Dell DR Series System
Administrator Guide

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your computer.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

2015 - 04

Rev. A09

Contents

1

Introduction to the DR Series System Documentation

The DR Series system documentation contains topics that explain how to use the Dell DR Series system to perform data storage operations and manage storage and replication containers. The topics in this administrator's guide introduce and describe the DR Series system graphical user interface (GUI), which you use to manage your backup and replication operations. You can access this comprehensive GUI and the associated DR Series system features and capabilities via a supported web browser.

In addition to the DR Series system GUI, another method for managing the DR Series system is a command-line interface (CLI). In some instances, the DR Series system GUI may provide additional features and options that are not available in the DR Series system CLI and vice versa. For example, Global View is only available in the GUI, while the ability to add and remove clients in only available in the CLI. For more information about the DR Series system CLI commands, see the *Dell DR Series System Command Line Reference Guide*.

About the DR Series System GUI Documentation

The DR Series system documentation describes how to use the graphical user interface (GUI) and its menus, tabs, and options to perform a wide variety of data storage operations, and to manage the related storage and replication containers.

The documentation is written for an administrator end-user and introduces and provides procedures for using the DR Series system GUI elements to easily manage your backup and deduplication operations. A comprehensive set of GUI-based procedures allow you to access all of the key management features and capabilities using a supported web browser.

NOTE: For information about the supported web browsers you can use with the DR Series system, see the *Dell DR Series System Interoperability Guide* available at **support.dell.com/manuals**.

What's New In This Release

For a list of the features, enhancements, and changes in the latest release, see the section, "What's New In This Release" in the *Dell DR Series System Release Notes*. If you are upgrading from a previous software version, please see, "Upgrade Notes," in the *Dell DR Series System Release Notes*. You can download the latest documentation, including release notes, at **dell.com/powervaultmanuals** by selecting your specific DR Series system.

Other Information You May Need

WARNING: Refer to the safety and regulatory information that shipped with your system. Warranty information may be included within this document or as a separate document. Other DR Series system related documentation includes the following documents, which are available at dell.com/powervaultmanuals by selecting your specific DR Series system.

- *Dell DR Series System Owner's Manual* — provides information about solution features and describes how to troubleshoot the system and how to install or replace hardware versions of the DR Series system components.

- *Dell DR Series System Command Line Reference Guide* — provides information about managing DR Series system data backup and replication operations using the DR Series system command line interface (CLI).
- *Dell DR Series System Getting Started Guide* — provides an overview of setting up your DR Series system hardware and includes technical specifications.
- *Setting Up Your Dell DR Series System* — provides information about network, initial setup, and user account settings needed to initialize the Dell DR Series system.
- *Dell DR Series System Interoperability Guide* — provides information on the supported hardware and software that can be used with the DR Series system.
- *Dell DR2000v Deployment Guide* — provides information for deploying the virtual Dell DR Series system, DR2000v.
- *Dell DR Series System Release Notes* — provide the latest information about new features and known issues with a specific product release.
- Any media that ships with your system that provides documentation and tools for configuring and managing your system, including those pertaining to the operating system, system management software, system updates, and system components that you purchased with your system.

NOTE: Always check for documentation updates on **dell.com/powervaultmanuals**, and read the documentation updates first because they often supersede information in other documents and contain the latest updated versions of the documents.

NOTE: Always check for the latest release notes on **dell.com/powervaultmanuals** and read the release notes first because they contain the most recently documented information about known issues with a specific product release.

Source Code Availability

A portion of the DR Series system software may contain or consist of open source software, which you can use under the terms and conditions of the specific license under which the open source software is distributed.

Under certain open source software licenses, you are also entitled to obtain the corresponding source files. For more information about this or to find the corresponding source files for respective programs, see the Dell **opensource.dell.com** website.

2

Understanding the DR Series System

The Dell DR Series system is a high-performance, disk-based backup and recovery appliance that is simple to deploy and manage and offers unsurpassed Total Cost of Ownership benefits. Features such as innovative firmware and an all-inclusive licensing model ensure optimal functionality and provide the assurance of no hidden costs for valuable future features.

NOTE: Unless otherwise noted, later references in this guide to "the system" or "DR Series system" are used interchangeably to represent the Dell DR Series system.

A purpose-built disk platform, the DR Series system provides advanced deduplication and compression technology to store data most efficiently. The DR Series hardware appliances are 2U, rack-based, system backup storage repositories, that include deduplication and compression technology in their operating systems. A virtual machine (VM) version is also available (that is combined with a DR Series hardware appliance) to provide robust, disk-based data backup capability on VMs, while taking advantage of a deduplication-enabled appliance.

Using Dell deduplication and compression algorithm technology, a DR Series system can achieve data reduction levels ranging from 10:1 to 15:1. This reduction in data results in less incremental storage needs and a smaller backup footprint. By taking advantage of deduplication and compression features and removing redundant data, the system:

- Delivers fast, reliable backup and restore functionality
- Reduces media usage and power and cooling requirements
- Improves overall data protection and retention costs

The benefits of data deduplication can be extended across the enterprise—through the deduplicated replication functionality—to provide a complete backup solution for multi-site environments. The shorter Recovery Time Objectives (RTO) and attainable Recovery Point Objectives (RPO) are also assured as critical backup data remains on disk and online longer. Capital and administrative costs are diminished at the same time as internal service level agreements (SLAs) are more easily met.

The DR Series system includes the following features:

- Advanced data protection and disaster recovery
- Two management interfaces, a command line interface (CLI) or a system graphical user interface (GUI) for the system software to manage storage containers
- Wide variety of data backup installations and environments
- A simple installation process that provides full, intuitive remote setup and management capabilities

The DR Series system is available in a variety of drive capacities and is ideal for SMB, enterprise, and remote office environments. For details about specific drive capacities and types available in the DR Series system, see the *DR Series System Interoperability Guide* or the latest *DR Series System Release Notes*.

NOTE: DR Series system hardware also supports the use of external data storage expansion shelves (also known as expansion enclosures). An added expansion shelf enclosure must be equal to or greater than each DR Series system internal drive slot capacity (0–11). For more information about expansion enclosures, see the topic, “Expansion Unit Limits,” in the *Dell DR Series System Interoperability Guide* and Installing an Expansion Shelf License, DR Series System - Expansion Shelf Cabling, and Expansion Shelf Licenses in this guide.

About the DR Series System

The Dell DR Series system is a backup and recovery solution designed to reduce your backup data footprint by using a number of comprehensive backup and deduplication operations that optimize storage savings. The DR Series system is available in the following types:

- DR2000v—a Virtual Machine (VM) template for ESX and Hyper-V.
- DR4000–which consists of pre-installed DR4000 system software on a Dell PowerEdge R510 appliance platform.
- DR4100–which consists of preinstalled DR4000 system software on a Dell PowerEdge R720xd appliance platform.
- DR6000–which consists of preinstalled DR6000 system software on a Dell PowerEdge R720xd appliance platform. This differs from the DR4100 by including a higher level of base system hardware.

The DR Series system consists of the following components:

- Software — System software is pre-installed, which supports record linkage and context-based lossless data compression methods.
- Hardware/VM — The hardware and virtual appliances that support the DR Series systems are listed below:
  - DR2000v system: a VM template in various capacities for ESX and HyperV that can be deployed on our existing VM infrastructure.
  - DR4000 system: Includes twelve 3.5 inch SAS or Nearline SAS chassis drives that are hot-swappable, two power supplies for power redundancy, and two cabled 2.5-inch SAS drives for the operating system. The operating system is installed on two 2.5–inch internal drives that are in a RAID 1 configuration in the DR4000 system.
  - DR4100 system: Includes twelve 3.5 inch SAS or Nearline SAS chassis drives that are hot-swappable, two power supplies for power redundancy, and includes two 2.5-inch drives that are hot-pluggable in the rear.
  - DR6000 system: Includes twelve 3.5 inch SAS or Nearline SAS chassis drives that are hot-swappable, two power supplies for power redundancy, and includes two 2.5-inch drives that are hot-pluggable in the rear.

  NOTE: For slot locations for the twelve 3.5–inch drives in the hardware appliance-based DR Series system types, see DR Series System and Data Operations.
- Expansion shelf—The hardware system appliance supports the addition of external Dell PowerVault MD1200 data storage expansion shelf enclosures. Adding an expansion shelf provides additional data storage for the DR Series system and also requires a license. Each added expansion shelf enclosure must be equal to or greater than each DR Series system internal drive slot capacity (0–11). For more information, see "Expansion Unit Limits" in the *Dell DR Series System Interoperability Guide* and see Expansion Shelf Licenses in this guide. For more general information about the supported storage enclosures, see "DR Series Expansion Shelf" in DR Series System and Data Operations.

Drive and Available Physical Capacities

The internal system drive capacity and available physical capacities of the DR Series system vary, depending on your system type and the drives installed. For details, see the *Dell DR Series System Interoperability Guide*, which describes the internal system drive capacity and available physical capacity (in decimal and binary values) in the hardware DR Series systems. It also includes the available capacities per virtual machine operating system (OS) for the DR2000v.

DR Series Data Storage Concepts

The topics in this section present several key data storage terms and concepts that help you to better understand the role that the DR Series system plays in meeting your data storage needs.

Data Deduplication and Compression

The DR Series system design uses various data-reduction technologies, including advanced deduplication algorithms, in addition to the generic and custom compression solutions that prove effective across many differing file types. Data deduplication and compression is addressed in the following areas:

- DR Series System — The DR Series system backup and recovery appliances provide both efficient and high-performance disk-based data protection to leverage the advanced deduplication and compression capabilities in the DR Series system software. The DR Series systems provide a key component that performs backup, recovery, and data protection operations.
- Deduplication — This technology eliminates redundant copies of data and in the process it decreases disk capacity requirements and reduces the bandwidth needed for data transfer. Deduplication can be a major asset for companies that are dealing with increasing data volumes and require a means for optimizing their data protection.
- Compression — This technology reduces the size of data that is stored, protected, and transmitted. Compression helps companies improve their backup and recovery times while helping reduce infrastructure and network resource constraints.

In general, DR Series systems are disk-based data protection appliances that offer advanced deduplication and compression capabilities to reduce the time and cost associated with backing up and restoring data. Based on deduplication and compression technology, the DR Series systems eliminate the need to maintain multiple copies of the same data. This lets customers keep more data online longer and reduce the need for tape backup dependency.

Using its deduplication and compression technology, DR Series systems can help achieve an expected data reduction ratio of 15:1. Achieving this reduction in data means that you need fewer incremental storage operations to run and it provides you with a smaller backup footprint. By removing redundant data, DR Series systems deliver fast reliable backup and restore functionality, reduce media usage and power and cooling requirements, and improve your overall data protection and retention costs.

You can extend the benefits of data deduplication across the enterprise as well by using the DR Series system deduplication replication function–to provide a complete backup solution for multi-site environments. With 64:1 deduplicated replication (32:1 for DR4X00, 8:1 for DR2000v), up to 64 nodes can be replicated simultaneously to separate, individual containers on one node. The DR Series systems use compression with replication to shrink the data that is needed to be moved across the wire to a container.

Replication can be scheduled based on your settings to occur during non-peak periods. The replication schedule you create can be set and prioritized to ingest data over replication data to ensure the most optimal back up windows based on your needs.

Unlike NFS and CIFS containers, OST and RDS container replication is handled by the Data Management Applications (DMAs) media servers.

