

Veritas™ Desktop and Laptop Option 9.8

Disaster Recovery Scenarios

Veritas Desktop and Laptop Option

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.

Legal Notice

Copyright (c) 2022 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.

This Veritas product may contain open source and other third party materials that are subject to a separate license. Please see the applicable Third Party Notice at <https://www.veritas.com/about/legal/license-agreements/>.

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 TECHNOLOGIES LLC 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/>

Technical Support

Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within the company to answer your questions in a timely fashion.

Our support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about our support offerings, you can visit our website at the following URL:

www.veritas.com/support

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.veritas.com/support

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
- Error messages and log files
- Troubleshooting that was performed before contacting Technical Support
- Recent software configuration changes and network changes

Licensing and registration

If your product requires registration or a license key, access our technical support Web page at the following URL:

www.veritas.com/support

Customer Service

Customer service information is available at the following URL:

www.veritas.com/support

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Advice about technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support Agreement Resources

If you want to contact us regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Worldwide (except Japan)

CustomerCare@veritas.com

Japan

CustomerCare_Japan@veritas.com

Contents

- Technical Support..... 3**
 - Contacting Technical Support..... 3
 - Licensing and registration 4
 - Customer Service 4
 - Support Agreement Resources..... 4
- Introduction 6**
 - Overview of DLO-Dedupe Setup 7
 - Disaster Recovery Scenarios..... 7

Introduction

This document explains the Disaster recovery scenarios for DLO versions 7.6 and above.

In a distributed and standalone setup, DLO is dependent on the following services:

- DLO Administration Service
- MindTree Storesmart Dedupe Server
- SQL Server (DLO / Instance Name)
- SQL Server (Dedupe / Instance Name)
- SQL Server Browser
- DLO Desktop Agent Change Journal Reader
- DLO Maintenance Service
- DLO Edge Server Service (Applicable to DLO 8.0 and above versions)
- DLO Web Server Service (Applicable to DLO 8.0 and above versions)

Important: For data restoration to be successful, we recommend that you take a periodic point in time (PIT) backups of critical components and server states.

The following are the four critical components required for data restoration:

1. DLO Database
2. Dedupe Database
3. DLO Network User Data Folder (NUDF)
4. Dedupe Storage Location (DSL)

The following configuration files on the Dedupe Server component should be backed up to preserve the configuration settings post a disaster recovery scenario:

For example, if Dedupe Server is installed in the path C:\Program Files\Veritas.

On the Dedupe Server:

S.No	Filename	Path
1.	All conf files	C:\Program Files\Veritas\Veritas DLO\Dedupe\Tomcat\conf
2.	Web.xml	C:\Program Files\Veritas\Veritas DLO\Dedupe\Tomcat\webapps\DedupeServer\WEB-INF
3.	log4j.properties	C:\Program Files\Veritas\Veritas DLO\Dedupe\Tomcat\webapps\DedupeServer\WEB-INF\classes

Note: Post the Disaster Recovery steps are performed, the above configuration files have to be manually replaced in their respective paths on the Dedupe Server. The DLO Administrator also needs to restart the Mindtree Storesmart Dedupe Server Service.

Overview of DLO-Dedupe Setup

Note: This recovery process is applicable to the setup where the DLO and Dedupe components are installed and configured together.

When a DLO Administration Server is configured with a Dedupe Server, the following components form a single logical entity in time.

- DLO configuration database
- Dedupe Server database files
- DLO file data in file server
- Dedupe Storage Location data

Hence, the backup and restore of these components should be performed together at a single logical point in time (PIT).

PIT across all the components requires the data writes to be stopped on all the components. The data writes can be stopped by disconnecting the individual components from the network or the Dedupe Server can be switched to maintenance mode by scheduling a Maintenance Window from the DLO Administration Console.

