Desktop Agent installation. If DLO is deployed using multiple Administration Servers, then install the Desktop Agents using the Install set from the appropriate server.

Desktop Agent Command-Line Installation Options

The Desktop Agent installation can be customized to run silently, or to display a basic user interface that does not allow the user to cancel the installation. This task is accomplished by modifying the SETUP.INI file in the DLO Agent setup directory. In the SETUP.INI file there is a value called CmdLine that starts with a /qf. Change the /qf as shown below:

Desktop Agent Command-Line Installation Options

/qf Option	Result
/qn	Silent installation **Note**: For a completely silent install, run the "setup.exe /s" after modifying the SETUP.INI file.
/qb!	Basic user interface displayed. There is no Cancel button.

Examples:

For a silent installation, edit CmdLine in the SETUP.INI file as follows:

Original:

```
CmdLine=/qf DEFAULTMEDIASERVER="Desktop3" LAUNCHCLIENT="1" /l*v

"%TEMP%\DLOAgentInstall.log"
```

Modified:

```
CmdLine=/qn DEFAULTMEDIASERVER="Desktop3" LAUNCHCLIENT="1" /l*v

"%TEMP%\DLOAgentInstall.log"
```

For an installation with a basic interface but no option to cancel the installation, edit CmdLine in the SETUP.INI file as follows:

Original:

```
CmdLine=/qf DEFAULTMEDIASERVER="Desktop3" LAUNCHCLIENT="1" /l*v

"%TEMP%\DLOAgentInstall.log"
```

Modified:

```
CmdLine=/qb! DEFAULTMEDIASERVER="Desktop3" LAUNCHCLIENT="1" /l*v

"%TEMP%\DLOAgentInstall.log"
```

Client Use

Depending on what is being backed up especially large PST files, initial client backup can be time consuming and CPU intensive. If possible, this should be done when the end user is not using their machine. Initial backups are recommended over the corporate network and not over BOI. Memory consumption is entirely dependent on backup set selection and can vary significantly. It is usually highest at the beginning of a backup during scanning and tapers off during backup file transfer. DLO runs as a normal priority thread and DLO does not significantly impact performance of other applications.

With DLO 9.0, backups are now faster than that of the previous versions. In addition to that, backups can be accelerated further by the Administrator using the Backup Acceleration option. For more information, refer Accelerating Backup Operation of *Veritas Desktop and Laptop Option Administrator's Guide* available at https://www.veritas.com/support/en_US/article.000116797.

The DLO client interface should only be opened when you need to restore files or modify your selections.

When using synchronization, client clocks should be accurate and should be synchronized and the regional settings should reflect their correct locale.

For best PST message handling performance, Outlook should be set up so that email is delivered first to the server and not directly to a local PST file. If mail is delivered directly to your PST file, all mails received need to be backed up by DLO. This process can impact users when they first log on and run Outlook, and all new mails are delivered to the PST file.

DLO Cache Folder

DLO is configured to protect specific files. These files are first moved to the DLO cache folder on the Client and then are transferred to the DLO Storage Server.

The default location of the DLO cache folder is C:\Users\<user>\AppData\Local\Veritas

The DLO cache folder can be changed from the default to a drive that has more free space. If DLO is configured to keep zero revisions locally, it will leave a zero byte file in the DLO cache folder.

File revision setting is configured in the Profile on the DLO Administration Server.

Deploying DLO

Most organizations use the standard DLO Deployment with the default Profile. For more information about the process, refer to the *Veritas Desktop and Laptop Option Administrator's Guide* available at https://www.veritas.com/support/en_US/article.000116797.

The basic process is as follows:

1. Install Veritas DLO.
2. Launch Veritas DLO Administration Console.
3. Use the DLO configuration wizard to do the following:
    a. Set a Recovery Password.

Note: The recovery password enables you to retrieve encrypted data that would otherwise be lost if the DLO database is damaged or corrupted. If this password is lost or forgotten, this data may be unrecoverable.

    b. Create one or more new Profiles (optional).
    c. Create a storage location on the file server to store DLO backup files.
    d. Create one or more automated user assignments to automatically assign desktop users to a Profile and storage location when they install DLO.
4. Make any required customization to the Profiles.
5. Install the Desktop Agent on desktop computers.

When the DLO Administration Console is launched for the first time, the *Recovery Password Wizard* appears. You must set a recovery password using this wizard or DLO will not run. The recovery password enables you to retrieve encrypted data that would otherwise be lost if the DLO database is damaged or corrupted. Once set, this recovery password can only be changed using DLO command-line interface tools.

Note: The recovery of only non-dedupe data can happen using the recovery password. For recovery of dedupe data, refer Disaster Recovery Scenarios of *Veritas Desktop and Laptop Option Administrator's Guide* available at https://www.veritas.com/support/en_US/article.000116797.

Administrator Management

Delegating Tasks

The administrator can create multiple administrators with full or restricted privileges and choose to delegate routine administrative tasks to them.

For more information, refer Managing Administrator Accounts of *Veritas Desktop and Laptop Option Administrator's Guide* available at https://www.veritas.com/support/en_US/article.000116797.

Usage of Dashboard

The administrator can have a regular monitoring of the status of client backups by checking **Backup Status** Chart and taking necessary actions on the agents as and when required. It is suggested that the administrator leverage on the information on DLO versions from the **Distribution of Computers - DLO Versions** chart to plan and execute client updates.

Usage of Reports

A regular monitoring of the client backups can also be achieved by regularly running the **Backup Status** Report.

Basic Troubleshooting

The **DLO Diagnostic Utility** can be run from the server and client sides periodically to check the DLO System health. In case of failures in terms of backups, restores and other connectivity failures, we suggest using the Diagnostic utility to narrow down and identify the root cause of the issues.

For more information, refer Veritas DLO Diagnostic Tool of *Veritas Desktop and Laptop Option Administrator's Guide* available at https://www.veritas.com/support/en_US/article.000116797.

Best Practices for Cloud Storage

There are two possible deployments of AWS Storage Gateway. The AWS Storage Gateway can be run either on-premises, as a virtual machine appliance, or in AWS, as an Amazon EC2 instance. It is however recommended to have AWS Storage Gateway deployed on-premises to experience seamless data transfers.

For more information on the deployment, refer to the document *Veritas_DLO_Storage_in_Cloud.pdf* available at https://www.veritas.com/support/en_US/article.000116796