The DR Series system supports the 64:1 replication of data (32:1 if on the DR4X00 and 8:1 for the DR2000v), whereby up to 64 source DR Series systems can write data to different individual containers on a single, target DR Series system. This supports, for example, the use case where branch or regional offices can each write their own data to a separate, distinct container on a main corporate DR Series system.

NOTE: Be aware that the storage capacity of the target DR Series system is directly affected by the number of source systems writing to its containers and by the amount being written by each of the source systems.

If the source and target systems reside in different Active Directory (AD) domains, then the data that resides on the target DR Series system may not be accessible. When AD is used for authentication for DR Series systems, the AD information is saved with the file. This can serve to restrict user access to the data based on the type of AD permissions that are in place.

NOTE: This same authentication information is replicated to the target DR Series system when you have replication configured. To prevent domain access issues, ensure that both the target and source systems reside in the same Active Directory domain.

For a complete list of supported management application, refer to the *DR Series System Interoperability Guide*.

Encryption at Rest

Data that resides on the DR Series system can be encrypted. When encryption is enabled, the DR Series system uses the Industry standard FIPS 140-2 compliant 256-bit Advanced Encryption Standard (AES) encryption algorithm for encrypting and decrypting user data. The content encryption key is managed by the key manager, which operates in either a Static mode or an Internal mode. In Static mode, a global, fixed key is used to encrypt all data. In internal mode, key lifecycle management is performed in which the keys are periodically rotated. The minimum key rotation period before the content encryption key can be rotated and a new key is generated is 7 days. This rotation period is user-configurable and can be specified in days. A user-defined passphrase is used to generate a pass phrase key, which is used to encrypt the content encryption keys. It is mandatory to define a passphrase to enable encryption. The system supports up to a limit of 1023 different content encryption keys.

Streams vs. Connections

This topic describes the differences between data streams and application connections.

Streams can be likened to the number of files written at the same time to a DR Series system. The DR Series system tracks the number of files being written and assembles the data into 4MB chunks before processing that section of the data. If the stream count is exceeded, the data is processed out of order and overall deduplication savings can be affected. For details on maximum stream count, see the *Dell DR Series System Interoperability Guide*.

Connections are created by applications; within a single connection, there can be multiple streams depending on the application and how many backup jobs are running in parallel over that single connection. Replication can use up to 16 streams over a single port using one connection.

For example, suppose you are running backups using Backup Exec and using DR4100 and the CIFS protocol. If you have:

- One Backup Exec server connected to the DR4100 over CIFS and one backup running, you have **one connection** and **one stream**.
- One Backup Exec server connected to the DR4100 over CIFS with 10 concurrent backups running, you have **one connection** and **ten streams**. This means that Backup Exec is writing ten different files to the DR4100.

Replication

Replication is the process by which the same key data is saved from multiple storage locations, with the goal of maintaining consistency between redundant resources in data storage environments. Data replication improves the level of fault-tolerance, which improves the reliability of maintaining saved data and permits accessibility to the same stored data.

The DR Series system uses an active form of replication that lets you configure a primary-backup scheme. During replication, the system processes data storage requests from a specified source to a specified replica target, which acts as a replica of the original source data. This replica can then be cascaded optionally to a third location called a Cascaded replica for an additional copy.

NOTE: The DR Series system software includes version checking that limits replication only between other DR Series systems that run the same system software release version. If versions are incompatible, the administrator is notified by an event.

NOTE: Replication for VTL containers is not currently supported. However this feature is actively being worked on and will be made available in a future DR release.

Replicas/Cascaded replicas are read-only and are updated with new or unique data during scheduled or manual replications. The DR Series system can be considered to act as a form of a storage replication process in which the backup and deduplication data is replicated in real-time or via a scheduled window in a network environment. In a replication relationship between two or three DR Series systems, this means that a relationship exists between a number of systems. One system acts as the source and the other as a replica, with an optional third cascaded replica if you have chosen to keep two instances of replicated data in your backup workflow.

Replication is done at the container level and is one directional from SRC to Replica to Optional Cascaded Replica; however, since replication is done at the container level you can set up various containers to meet your specific replication requirements for your specific workflow. This form of replication is supported for the CIFS, NFS, Rapid CIFS, and Rapid NFS protocols and is fully handled by the DR Series system.

Unlike NFS, CIFS, Rapid NFS or Rapid CIFS containers, RDA with OST, RDA with NetVault Backup, and RDA with vRanger container replication is handled by Data Management Applications (DMAs) media servers.

The DR Series system supports the 64:1 replication of data (32:1 if on DR4X00 and 8:1 on DR2000v), whereby up to 64 source DR Series systems can write data to different individual containers on a single, target DR Series system. This supports the use case where branch or regional offices can each write their own data to a separate, distinct container on a main corporate DR Series system.

NOTE: Be aware that the storage capacity of the target DR Series system is directly affected by the number of source systems writing to its containers, and by the amount being written by each of the source systems.

If the source and target systems (replica or cascaded replica) are in different Active Directory (AD) domains, then the data that resides on the target system may not be accessible. When AD is used to perform authentication for DR Series systems, the AD information is saved with the file. This can act to restrict user access to the data based on the type of AD permissions that are in place.

NOTE: This same authentication information is replicated to the target DR Series system when you have replication configured. To prevent domain access issues, ensure that both the target and source systems reside in the same Active Directory domain.

Replication Seeding

The DR Series systems support replication seeding, which provides the ability to create a local seed and place it in a remote system. The seed backup is a process on the source DR Series system, which collects all of the unique data chunks from the containers and stores them on the target device. This is helpful if you have a new replication target DR to set up, the amount of data to be replicated is very large, and the network bandwidth is low. You can seed the target replica with the source data saved on a third party device, for example, a CIFS—mounted share, attach it to the target DR and then get the data into the target DR. Once the seeding is complete, replication is enabled between source and target and replication re-synchronization is done to complete any pending data transfers. Thereby, continuous replication can be done, which reduces network traffic significantly, and data can be replicated and synced with the target in a short amount of time.

You initiate seeding using CLI, and the data to be seeded is gathered in an organized manner and stored in the target devices. Refer to the *Dell DR Series System Command Line Reference Guide* for more information about replication seeding support.

Reverse Replication

The concept of reverse replication is not a supported operation on DR Series systems. This is because replica containers are always in a R-O (read-only) mode on the DR Series system, thus making write operations a non-supported operation.

Alternate Ways to Retrieve Data

Under very specific conditions, it might be possible for replica containers to support a type of write operation whose sole function is to restore data from an archival target. For example, data could be replicated back to the remote site where a data management application (DMA), or backup software, is connected to allow this data to be restored directly.

This specific type of case applies only to configurations where data is backed up from a remote location to a local container, and then replicated over a WAN to a replica container that is backed up to tape. The data needs to be restored from the tape backup to the original location; first back to a DR Series system replica container, and then back to the original source location of the data on the other side of the WAN link.

NOTE: If you choose to use this alternate workaround method, you must set up a new data storage unit in the DMA, and import the images before a restore to the original location can occur.

To leverage this type of deduplication across the WAN, complete the following:

1. Make sure that the replication operation has completed (between source and target).
2. Delete the current replication relationship, and re-create a replication relationship (reversing the source and target roles).
3. Restore data to the original source container (now the target).
4. Make sure that the replication operation has completed.
5. Delete the replication relationship and re-create a replication relationship (restoring original source and target destinations).

Under this scenario, a fraction of the data to be recovered is sent across the WAN link. This could speed up a remote restore significantly. However, there are some downsides to this type of scenario:

- If step 1 is not followed correctly, any changes not fully replicated are lost.
- During steps 2 and 3, any data that is written to the original DR Series system source container may be lost.
- During step 4, if the data is not fully replicated back before the switch is made, it may be lost.

Alternatively, you could still support this type of effort by completing the following:

1. Create a new container on the target DR Series system.
2. Set up replication from this container back to the source DR Series system container.
3. Set up a new disk storage unit in the DMA and make sure that the DMA is aware of any new images.
4. Import the old images back into the DMA from the target DR Series system (the original source location).
5. Use a new disk storage unit in the DMA, and then restore the data back to the original client.

Reverse Replication: Alternate Method

To support an alternate method of reverse replication, complete the following:

1. Create a new container on the target DR Series system.
2. Set up replication from this container back to the source DR Series system container.
3. Set up a new disk storage unit in the DMA and make sure that the DMA is aware of any new images.
4. Import the old images back into the DMA from the target DR Series system (the original source location).
5. Use a new disk storage unit in the DMA, and then restore the data back to the original client.

Supported File System and Tape Access Protocols

The DR Series system supports the following file system and tape access protocols. The Rapid Data Access (RDA) protocols below provide a logical disk interface that can be used with network storage devices to store data and support data storage operation.

- Network File System (NFS)
- Common Internet File System (CIFS)

- DR Rapid
  - Rapid NFS
  - Rapid CIFS
  - RDA with OpenStorage Technology (OST)
  - RDA with NetVault Backup
  - RDA with vRanger
- Virtual Tape Library (VTL)
  - Network Data Management Protocol (NDMP)
  - Internet Small Computer System Interface (iSCSI)

NFS

The Network File System (NFS) is a file system protocol that is designated to be a file server standard, and its protocol uses the Remote Procedure Call (RPC) method of communication between computers. Clients can access files via the network similar to the way that local storage is accessed.

NFS is a client-server application in which a client can view, store, and update files on a remote system just like they are working on a local system. System or Network Administrators can mount all or a portion of a file system, and the file system (or portion) that is mounted can be accessed using the privileges assigned to each file.

NOTE: If you want to do a mount on AIX, you must set the nfs_use_reserved_ports and portcheck parameters first. The parameters cannot be set to 0. For example: `root@aixhost1 / # nfso -po portcheck=1`
`root@aixhost1 / # nfso -po nfs_use_reserved_ports=1`

CIFS

The Common Internet File System (CIFS) remote file access protocol is one supported by the DR Series system, and is also known as a Server Message Block (SMB). SMB occurs more commonly than the Network File System (NFS) protocol on systems that run the Microsoft Windows operating system. CIFS allows programs to request files or services on remote computers.

CIFS also uses the client-server programming model, whereby the client requests access to a file or passes a message to a program running on the server. Servers review all requested actions and return a response. CIFS is a public (or open) variation of the SMB that was originally developed and used by Microsoft.

NOTE: The DR Series system currently supports version 1.0 of the Server Message Block (SMB).

NOTE: For details on CIFS feature restrictions, see the *Dell DR Series System Interoperability Guide*, at **support.dell.com/manuals**.

CIFS ACL Support

The DR Series system software supports the use of access control lists (ACLs) for CIFS and share-level permissions. By definition, an ACL is simply a list of permissions that can be associated with any network resource.

Each ACL can contain access control entries (ACEs) that define or describe the permissions for an individual user or a group of users. An ACL can consist of zero (meaning that all users have access) or a number of ACEs that define specific permissions on a per-user or per-group basis.

NOTE: If an ACE list is empty (meaning that it contains zero entries), this means that all access requests will be granted.

An ACL describes the entities that are allowed to access a specific resource. ACLs are a built-in access control mechanism in the Windows operating systems.

NOTE: The DR Series system supports setting up share-level permissions for a CIFS share using a Microsoft Windows administrative tool. Share-level permissions let you control access to shares. For more information, see Configuring Share-Level Security.