Backup

- Schedule a Maintenance Window with sufficient time out for backing up all components. If backup time cannot be estimated in advance, then a time out of '9999' minutes can be specified.
- Back up all the components and tag them together for easy identification of the same Point in Time for all the components.
- Stop the Maintenance Window from the DLO Administration Console.

For more information on scheduling or stopping a Maintenance Window, refer to the section “*Dedupe Server Maintenance*” in the *DLO Administrator's Guide*.

Restore

In case of a disaster, data of all the components should be restored to a suitable logical PIT backup.

To restore the data, follow these steps:

1. Shut down the Dedupe Server if it is running.
2. Restore all components data to the same logical Point in Time.
3. Run the following command: `DDAdminCU.exe -ConfirmDR`
4. Start the Dedupe Server.

We recommend that you follow this procedure for backup and restore operations, and thus prevent data loss or any issue related to data integrity.

Disaster Recovery Scenarios

The disaster recovery scenarios have been tested and qualified in the following distributed setup:

- Server 1: DLO Administration Server, DLO Admin Console and DLO Maintenance Server
- Server 2: Mindtree Storesmart Dedupe Server
- Server 3: Database Service (DB Service)
- Server 4: DLO Storage Location (NUDF)

- Server 5: Dedupe Storage Location (DSL)
- All DLO components residing on a single computer

Note: Database and NUDF is required to perform Disaster Recovery.

The following table contains various disaster recovery scenarios where data can be restored successfully.

No.	Scenario	Result	Remarks
Dedupe Disabled Profile			
1	All critical components and server states are backed up	All the components are restored to the point in time when it was backed up. To restore data using the Emergency Restore feature, use the recovery password that was provided while configuring DLO for the first time.	Restore and backups are successful.
2	Only the DLO Database and NUDF are backed up	<ol style="list-style-type: none"> 1. After the DLO installation is completed, stop the SQL service on the DB server. 2. Replace the DLO DB files and start the SQL service. 3. Now, launch the DLO Admin console. 4. Restore the data. 	The DLO clients that were configured earlier can continue to back up and restore data.
Dedupe Enabled Profile			
4	All critical components and server states are backed up	All the components are restored to the point in time when it was backed up. To restore data using the Emergency Restore feature, use the recovery password that was provided while configuring DLO for the first time.	Restore and backups are successful.
5	Dedupe DB,DLO DB,DSL and DLO Storage backed up	<ol style="list-style-type: none"> 1. After the DLO installation is completed, stop the SQL service on the DB server. 2. Replace the existing DLO DB files with the files that were backed up at an earlier PIT. 3. Start the SQL service. 4. Stop the Mindtree Storesmart Dedupe Server service. 5. Open the command prompt on the Dedupe server machine and run this command from the installation path: DDAdminCU.exe - ConfirmDR 6. Click OK and complete the DR process. 7. Start the Mindtree Storesmart Dedupe Server service. 8. Now, launch the DLO Admin console. 9. To verify that the data restored from the PIT backup is intact, 	Data can be restored from the DLO Admin console and by using the Emergency Restore feature. The DLO clients that were configured earlier can continue to back up and restore data.

No.	Scenario	Result	Remarks
		click the Restore tab on the DLO Admin console and restore data.	

Combination of Dedupe and Non-Dedupe Data			
6	All critical components and Server states are backed up	All the components are restored to the point in time when it was backed up. To restore data using the Emergency Restore feature, use the recovery password that was provided while configuring DLO for the first time.	Restore and backups are successful
7	Only the DLO Database and NUDF are backed up	<ol style="list-style-type: none"> 1. After the DLO installation is completed, stop the SQL service on the DB server. 2. Replace the existing DLO DB files with the files that were backed up at an earlier PIT. 3. Start the SQL service. 4. Now, launch the DLO admin console. 5. Restore the non-dedupe data. 	Non-Dedupe data can be restored

Note: For DLO 8.0 and above versions, Edge and IO Servers are not critical components with respect to data recovery. These components can be reconfigured once all components are recovered to original state.