NOTE: Any user that is part of BUILTIN\Administrators can edit ACLs on CIFS shares. The local DR Series system administrator is included in the BUILTIN\Administrators group. To add additional domain groups to the BUILTIN \Administrators group, you can use the Computer Manager tool on a Windows client to connect to the DR Series system as Domain administrator and add any groups you want. This capability allows users other than the Domain administrator to modify an ACL as needed.

Access Control List Support in Containers

All new containers apply a default Access Control List (ACL) at the root of the container. This default ACL is the same as that which would be created by a Microsoft Windows 2003 Server. Therefore, these new containers with the default ACL support the following permission types:

NOTE: Any user that is part of BUILTIN\Administrators can edit ACLs on CIFS shares. The local DR Series system administrator is included in the BUILTIN\Administrators group. To add additional domain groups to the BUILTIN \Administrators group, you can use the Computer Manager tool on a Windows client to connect to the DR Series system as Domain administrator and add any groups you want. This capability allows users other than the Domain administrator to modify an ACL as needed.

- BUILTIN\Administrators:

Allows	Full access, object inherit, and container inherit.
Applies to	This folder, subfolders, and files.

- CREATOR OWNER:

Allows	Full access, inherit only, object inherit, and container inherit.
Applies to	Subfolders and files only.

- EVERYONE:

Allows	Traverse folders, execute files, list folders, read data, read attributes, and read extended attributes.
Applies to	This folder only.

- NT AUTHORITY\SYSTEM:

Allows	Full access, object inherit, and container inherit.
Applies to	This folder, subfolders, and files.

- BUILTIN\Users:

Allows	Create folders and append data, inherit-only, and container inherit.
Applies to	This folder, subfolders, and files.

- BUILTIN\Users:

Allows	Read and execute, and container inherit.
Applies to	This folder, subfolders, and files.

- BUILTIN\Users:

Allows	Create files and write data, object inherit, and container inherit.
Applies to	Subfolders only.

NOTE: If these permissions are unsuitable for your needs, you can modify the default ACL to suit your own requirement using the Windows ACL Editor (for example, using **Properties** → **Security** from Windows Explorer).

NOTE: The system does not understand the Owner Rights permission and sets the owner of new files/folders created by the Domain Administrators as DOM\Administrator rather than as BUILTIN\Administrators.

Unix Permissions Guidelines

For a user to create, delete, or rename a file or a directory requires Write access to the parent directory that contains these files. Only the owner of a file (or the root user) can change permissions.

Permissions are based on the user IDs (UIDs) for the file Owner and group IDs (GIDs) for the primary group. Files have owner IDs and group owner IDs. To enable Unix access, the DR Series system supports three levels of users:

- Owner (of the file)
- Group (group in which the owner belongs)
- Other (other users with an account on the system)

Each of these three user types support the following access permissions:

- Read (read access that allows user to read files)
- Write (write access that allows user to create or write to a file)
- Execute (access that allows user to execute files or traverse directories in the filesystem)

NOTE: A root user has all levels of permission access, and a user can be a member of a single group or of multiple groups (up to 32 groups are allowed in Unix).

Windows Permissions Guidelines

To enable Windows access, the DR Series system supports access control lists (ACLs) that contain zero or more access control entries (ACEs), and an empty ACE list grants all access requests. The Windows New Technology File System (NTFS) uses ACLs as part of the security descriptor (SD) process, which requires permissions to access such filesystem objects as files and directories. ACLs support two levels of users:

- Owners
- Groups

Both Owners and Groups have Security IDs (SIDs) that define and identify an object owner or the group owning an object. ACEs in an ACL consist of a SID, a specific permission that either allows or denies access and also defines which of the following inheritance settings apply:

- IO—inherit-only: not used for access checking.
- OI—object inherit: new files get this ACE added.
- CI—container inherit: new directories get this ACE added.

Windows NTFS ACLs include the following read, write, append, execute, and delete permissions that allow users to:

- Synchronize access
- Read data or list the directory
- Write data or add a file

- Append data or add a folder
- Read Extended Attributes (EAs)
- Write EAs
- Execute file or traverse folders
- Delete child or delete folders
- Delete a file

The Owner user type has two default permissions:

- Write discretionary ACL
- Read control

Rapid NFS and Rapid CIFS

Rapid NFS and Rapid CIFS enable write operation acceleration on clients that use DR replication and NFS or CIFS file system protocols. Similar to OST and RDS, these accelerators allow for better coordination and integration between DR Series system backup, restore, and optimized deduplication operations with Data Management Applications (DMAs) such as CommVault, EMC Networker, and Tivoli Storage Manager. For the current list of qualified DMAs, see the *Dell DR Series System Interoperability Guide*.

Rapid NFS is a new client file system type that ensures that only unique data is written to the DR Series system. It uses user space components and file system in user space (FUSE) to accomplish this. Metadata operations such as file creates and permission changes go through the standard NFS protocol, whereas write operations go through RDNFS.

Rapid CIFS is a Windows-certified filter driver that also ensures that only unique data is written to the DR Series system.

All chunking and hash computations are done at the media or client server level.

Rapid NFS and Rapid CIFS require you to install a plug-in on the client or media server, depending on your DMA and configuration. For details, see the Configuring and Using Rapid NFS and Rapid CIFS chapter.

DR Rapid for the DR Series System

DR Rapid is developed by Dell and provides a logical disk interface for use with network storage devices. DR Rapid allows for better coordination and integration between DR Series system backup, restore, and optimized duplication operations with backup applications, such as Dell NetVault Backup (NVBU).

The DR Series system and backup application integration is done using DR Rapid plugins developed by Dell. Plugins allow backup application control over backup image creation, deletion, and duplication. They also allow deduplication and compression operations to happen on the client-side so that network traffic can be reduced.

DR Rapid allows the supported backup applications to communicate directly with the DR Series system and determine whether a specific chunk of data already exists on the system. If the data already exists, only the pointers need to be updated on the DR Series system, and the duplicate chunk of data does not need to be transferred to the system. This process provides two benefits: it improves the overall backup speed, and also reduces the network load.

RDA with OST for the DR Series System

OpenStorage Technology (OST) is developed by Symantec and provides a logical disk interface for use with network storage devices. The DR Series system appliance can use OST via DR Rapid plug-in software to integrate its data storage operations with a number of data management applications (DMAs). Within Dell, OST is part of DR Rapid.

RDA with OST allows for better coordination and tighter integration between DR Series system backup, restore, and optimized duplication operations and data management applications. For a list of the supported applications, see the *Dell DR Series System Interoperability Guide*.

Integration is done via a RDA with OST plug-in developed for the DR Series system, through which data management applications can control when the backup images are created, duplicated, and deleted. The major benefit of RDA with OST is that it allows the deduplication operations to happen on the client side so that network traffic can be reduced.

The RDA with OST plug-in allows data management applications to take full advantage of such DR Series system features as data deduplication, replication, and energy efficiency. DR Series systems can access the OpenStorage API code through the plug-in, which can be installed on the media server platform choice you make (Windows or Linux). The OST protocol allows the supported backup applications to communicate directly with the DR Series system and determine whether a specific chunk of data already exists on the system. This process means that if the data already exists, only the pointers need to be updated on the DR Series system, and the duplicate chunk of data does not need to be transferred to the system. This process provides two benefits: it improves the overall backup speed, and also reduces the network load.

When RDA with OST is used with the DR Series system, it offers the following benefits:

- OST protocol provides faster and improved data transfers:
  - Focused on backups with minimal overhead
  - Accommodates larger data transfer sizes
  - Provides throughput that is significantly better than CIFS or NFS
- RDA with OST and DMA integration:
  - OpenStorage API enables the DMA-to-media server software communications
  - DR Series system storage capabilities can be used without extensive changes to DMAs
  - Backup and replication operations are simplified by using built-in DMA policies
- DR Series system and RDA with OST:
  - Control channel uses TCP port 10011
  - Data channel uses TCP port 11000
  - Optimized write operations enable client-side deduplication
- Replication operations between DR Series systems:
  - No configuration required on source or target DR Series systems
  - Replication is file-based, not container-based
  - Triggered by DMA optimized duplication operation
  - DR Series system transfers the data file (not the media server)
  - After duplication, DR Series system notifies DMA to update its catalog (acknowledging the second backup)
  - Supports different retention policies between source and replica

Software Components and Operational Guidelines

To better coordinate and integrate OpenStorage Technology (OST) with the DR Series system data storage operations, the following guidelines list the required components and supported operations. For details on the supported operating systems and DMA versions, see the *Dell DR Series System Interoperability Guide*.

The Dell DR Series system licensing is all-inclusive, so that no additional Dell licensing is required to use OST or the optimized duplication capability. The Dell OST plug-in that gets installed on a supported Linux or Windows media server platform is a free download from Dell. However, Symantec NetBackup requires that you purchase a Symantec OpenStorage Disk Option license. Similarly, Symantec Backup Exec requires that you purchase the Deduplication Option to enable the OST feature.

- OST Media Server Component:

  - An OST server component resides on the DR Series system
  - For Linux media server installations, use the Linux OST plug-in and the Red Hat Package Manager (RPM) installer
  - For Windows media server installations, use the Windows OST plug-in and the Microsoft (MSI) installer
- Windows-based OST plug-in
- Linux-based 64-bit OST plug-in
- Supported Symantec OpenStorage (OST) protocol:
  - Symantec, version 9
  - Symantec, version 10
- Supported Symantec DMAs
  - NetBackup
  - Backup Exec
- Supported OST operations
  - Backup (Passthrough writes and Optimized writes)
  - Restore
  - Replication

Supported Virtual Tape Library Access Protocols

The DR Series system supports the following virtual tape library (VTL) tape access protocols.

- Network Data Management Protocol (NDMP)
- Internet Small Computer System Interface (iSCSI)

NDMP

The Network Data Management protocol (NDMP) is used to control data backup and recovery between primary and secondary storage in a network environment. For example, a NAS server (Filer) can talk to a tape drive for the purposes of a backup.

You can use the protocol with a centralized data management application (DMA) to back up data on file servers running on different platforms to tape drives or tape libraries located elsewhere within the network. The protocol separates the data path from the control path and minimizes demands on network resources. With NDMP, a network file server can communicate directly to a network-attached tape drive or virtual tape library (VTL) for backup or recovery.

The DR Series system VTL container type is designed to work seamlessly with the NDMP protocol.

iSCSI

iSCSI or **Internet Small Computer System Interface** is an Internet Protocol (IP)-based storage networking standard for storage subsystems. It is a carrier protocol for SCSI. SCSI commands are sent over IP networks by using iSCSI. It also facilitates data transfers over intranets and to manage storage over long distances. iSCSI can be used to transmit data over LANs or WANs.

In iSCSI, clients are called *initiators* and SCSI storage devices are *targets*. The protocol allows an *initiator* to send SCSI commands (*CDBs*) to the *targets* on remote servers. It is a storage area network (SAN) protocol, allowing organizations to consolidate storage into data center storage arrays while providing hosts (such as database and web servers) with the illusion of locally attached disks. Unlike traditional Fibre Channel, which requires different cabling, iSCSI can be run over long distances using existing network infrastructure.

iSCSI is a low-cost alternative to Fibre Channel, which requires dedicated infrastructure except in FCoE (Fibre Channel over Ethernet). Note that the performance of an iSCSI SAN deployment can be degraded if not operated on a dedicated network or subnet

The VTL container type is designed to work seamlessly with the iSCSI protocol. For details, see the topic, Creating Storage Containers.

DR Series System Hardware and Data Operations (DR4X00/DR6000)

Data is stored and resides on the Dell DR Series system hardware appliance (DR4X00/DR6000), a two-rack unit (RU) appliance, which has the DR Series system software pre-installed.

The DR Series system hardware consists of a total of 14 drives. Two of these drives are 2.5-inch drives that are configured as a Redundant Array of Independent Disks (RAID) 1 on the RAID Controller, and this is considered to be volume 1. In the DR4000 system, these drives are internal, while in the DR4100 and DR6000 systems, these drives are accessible from the rear of the appliance. The data that is being backed up is stored on the 12 virtual disks that reside on the DR Series system. The DR Series system also supports additional storage in the form of external expansion shelf enclosures (see the *DR Series Expansion Shelf* section in this topic). The hot-swappable data drives that are attached to the RAID controller are configured as:

- 11 drives that operate as RAID 6, which act as virtual-disks for data storage (drives 1–11).
- The remaining drive (drive 0) acts as the dedicated hot-spare drive for RAID 6 for the system.

The DR Series system supports RAID 6, which allows the appliance to continue read and write requests to the RAID array virtual disks even in the event of up to two concurrent disk failures, providing protection to your mission-critical data. In this way, the system design supports double-data drive failure survivability.

If the system detects that one of the 11 virtual drives has failed, then the dedicated hot spare (drive slot 0) becomes an active member of the RAID group. Data is then automatically copied to the hot spare as it acts as the replacement for the failed drive. The dedicated hot spare remains inactive until it is called upon to replace a failed drive. This scenario is usually encountered when a faulty data drive is replaced. The hot spare can act as replacement for both internal mirrored drives and the RAID 6 drive arrays.

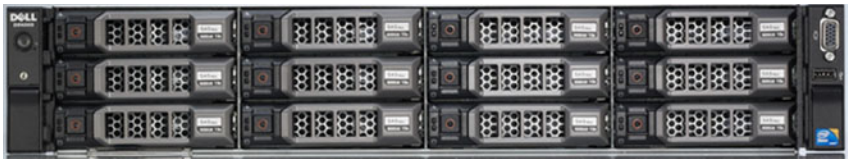


Figure 1. DR Series System Drive Slot Locations

Drive 0 (top)	Drive 3 (top)	Drive 6 (top)	Drive 9 (top)
Drive 1 (middle)	Drive 4 (middle)	Drive 7 (middle)	Drive 10 (middle)
Drive 2 (bottom)	Drive 5 (bottom)	Drive 8 (bottom)	Drive 11 (bottom)

DR Series Expansion Shelf

Each DR Series system appliance supports the installation and connection of Dell PowerVault MD1200 data storage expansion shelf enclosures. Each expansion shelf contains 12 physical disks in an enclosure, which provides additional data storage capacity for the basic DR Series system. The supported data storage expansion shelves can be added in a variety of capacities based on your DR Series system version; for details, see the *Dell DR Series System Interoperability Guide*.

The physical disks in each expansion shelf are required to be Dell-certified Serial Attached SCSI (SAS) drives, and the physical drives in the expansion shelf uses slots 1–11 configured as RAID 6, with slot 0 being a global hot spare (GHS).

When being configured, the first expansion shelf is identified as Enclosure 1 (in the case where two enclosures are added, these would be Enclosure 1 and Enclosure 2). Adding an expansion shelf to support the DR Series system requires a license. For more information, see Expansion Shelf Licenses.

NOTE: The 300 Gigabyte (GB) drive capacity (2.7 TB) version of the DR Series system does not support the addition of expansion shelf enclosures.

NOTE: If you are running a DR Series system with an installed release of system software prior to 2.1, and you intend to upgrade to release 3.x system software and add an external expansion shelf (or shelves), Dell recommends that you observe the following best practice sequence of operations to avoid any issues:

- Upgrade the DR Series system with the release 3.x system software
- Power off the DR Series system
- Connect the external expansion shelf (or shelves) with cabling to the DR Series system
- Power on the external expansion shelf (or shelves)
- Power on the DR Series system

NOTE: If you install an expansion shelf enclosure to support a DR Series system, each shelf must use physical disks that have a capacity equal to or greater than each DR Series system internal drive slot capacity (0–11) that they are supporting.

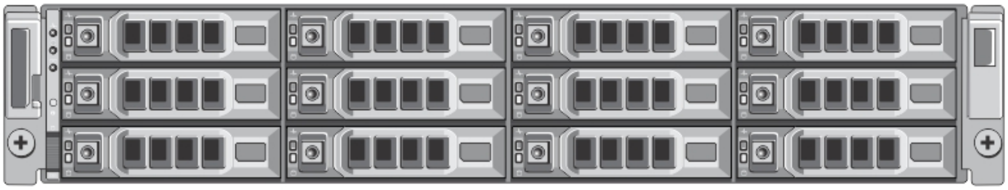


Figure 2. DR Series System Expansion Shelf (MD1200) Drive Slot Locations

Drive 0 (top)	Drive 3 (top)	Drive 6 (top)	Drive 9 (top)
Drive 1 (middle)	Drive 4 (middle)	Drive 7 (middle)	Drive 10 (middle)
Drive 2 (bottom)	Drive 5 (bottom)	Drive 8 (bottom)	Drive 11 (bottom)

Understanding the Process for Adding a DR Series Expansion Shelf

The process for adding an expansion shelf requires the following:

- Physically adding or installing the expansion shelf (for more information, see Adding a DR Series System Expansion Shelf)
- Cabling the expansion shelf to the DR Series system (for more information, see DR Series System - Expansion Shelf Cabling)
- Installing the license for an expansion shelf (for more information, see Installing an Expansion Shelf License)
- Using the DR Series system GUI to add or detect the expansion shelf (for more information, see Adding a DR Series System Expansion Shelf)

Supported Software and Hardware

For a complete list of the latest supported software and hardware for the DR Series system, refer to the *Dell DR Series System Interoperability Guide*. You can download this guide by visiting dell.com/powervaultmanuals and selecting your specific DR Series system, which opens the product support page to view product documentation for your system.

The *Dell DR Series System Interoperability Guide* lists the following supported hardware and software categories:

- Hardware
  - BIOS
  - RAID controllers
  - Hard drives (internal)
  - Hard drives (external)
  - Expansion unit limits
  - USB flash drives
  - Network interface controllers
  - iDRAC Enterprise
  - Marvell WAM controller
- Software
  - Operating System
  - Supported backup software
  - Network file protocols and backup client operating systems
  - Supported web browsers
  - Supported system limits
  - Supported OST software and components
  - Supported RDS software and components
  - Supported Rapid NFS and Rapid CIFS software and components

Terminal Emulation Applications

To access the DR Series system command line interface (CLI), the following terminal emulation applications can be used:

- FoxTerm
- Win32 console
- PuTTY
- Tera Term Pro

NOTE: The listed terminal emulation applications are not the only ones that work with the DR Series system. This list is only intended to provide examples of terminal emulation applications that can be used.

DR Series (DR4X00/DR6000) — Expansion Shelf Cabling

Each DR Series system appliance is capable of supporting additional storage capacity by connecting Dell PowerVault MD1200 data storage expansion shelf enclosures. Each expansion shelf enclosure contains 12 physical disks that provide additional data storage capacity for a basic DR Series system. For the expansion unit limits and supported capacities, see the *Dell DR Series System Interoperability Guide*.

Figure 1 and Figure 2 display the recommended method for cabling between the DR Series system's PERC controller card to the appropriate connectors on the rear of the Dell PowerVault MD1200 expansion shelf enclosure.

Make sure that the Dell PowerVault MD1200 front panel selector switch is set to its Unified mode (with the switch set to its "up" position, indicated by a single Volume icon). Figure 1 shows the SAS In ports on the Enclosure Management Module (EMM) on the rear of the Dell MD1200. Figure 2 shows the recommended redundant path cabling configuration, which includes cable connections from both PERC H800 connectors on the DR4000 system (or the PERC H810 on a DR4100/DR6000 system) to the two SAS In ports on the EMM rear chassis of the Dell PowerVault MD1200.

If you plan on installing multiple expansion shelf enclosures, then the two SAS In ports on the rear chassis of the EMM on the additional enclosure are daisy-chained to the two SAS Out ports on the EMM rear chassis on the first enclosure. This is considered a redundant mode connection via the SAS In/Out connectors on the enclosures with the DR Series system appliance.

If you install multiple enclosures and cable them as described here, make sure to set the enclosure mode switch on the MD1200 front chassis to the top (unified mode) position. For more information, see *Dell PowerVault MD1200 and MD1220 Storage Enclosures Hardware Owner's Manual* at **support.dell.com/manuals**.

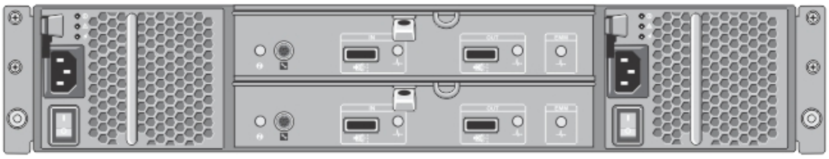


Figure 3. Dell PowerVault MD1200 Rear Chassis

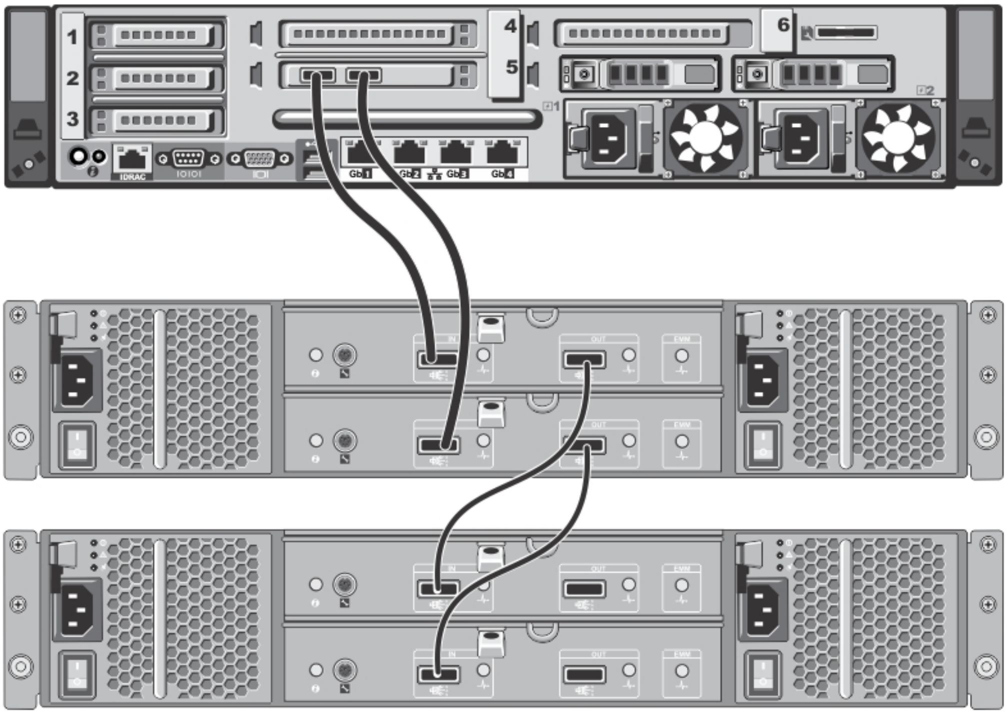


Figure 4. Unified Mode Daisy-Chained Redundant Path Dell PowerVault MD1200 Enclosures

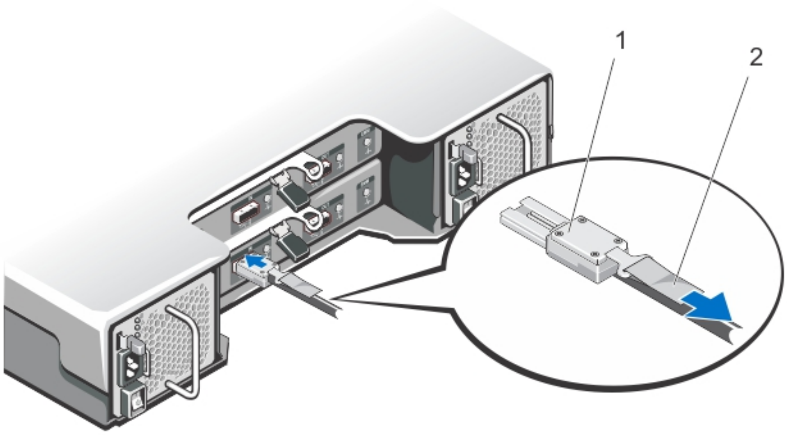


Figure 5. SAS Port and Cable Connections (Dell PowerVault MD1200 EMM)

1.	SAS cable	2.	pull-tab

Adding a DR Series System Expansion Shelf (DR4X00/DR6000)

To set up, add, and connect an expansion shelf correctly to the DR Series system (DR4X00/DR6000), you need to complete the following tasks.

- Power off the DR Series system.
- Install all cabling that connects the external expansion shelf (or shelves) to the DR Series system (For information, see the topic, DR Series System - Expansion Shelf Cabling).
- Power on the external expansion shelf (or shelves), and then
  power on the DR Series system.
- Install the Dell license for expansion shelf enclosures (for information, see Installing an Expansion Shelf License).
- In the DR Series system GUI, add and activate the expansion shelf enclosure on the **Storage** page (as described in the steps below).

To add an expansion shelf to the DR Series system, complete the following steps:

1. Click **Storage** in the navigation panel.

   The **Storage** page is displayed. (This step assumes that you have completed all expansion shelf enclosure cable connections and that green LEDs are displayed next to the fastplugs on the rear chassis, indicating that cable connections are active.)
2. In the Physical Storage pane, click **Add** in the **Configured** column of the Physical Storage summary table that corresponds to the enclosure you want to add (*Not Configured* is the displayed **State** for the enclosure).

   The **Enclosure Addition** dialog is displayed that indicates that all input-output to the system will be stopped during an enclosure addition, and prompts you to click **OK** to continue or click **Cancel** to stop this process.
3. Click **OK** to continue adding the enclosure to the DR Series system.
4. If you clicked **OK**, an **Enclosure Addition** dialog box is displayed that indicates this process may take up to 10 minutes to complete.

   A **System Status** dialog then displays with the following message: *The system is currently adding an enclosure. Please wait for this process to complete and the system to become operational.*

5. Once the previous step completes, to verify that an enclosure was added, click **Dashboard**→ **Health**.

   The **Health** page is displayed, and each properly cabled and activated expansion shelf enclosure has a corresponding tab that displays a green status check mark (for example, if you have installed two enclosures, two tabs are displayed: **Enclosure 1** and **Enclosure 2**).

   NOTE: If the **Enclosure** tab does not display a green status check mark, this indicates that there is an issue with the enclosure (such as it has not been properly connected or activated).

6. After adding an expansion shelf enclosure, make sure that you install an expansion shelf license.

   For more information, see Installing an Expansion Shelf License.

3

Setting Up the Physical DR Series System

You can interact with the physical DR Series system using one of two supported methods: a web-based graphical user interface (GUI) accessed using a web browser or a command line interface (CLI) using a terminal emulator application (for example, PuTTY). Before you can interact with your system, you must first, however, ensure that the DR Series system is properly set up.

NOTE: The topics in this section apply to physical DR Series systems. For information about setting up the virtual DR Series system, DR2000v, see the *Dell DR2000v Deployment Guide* for your specific VM platform and the *Dell DR Series System Interoperability Guide*. For more information on the DR Series system CLI commands, see the *Dell DR Series System Command Line Reference Guide*.

Refer to the following topics for information about setting up the DR Series system hardware.

Related Links

Interacting with the DR Series System
Connections for Initializing a DR Series System
Initializing the DR Series System
Accessing iDRAC6/iDRAC7 Using RACADM
Logging in Using a Web Interface

Interacting With the DR Series System

You interact with the DR Series system using its web-based graphical user interface (GUI) through a browser-based connection. The DR Series system GUI provides a single, comprehensive data management interface that lets you create new data containers, modify or delete existing containers, and perform a number of data-related operations using its features and settings.

NOTE: A second method for interacting with the DR Series system is by using its command-line interface (CLI) via a terminal emulator application (for example, PuTTY).

You can create and manage containers that are the repositories where you store your backup and deduplicated data. A data container is a shared file system that is imported using a client, and is accessible via file system protocols. For details, see Supported File System Protocols.

The DR Series system provides real-time summary tables, detail tables, and graphs that let you monitor the status of the data capacity, storage savings, and the throughput of the containers you are managing using its set of GUI features.

Networking Preparations for the DR Series System

Before you can start using the DR Series system, ensure that you have satisfied the following networking prerequisites:

- **Network:** An active network is available using Ethernet cables and connections.

  NOTE: If your DR Series system is equipped with a 1-GbE NIC, Dell recommends using CAT6 (or CAT6a) copper cabling. If your DR Series system is equipped with a 10-GbE NIC, Dell recommends using CAT6a copper cabling.

  NOTE: If your DR Series system is equipped with a 10-GbE enhanced small form-factor pluggable (SFP+) NIC, you must use Dell-supported SFP+ LC fiber-optic transceivers or twin-axial cabling.

- **IP Addresses:** You need to make sure to have IP addresses that you use for the DR Series system. The DR Series system ships with a default IP address and subnet mask address, which should only be used for an initial system configuration.

  NOTE: You need to have an IP address available to replace the default IP address if you choose the static mode of IP addressing, or select to use the DHCP mode of IP addressing.

  To perform an initial configuration, you need:

  – An IP address for the system

  – A subnet mask address

  – A default gateway address

  – A DNS suffix address

  – A primary DNS server IP address

  – (Optional) A secondary DNS server IP address
- **NIC Connections:** To configure NIC connection bonding remember that, by default, the DR Series system will configure its NIC interfaces together as a bonded team (and only one IP address is needed because the bonded NICs assume the primary interface address). NIC connection bonding can use either of these configurations:

  – Adaptive load balancing (ALB), which is the default setting, does not require any special network switch support. Ensure that the data source system resides on the same subnet as the DR Series system. For more information, see Configuring Networking Settings.

  – 802.3ad or dynamic link aggregation (using the IEEE 802.3ad standard). 802.3ad requires special switch configuration before using the system (contact your network administrator for an 802.3ad configuration).

  NOTE: To configure a 10-GbE NIC or 10-GbE SFP+ bonded configuration, connect only the 10-GbE/10-GbE SFP+ NICs. You can use the Advanced Networking feature in the command line interface to modify the default factory configuration.
- DNS: you need a DNS domain available, and you need to know the primary DNS server IP address (and a secondary DNS server IP address, if you choose to configure one).
- Replication ports: the replication service in the DR Series system requires that enabled fixed ports be configured to support replication operations that are to be performed across firewalls (TCP ports 9904, 9911, 9915, and 9916).

  For more information about replication ports, see Managing Replication Operations, and for more information about system ports, see Supported Ports in a DR Series System.

  NOTE: For the latest details about supported hardware and software for the Dell DR Series system, see the *Dell DR Series System Interoperability Guide* at **support.dell.com/manuals**.

Connections for Initializing a DR Series System

There are two supported methods for connecting to the DR Series system for logging in and performing the initial system configuration via the DR Series system CLI:

- **Local console connection**: this is a local access connection made between a local workstation and the DR Series system (with one connection made to a USB keyboard port on the DR Series front/rear chassis, and a second connection made to the VGA monitor port on the DR Series system rear chassis. (See Figure 3 for locations in the DR Series System Rear Chassis Port Locations in the Local Console Connection.)
- **iDRAC connection**: this is a remote access connection made between an integrated Dell Remote Access Controller (iDRAC) and the dedicated management port on the DR Series system rear chassis. (See Figure 3 for locations in the DR Series System Rear Chassis Port Locations in the Local Console Connection.)

Initializing the DR Series System

Before you can start using the DR Series system graphical user interface (GUI) for the first time, you must properly initialize the system. To initialize the DR Series system, complete the following:

1. Log in to the DR Series system CLI by using a local console KVM (keyboard-video monitor) connection or an iDRAC connection. For more information, see Local Console Connection, or iDRAC Connection.
2. Configure your system network settings using the **Initial System Configuration Wizard**. For more information, see Logging in and Initializing the DR Series System.

The **Initial System Configuration Wizard** lets you configure the following network settings to complete a first-time initialization of your system:

- IP addressing mode
- Subnet mask address
- Default gateway address
- DNS suffix address
- Primary DNS server IP address
- (Optional) Secondary DNS server IP address
- Host name for system

Default IP Address and Subnet Mask Address

This topic lists the following default address values that can be used for initialization of a DR Series system:

- IP address—10.77.88.99
- Subnet mask address—255.0.0.0

There are two key factors related to default address values and initializing a DR Series system:

- Using the local console
- Reserving MAC addresses using DHCP

If the network where the system will reside does not have or does not support DHCP, then the DR Series system can use the default IP (10.77.88.99) and subnet mask (255.0.0.0) addresses provided for initialization. If the network where the system will reside does not have or support reserving an IP address for the MAC address of the NICs in the DHCP server, then DHCP assigns an arbitrary IP address that is unknown (and which is unusable by you) during initialization.

As a result, if your network does not support DHCP or if you cannot reserve an IP address for the specific MAC addresses of the DHCP network interface cards (NICs), then Dell recommends that you use the local console connection method and the **Initial System Configuration Wizard**.

NOTE: After successfully initializing and configuring your system, you can modify the IP address to use either a static IP address or use dynamic IP addressing (DHCP), and modify the subnet mask address to be one that is supported by your network.

NOTE: If you have not run the **Initial System Configuration Wizard** on one (or more) DR Series system(s) being installed into the same network, there is a potential that the system (or systems) may come up with the same default IP address (10.77.88.99). The default IP address is not user-configurable and it can potentially result in becoming a duplicate IP address in the case of multiple systems.

Initialization issues could include when a network has had a network power outage, the DHCP server in the network is misconfigured, or if the **Initial System Configuration Wizard** has never been run.

If your network does not accept the default subnet mask address (255.0.0.0), you can establish a connection between the DR Series system and a laptop workstation. In this case, make sure that you connect using SSH, and use the default IP address to run the **Initial System Configuration Wizard**.

If you are using a known static IP address, you can skip running the **Initial System Configuration Wizard**, and directly configure the DR Series system using its user interface.

To configure the DR Series system, select **System Configuration** → **Networking**, and configure the network settings as desired. For more information, see Configuring Networking Settings.

NOTE: For details about logging in and using the **Initial System Configuration Wizard**, see Configuring Networking Settings.

Local Console Connection

To configure a local console connection, you must make the following two rear chassis cable connections:

- VGA port and your video monitor
- USB port and your keyboard

To make local console cable connections for the DR Series system appliance, complete the following:

1. (**DR4000 system**) Locate the VGA monitor port and the USB ports on the back of your system. See Figure 3 for the VGA and USB port locations and complete steps 1 to 4. For the DR4100/DR6000 system, skip to step 5.
2. Connect the video monitor to the VGA port on the back of your system (see item 1 in the DR4000 System Rear Chassis Port Locations table).
3. Connect the USB keyboard to one of the two USB ports on the back of your system (see item 3 in DR4000 System Rear Chassis Port Locations table).
4. You are now ready to perform initialization using the DR Series system CLI login process. For more information, see Logging in and Initializing the DR Series System.

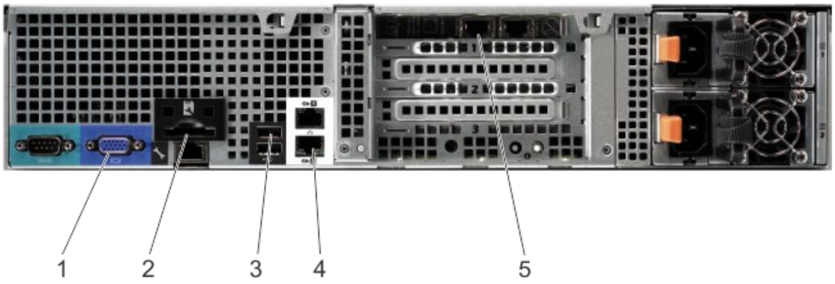


Figure 6. DR4000 System Rear Chassis Port Locations

Item	Indicator, Button, or Connector	Icon	Description
1	Video connector	IOI	Connects a VGA display to the system.
2	iDRAC6 Enterprise port	🔧	Dedicated management port for the iDRAC6 Enterprise card.
3	USB connectors (2)	⭠	Connects USB devices to the system. The ports are USB 2.0-compliant.
4	Ethernet connectors (2)	品	Embedded 10/100/1000 NIC connectors.

Item	Indicator, Button, or Connector	Icon	Description
5	Ethernet Connectors (2) on expansion card		1-GbE/10-GbE/10-GbE SFP+ Ethernet Port

To make local console cable connections for the DR4100 system appliance, complete the following:

> **NOTE:** For the 1–GbE ports, these are two internal LAN on Motherboard (LOM) ports referenced in item 4 above that reside on the motherboard, and two ports on an expansion card referenced in item 5 above. If the system is using the two 10–GbE ports, these reside on an expansion card referenced in item 5 above.

5. (**DR4100/DR6000 system**) Locate the VGA monitor port and the USB ports on the back of your system. See Figure 3 for the VGA and USB port locations and complete steps 5 to 8.
6. Connect the video monitor to the VGA port on the back of your system (see item 2 in the DR4100/DR6000 System Rear Chassis Port Locations table).
7. Connect the USB keyboard to one of the two USB ports on the back of your system (see item 3 in the DR4100/DR6000 System Rear Chassis Port Locations table).
8. You are now ready to perform initialization using the DR Series system CLI login process. For more information, see Logging in and Initializing the DR Series System.

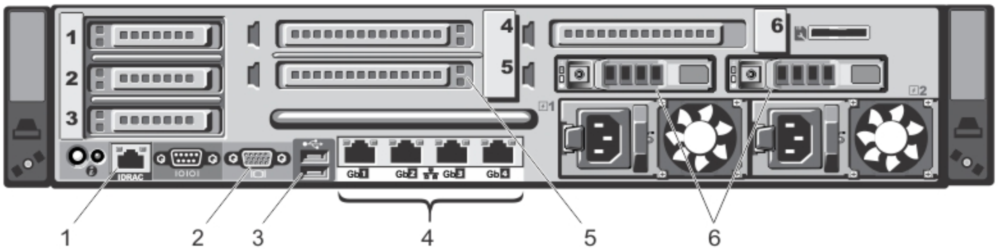


Figure 7. DR4100/DR6000 System Rear Chassis Port Locations

Item	Indicator, Button, or Connector	Icon	Description
1	iDRAC7 Enterprise port	🔧	Dedicated management port for the iDRAC7 Enterprise card (port is available only if an iDRAC7 Enterprise license is installed on your system).
2	Video connector	IOI	Connects a VGA display to the system.
3	USB connectors (2)		Connects USB devices to the system. The ports are USB 2.0-compliant.
4	Ethernet connectors (4)	🖧	Four integrated 10/100/1000 NIC connectors, or four integrated connectors that include: • Two 10/100/1000 Mbps NIC connectors • Two 100 Mbps/1 Gbps/10 Gbps SFP+/10-GbE T connectors
5	PCIe expansion card slots (3)		Connect up to three full-height PCI Express expansion cards
6	Hard drives (2)		Provides two hot-swappable 2.5-inch hard drives

NOTE: The DR4100/DR6000 system supports up to six 1–GbE ports or up to two 10–GbE ports. For the 1–GbE ports, these are four internal LAN on Motherboard (LOM) ports referenced in item 4 above that reside on the network daughter card (NDC), and two additional ports on a PCI Express expansion card referenced in item 5 above. If the system is using the two 10–GbE ports, these ports reside on the NDC.

iDRAC Connection

The iDRAC connection requires a network connection between the integrated Dell Remote Access Control (iDRAC) management port on the DR Series system and another computer running the iDRAC remote console session in a supported browser. The iDRAC provides remote console redirection, power control, and the out-of-band (OOB) system management functions for the DR Series system. iDRAC connections are configured using console redirection and the iDRAC6/7 web interface. The login values you can use for making iDRAC connections are:

- Default username: **root**
- Default password: **calvin**
- Default static IP address: **192.168.0.120**

For information on how to configure the iDRAC, see the Dell RACADM Reference Guides at **support.dell.com/manuals** and Accessing iDRAC6/iDRAC7 Using RACADM.

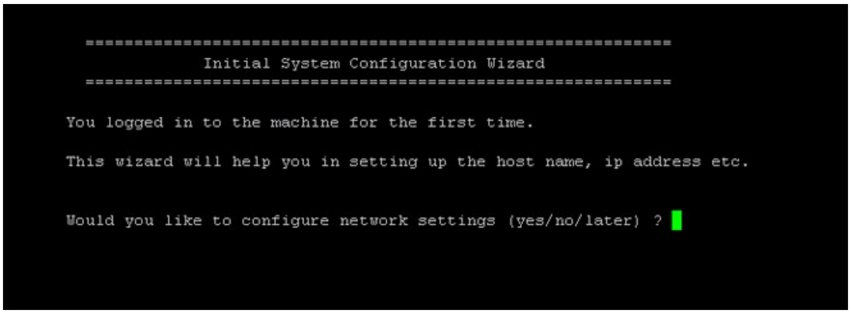
When the **Dell DR Series System** splash screen is displayed, you are ready to begin initialization using the DR Series system CLI login process. For more information, see Logging in and Initializing the DR Series System.

Logging in and Initializing the DR Series System

Use the DR Series system CLI and the **Initial System Configuration Wizard** to log in to and initialize the system. After completing a local console or iDRAC connection, log in to the DR Series system CLI:

1. Launch a terminal emulator application (like PuTTY), and type the default IP address for the DR Series system (if you are not using iDRAC or local console).
2. At the **login as:** prompt, type **administrator**, and press **<Enter>**.
3. At the **administrator@<system_name> password:** prompt, type the default administrator password (**St0r@ge!**), and press **<Enter>**.

   The **Initial System Configuration Wizard** window is displayed.



```
  ============================================================
              Initial System Configuration Wizard
  ============================================================

 You logged in to the machine for the first time.

 This wizard will help you in setting up the host name, ip address etc.


 Would you like to configure network settings (yes/no/later) ?
```

Figure 8. Initial System Configuration Wizard Window

4. To configure the network settings, type **y** (for yes), and press **<Enter>**.
5. To configure the use of the default IP address that ships with the system, choose to use static IP addressing.

   To do this, at the DHCP prompt, type **no** (this selects static IP addressing), and press **<Enter>**.

NOTE: When you select static IP addressing, you are prompted to type the static IP address (for example, you could use the default IP, 10.77.88.99) for the system, and press <**Enter**>. If your network supports the use of DHCP, type **yes** at the DHCP prompt, press <**Enter**>, and respond to any prompts.

6. To configure a subnet mask address, type the subnet mask address you want to use (for example, you could use the default subnet mask address, 255.0.0.0), and press <**Enter**>.
7. To configure a default gateway address, type the default gateway address you want to use (for example, 10.10.20.10), and press <**Enter**>.
8. To configure a DNS Suffix, type the DNS suffix you want to use (for example, storage.local), and press <**Enter**>.
9. To configure a primary DNS server IP address, type an IP address you want to use for the primary DNS server (for example, 10.10.10.10), and press <**Enter**>.
10. (Optional) To configure a secondary DNS server IP address, type **y** (for yes), and press <**Enter**>.

    If you responded **yes**, type an IP address you want to use for the secondary DNS server (for example, 10.10.10.11), and press <**Enter**>.
11. To change the default host name (for example, the serial number of the DR Series hardware appliance), type **y** (for yes) and press <**Enter**>.

    If you responded **yes**, type the host name you want to use, and press <**Enter**>. After you configure your host name response, the current system settings are displayed.
12. To accept these settings, type **y** (for yes), and press <**Enter**>.
13. If you want to change any of these settings, type **n** (for no), and press <**Enter**>. Modify the settings as needed, and press <**Enter**>.

    When completed, a successful initialization message is displayed.
14. At the prompt, type **exit** and press <**Enter**> to end the DR Series system CLI session.

You are now ready to log in to the system using the DR Series system GUI.

NOTE: Before you log into the system using the DR Series system GUI, make sure to register it in the local Domain Name System (DNS) for your network so that it is a DNS-resolvable entry.

NOTE: At this point, you could modify the bonding mode to use 802.3ad, if this configuration is available in your network.

Accessing iDRAC6/iDRAC7 Using RACADM

You can use SSH-based or Telnet-based interfaces to access iDRAC6/iDRAC7 using the RACADM utility. RACADM (remote access controller administration) is a Dell command-line utility that allows you to set up and configure the integrated Dell Remote Access Control (iDRAC) interface card to provide an out-of-band management capability.

The iDRAC card contains a controller with its own processor, memory, network connection, and access to the system bus. This gives system or network administrators the capability to configure a system as if they were sitting at the local console using the power management, virtual medial access and remote console capabilities, by using a supported web browser or command line interface.

The login values you can use for making iDRAC connections are:

- Default username: **root**
- Default password: **calvin**
- Default static IP address: **192.168.0.120**

For more information, see the *RACADM Reference Guides for iDRAC*, the *Integrated Dell Remote Access Controller 6 (iDRAC6) User Guide*, or the *Integrated Dell Remote Access Controller 7 (iDRAC7) User Guide* that are available at **support.dell.com/manuals**.

Logging in Using a Web Interface for the First Time

To log in to the DR Series system using a browser-based connection, complete the following:

1. In a supported web browser, type the IP address or hostname of the system in the browser **Address bar**, and press **<Enter>**.

   The **DR Series System Login** page is displayed.

   NOTE: The **DR Series System Login** page may display a warning message if the web browser you are using does not properly support the DR Series system. If you are running a Microsoft Internet Explorer (IE) web browser, make sure that you disable the **Compatibility View**. For more information about disabling the **Compatibility View** settings, see Disabling the Compatibility View Settings. For more information about the supported web browsers, see the *Dell DR Series System Interoperability Guide*.

   NOTE: For best results when using IE web browsers in combination with supported Windows-based servers, ensure that **Active Scripting** (JavaScript) is enabled on the Windows client. This setting is often disabled by default on Windows-based servers. For more information on enabling Active Scripting, see Enabling Active Scripting in Windows IE Browsers.

   NOTE: If you want to reset your login password, click **Reset Password** on the **DR Series System Login** page. The **Reset Password** dialog is displayed.

   The reset options displayed depend on the password reset option you configured earlier. For more information see, Modifying Password Reseting Options.
   By default, the service tag option is displayed. In **Service Tag**, enter the service tag number ID for the system, and click **Reset Password** to reset the system password back to its default setting (or click **Cancel** to return to the **DR Series System Login** page).

2. In **Password**, type **St0r@ge!** and click **Log in** or press **<Enter>**.

   The **Customer Registration and Notification** page is displayed. Before you can begin using the DR Series system graphical user interface (GUI), you need to properly register the system with Dell. In addition, this page also allows you to sign up for notifications about appliance alerts and system software updates. For more information, see Registering a DR Series System.

3. In the Settings pane of the **Customer Registration and Notification** page, complete the following:

   a. In **Contact Name**, enter a system contact name.
   b. In **Relay Host**, enter a hostname or IP address for the relay host.
   c. In **Email Address**, enter an email address for the contact.
   d. Select **Notify me of [DR Series] appliance alerts** to be notified about system appliance alerts.
   e. Select **Notify me of [DR Series] software updates** to be notified about system software updates.
   f. Select **Notify me of [DR Series] daily container statistics** to be notified about container statistics on a daily basis.
   g. Select **Don't show me this again** to not display the **Customer Registration and Notification** page again.
   h. Click **Confirm** to have the DR Series system accept your settings (or click **Skip** without configuring any settings) to proceed with initialization.

   The **Initial System Configuration Wizard** page is displayed.

4. To start the initial system configuration process, click **Yes**.

   The **Initial Configuration — Change Administrator Password** page is displayed.

   NOTE: If you click **No**, you will bypass the initial system configuration process, and the DR Series system **Dashboard** page is displayed. However, when you next log in to the DR Series system, you will be prompted to perform the initial system configuration process again with the **Initial System Configuration Wizard** page is displayed.

5. In the Settings pane of the **Initial Configuration — Change Administrator Password** page, complete the following:

   a. In **Current Password**, enter the current administrator password.

   b. In **New Password**, enter the new administrator password.

   c. In **Retype New Password**, enter the new administrator password again to confirm it.

   d. Click **Next** to continue with the initial configuration process (or click **Back** to return to the previous page, or click **Exit** to close the **Initial System Configuration Wizard**).

   The **Initial Configuration — Networking** page is displayed.

6. In the Settings pane of the **Initial Configuration — Networking** page, complete the following:

   a. In **Hostname**, enter a hostname that meets the hostname naming convention: A-Z, a-z, 0–9, the dash special character (-), within a maximum 19 character limit.

   b. In **IP Address**, select the **Static** or **DHCP** mode of IP addressing, and if planning to use a **Secondary DNS**, enter an IP address for the secondary domain name system.

   c. In **Bonding**, select the **Mode** choice from the drop-down list (ALB or 802.3ad).

   Dell recommends that you verify the system can accept your bonding selection type. The connection will be lost unless it is correctly configured. For more information, see Configuring Networking Settings.

   d. In **Bonding**, enter the **MTU** value for the maximum transmission unit (the MTU accepts values between 512 and 9000). For more information, see Configuring Networking Settings.

   e. In **Active Directory**, enter a fully qualified domain name for the Active Directory Services (ADS) domain in **Domain Name (FQDN)**, enter an organization name in **Org Unit**, enter a valid ADS username in **Username**, and enter a valid ADS password in **Password**.

   For more information, see Configuring Active Directory Settings.

   NOTE: If an ADS domain has already been configured, you will not be allowed to change the values for the **Hostname** or **IP Address** settings.

   f. Click **Next** to continue with the initial configuration process (or click **Back** to return to the previous page, or click **Exit** to close the **Initial System Configuration Wizard**).

   The **Initial Configuration — Date and Time** page is displayed.

   NOTE: If the Microsoft Active Directory Services (ADS) domain has already been configured, the **Initial Configuration — Date and Time** page will not display.

7. In the Settings pane, select the **Mode** choice (**NTP** or **Manual**).

   a. If you select **NTP**, accept or revise the NTP servers as desired (you are limited to only three NTP servers), and in **Time Zone**, select the desired time zone from the drop-down list.

   b. If you select **Manual**, in **Time Zone**, select the desired time zone from the drop-down list, click the **Calendar** icon and select the desired day in the month, and adjust the **Hour** and **Minute** sliders to the desired time (or click **Now** to choose the current date and time), and click **Done**.

   c. Click **Next** to continue with the initial configuration process (or click **Back** to return to the previous page, or click **Exit** to close the **Initial System Configuration Wizard**)

   For more information, see Configuring System Date and Time Settings.

   NOTE: Dell recommends using NTP when the DR Series system is part of a workgroup and not part of an domain. When the DR Series system is joined to a domain, such as the Microsoft Active Directory Services (ADS) domain, NTP is disabled.

   The **Initial Configuration — Summary** page is displayed.

8. The **Initial Configuration — Summary** page displays a summary of all of the initial configuration changes you have made. Click **Finish** to complete the **Initial System Configuration Wizard** (or click **Back** to return to a previous page to change a setting).

   The **Initial Software Upgrade** page is displayed and prompts you to verify the current installed system software version.

9. Click **Dashboard** in the navigation panel.

   The DR Series system main window consists of the following components:

- Navigation panel
- System Status bar
- System Information pane
- Command bar

Your login username is displayed at the top of the page. If you are logged in as a domain user, the domain is displayed in the format of domain\username. (You can only log in as a domain user after configuring Login Groups under Active Directory. This is a requirement for using Global View.)

NOTE: You can display the Help system documentation by clicking **Help**, or log out of the system by clicking **Log out** at the top right of any page.

NOTE: When logged in, a **Logout Confirmation** dialog is displayed after 45 minutes of non-use. This dialog displays for 30 seconds before the DR Series system performs a forced timeout. Click **Continue** to reset the 45-minute logout timer. If you do not click **Continue** before the 30-second interval elapses, the DR Series system logs you out. You must log in again to resume using the DR Series system features and GUI.

Registering a DR Series System

Before you can start using the DR Series system using its graphical user interface (GUI) for the first time, you must properly register the system with Dell by completing the **Customer Registration and Notification** page. The **Customer Registration and Notification** page is displayed when you initially log into a DR Series system using a web interface connection, and it consists of the following text boxes and check boxes in the Settings pane:

- **Contact Name**
- **Relay Host**
- **Email Address**
- **Notify me of [DR Series] appliance alerts**. If this check box is selected, you are notified of all warning and critical severity system alerts, which are the types that may require user action. For more information, see Displaying System Alerts.
- **Notify me of [DR Series] software updates**. If this check box is selected, you are notified by Dell about any new system software upgrades or maintenance releases.
- **Notify me of [DR Series] daily container stats reports**. If this check box is selected, you are notified by Dell about your container statistics on a daily basis. For more information, see Displaying Container Statistics.
- **Don't show me this again**

To register a DR Series system:

1. In **Contact Name**, enter the name of the DR Series system contact.
2. In **Relay Host**, enter the hostname or IP address for the DR Series system email relay host.
3. In **Email Address**, enter an email address for the system contact.
4. To be notified about DR Series system appliance alerts, select the **Notify me of [DR Series] appliance alerts** check box.
5. To be notified about DR Series system software updates, select the **Notify me of [DR Series] software updates** check box.
6. To be notified about DR Series system container statistics on a daily basis, select the **Notify me of [DR Series] daily container statistics** check box.
7. To not display the **Customer Registration and Notification** page again, select the **Don't show me this again** check box.
8. Click **Confirm** for the DR Series system to accept your values (or click **Skip**) to proceed to the **Initial System Configuration Wizard** page.

Enabling Active Scripting in Windows IE Browsers

To enable **Active Scripting** (JavaScript) in Microsoft Windows Internet Explorer (IE) web browsers, complete the following:

NOTE: This procedure describes how to configure your Windows IE web browser to enable **Active Scripting** (JavaScript). This setting is often disabled by default on Windows-based servers

1. Launch the IE web browser, and click **Tools→ Internet Options**.

   The **Internet Options** page is displayed.
2. Click the **Security** tab, and click **Custom level...**.

   The **Security Settings — Local Intranet Zone** page is displayed.
3. Using the right scroll bar, scroll down the **Settings** choices until you reach **Scripting**.
4. In **Active scripting**, click **Enable**.
5. Click **OK** to enable JavaScript and the Active Scripting feature for your web browser.

   The **Internet Options** page is displayed.
6. Click **OK** to close the **Internet Options** page.

Disabling the Compatibility View Settings

To disable the **Compatibility View** settings of the IE web browser you are using to log in to access the DR Series system graphic user interface (GUI), complete the following:

NOTE: This procedure describes how to disable the **Compatibility View** settings to ensure there is no conflict between different versions of the Microsoft Internet Explorer (IE) web browser you use to access the DR Series system. Disabling the compatibility view settings requires that the **Display all websites in Compatibility View** check box option in the **Compatibility View Settings** page remains unselected, and that there are no DR Series systems or domains associated with these systems listed in the Compatibility View list on this page.

1. Launch the IE web browser, and click **Tools→ Compatibility View settings**.

   The **Compatibility View Settings** page is displayed.
2. If selected, deselect the **Display all websites in Compatibility View** check box option.
3. If any DR Series systems are listed in the Compatibility View list, select the entry and click **Remove**.

   Repeat this step for any additional DR Series systems that are listed.
4. Click **Close** to exit from the **Compatibility View Settings** page.

4

Configuring the DR Series System Settings

This topic introduces the concept that before you can run any DR Series system operations, you first need to understand the following key tasks:

- How to initialize the system
- How to shut down or reboot the system
- How to manage the system password

Initializing the DR Series system requires that you configure and manage a number of very important system settings.

NOTE: Dell recommends that you use the **Initial System Configuration Wizard** to configure your DR Series system. Changing some of the system settings using the DR Series system GUI (such as bonding, MTU, hostname, IP address, and DNS) can cause issues that may affect your DR Series system GUI access.

For more information about initializing the system, see Initializing the DR Series System.

For more information about shutting down or rebooting the system, see Shutting Down the DR Series System and Rebooting the DR Series System.

For more information about managing the system password, see Managing the DR Series System Password.

Configuring Networking Settings

You can configure the networking settings that were configured using the **Initial System Configuration Wizard** process for the DR Series system in the following tabs:

NOTE: For the Ethernet port settings on the NICs, this example only shows Eth0 and Eth1 (depending upon your system configuration, you could have NICs configured with Ethernet port settings in the Eth0–Eth5 range). For more information, see Local Console Connection.

- **Hostname**
  - Hostname (FQDN)
  - iDRAC IP Address
- **DNS**
  - Domain Suffix
  - Primary DNS
  - Secondary DNS
- **Interfaces**
  - Device
  - Mode
  - MAC Address
  - MTU (maximum transmission unit)
  - Bonding Option

  - Slave Interfaces
- Eth0
  - MAC
  - Maximum Speed
  - Speed
  - Duplex
- Eth1
  - MAC
  - Maximum Speed
  - Speed
  - Duplex

To configure new networking settings (or to change from those set using the **Initial System Configuration Wizard**), complete the following:

1. Select **System Configuration → Networking**.

   The **Networking** page is displayed. Select settings for hostname, IP Address, DNS, Bonding, or to view the Ethernet port settings (Eth0-Eth3) for the DR Series system.

   - To configure hostname, skip to step 2.
   - To configure IP addressing, skip to step 5.
   - To configure DNS, skip to step 10.
2. To change the current Hostname, select the **Hostname** tab and click **Edit Hostname** on the options bar.

   The **Edit Hostname** dialog is displayed.
3. Type a hostname in **Hostname** that meets the following supported character types and length:
   - Alphabetic—allows A-Z, a-z, or a combination of upper and lower case alphabetic characters.
   - Numeric—allows numerals zero (0) through 9.
   - Special characters—allows only the dash (-) character.
   - Length limit—hostnames cannot exceed the maximum length of 19 characters.
4. Click **Submit** to set the new hostname for your system.
5. To change the current IP address settings for the selected NIC bond or Ethernet port, select the **Interfaces** tab and click **Edit Interfaces** on the options bar.

   The **Edit Interface — <bond or Ethernet port number>** dialog is displayed.
6. Under **IP Address**, in **Mode**, select **Static** (to set static IP addressing for your system), or select **DHCP** (to set dynamic IP addressing for your system).

   NOTE: To select the **DHCP** mode of IP addressing, select **DHCP**, and click **Submit**. The remaining substeps in this step only need to be completed if you selected the **Static** mode of IP addressing for the DR Series system.

   a. In **New IP Address**, type an IP address that represents the new IP address for your system.
   b. In **Netmask**, type an netmask address value that represents your system (the system IP address and netmask identify the network to which your system belongs).
   c. In **Gateway**, type an IP address for the gateway associated with your system.
7. Under **MTU**, in **MTU**, enter the value you want to set as the maximum.

NOTE: Ensure that the value that you enter in MTU is the same for the clients, Ethernet Switch, and the appliance. The connection between the clients, the Ethernet switches, and the appliance will break if the MTU number is not the same on all the components.

NOTE: In computer networking, jumbo frames are Ethernet frames with more than 1500 bytes of payload (but in some cases, jumbo frames can carry up to 9000 bytes of payload). Many Gigabit Ethernet switches and Gigabit Ethernet network interface cards support jumbo frames. Some Fast Ethernet switches and Fast Ethernet network interface cards also support jumbo frames.

Some computer manufacturers use 9000 bytes as the conventional limit for jumbo frame sizes. To support jumbo frames used in an Internet Protocol subnetwork, both the host DR Series system (initiator or source) and the target DR Series system have to be configured for 9000 MTU.

Consequently, interfaces using a standard frame size and those using the jumbo frame size should not be in the same subnet. To reduce the chance of interoperability issues, network interface cards capable of supporting jumbo frames require specific configurations to use jumbo frames.

To verify that the destination system can support a specific frame size, use the DR Series system CLI command **network --ping --destination <IP address> --size <number of bytes>**.

For more information, contact Dell Support for assistance (for details, see Contacting Dell).

NOTE: Make sure that if you are using any Dell network switches that you take full advantage of the latest switch firmware upgrades and application notes. The application notes provide procedures that assist you in performing switch firmware upgrades and saving configuration files (for complete details, see **support.dell.com/** and navigate to **Drivers and Downloads** for your system type).

NOTE: When setting or changing the MTU value, make sure that you verify that the Ethernet network switch is capable of supporting an MTU size that is equal to or larger than the value you are setting. Any mismatch in MTU values between the clients, Ethernet network switch, and the DR Series system appliance will make it inoperable.

Dell suggests that you observe standard best practices when deploying jumbo frames in networks, and recommends using jumbo frames with the DR Series system because this frame size typically provides the best performance. However, for networks that do not support jumbo frames, the DR Series system also supports using the standard frame size.

8. Under **Bonding**, from the **Bonding configuration** list, select the appropriate bonding configuration.

   NOTE: You may lose the connection to the system if you change the bonding configuration. Change the bonding configuration only if the system accepts the new bonding type.

   - **ALB**—Configures adaptive load balancing (ALB), which is the default setting.

     NOTE: ALB load balancing does not balance the load properly when your backup servers are on a remote subnet. This is because ALB uses the address resolution protocol (ARP) and ARP updates are subnet-specific. Because this is the case, ARP broadcasts and updates are not sent across the router. Instead, all traffic is sent to the first interface in the bond. To resolve this ARP-specific issue, make sure that your data source systems reside on the same subnet as the DR Series system.

   - **802.3ad**—Configures dynamic link aggregation using the IEEE 802.ad standard.

     CAUTION: If you change the existing bonding setting, the connection to the DR Series system may be lost unless you are sure that the system can accept this bonding type.

9. Click **Submit** to have the DR Series system accept the new values (or click **Cancel** to display the **Networking** page).

   The **Updated IP Address** dialog is displayed when the selection is successful (if you change the static IP address manually, you need to use this IP address in the browser when you log back into the DR Series system).

10. To configure **DNS** settings for your system, select the **DNS** tab and click **Edit DNS** on the options bar.

    The **Edit DNS** dialog is displayed.

11. In **Domain Suffix**, type a domain suffix to use.

    For example, `acme.local`. This is a required field.

12. In **Primary DNS**, type an IP address that represents the primary DNS server for your system; this is a required field.
13. For **Secondary DNS**, type an IP address that represents the secondary DNS server for your system; this is an optional field.
14. Click **Submit** to have the DR Series system accept the new values (or click **Cancel** to display the **Networking** page).

    The **Updated DNS** dialog is displayed when the selection is successful.

Networking Page and Ethernet Port Values

The **Networking** page displays the currently configured multiple Ethernet ports for the DR Series system in a series of panes. For 1–Gigabit Ethernet (GbE) ports in the DR4000 system this could be Eth0, Eth1, Eth2, and Eth3, and in the DR4100 system this could be Eth0, Eth1, Eth2, Eth3, Eth4, and Eth5. For 10-GbE/10-GbE SFP+ NICs, this means that the two ports are bonded together into a single interface. For example, the DR Series system port configuration is as follows:

- In a 1-GbE NIC configuration: the DR4000 system supports up to four 1–GbE ports, which consists of up to two internal LAN on Motherboard (LOM) ports and two ports on an expansion card that are bonded together. The DR4100 system supports up to six 1–GbE ports, which consists of up to four internal LOM ports on the network daughter card (NDC) and two ports on a PCI Express expansion card.
- In a 10-GbE or 10-GbE SFP+NIC configuration: the DR4000 system supports up to two 10–GbE or 10–GbE SFP+ ports on an expansion card that are bonded together. The DR4100 system supports up to two 10-GbE or 10-GbE SFP+ ports that reside on the NDC that are bonded together.

NOTE: For more information on advanced networking options see the Command Line Interface Guide available at **dell.com/support/manuals**.

The ports for bonded NICs display: MAC address, port speed in megabtyes per second (MB/s), maximum speed, and duplex setting. The following example shows Ethernet port values for the four ports in a 1-GbE NIC bonded configuration on a DR4000 system:

Eth0:

- MAC: 00:30:59:9A:00:96
- Speed: 1000Mb/s
- Max Speed: 1000baseT/Full
- Duplex: Full

Eth1:

- MAC: 00:30:59:9A:00:97
- Speed: 1000Mb/s
- Max Speed: 1000baseT/Full
- Duplex: Full

Eth2:

- MAC: 00:30:59:9A:00:98
- Speed: 1000Mb/s
- Max Speed: 1000baseT/Full
- Duplex: Full

Eth3:

- MAC: 00:30:59:9A:00:99
- Speed: 1000Mb/s
- Max Speed: 1000baseT/Full
- Duplex: Full

Managing the DR Series System Password

You can manage the login password that is used when logging in to the DR Series system in two ways:

- By modifying the existing login password using the **Edit Password** option in the **System Configuration** page. For more information, see Modifying the System Password.
- By resetting the login password to its default value using the **Reset Password** option in the **DR Series System Login** page. For more information, see Resetting the Default System Password.

Modifying the System Password

To configure a new password or to modify an existing password for logging in to the DR Series system, complete the following:

1. To change the system password, do one of the following:.
   - In the navigation panel, select **System Configuration**, the **System Configuration** page is displayed. Click **Password Management**.
   - In the navigation panel, select **System Configuration** → **Password**, the **Password Management** page is displayed.
2. Click **Edit Password**.

   The **Edit Password** dialog is displayed.
3. In **Current password**, type the current password for the system.
4. In **New password**, type the new system password.
5. In **Confirm password**, retype the new password to confirm this as the new password replacing the existing system password.
6. Click **Change Password** (or click **Cancel** to display the **System Configuration** page).

   If successful, a **Password change was successful** dialog is displayed.

Resetting the Default System Password

To reset the system to use the default password (**St0r@ge!**) for logging in, complete the following:

1. In the **Login** window, click **Reset Password**.

   The **Reset Password** dialog is displayed.

   If the password reset option is set to **Service Tag**, proceed to step 2.

   If the password reset option is set to **Service Tag and Administrator Email**, proceed to step 4.
2. In **Service Tag**, type the Service Tag associated with your system, and click **Reset Password**.

   NOTE: If you are unsure of the Service Tag associated with your DR Series system, it can be found on the **Support** page (click **Support** in the navigation panel to display the Support Information pane, which displays the Service Tag).

   The **Login** window is displayed, and a **Password has been reset** dialog is displayed.

3. To log in using the default password, type **St0r@ge!** , and click **Login**.

   NOTE: After you have reset the login password to its default and logged in to the DR Series system, Dell recommends for security reasons that you create a new unique login password.

4. In **Service Tag**, type the Service Tag associated with your system.

   NOTE: If you are unsure of the Service Tag associated with your DR Series system, it can be found on the **Support** page (click **Support** in the navigation panel to display the Support Information pane, which displays the Service Tag).

5. In **Administrator Email** enter the email address of the administrator of this system.

   The **Administrator Email** that you enter must match the administrator email address configured in the DR Series system. If you have set security questions, the security questions are displayed.

6. Enter the answers to the configured security questions in **Answer 1** and **Answer 2**.
7. Click **Send Now**.

   An email with a unique code, used to reset the password, is sent only to the configured administrator email address. The code is valid for only 15 minutes. The password reset code expires after 15 minutes and cannot be used. You must repeat the password reset procedure to regenerate the code again.

Shutting Down the DR Series System

If needed, you can shut down the DR Series system by selecting **Shutdown** in the **System Configuration** page. However, you should fully understand what this action means to system operations before attempting to shut down the system.

CAUTION: Shutdown powers Off the appliance on which the DR Series system software is installed. Once powered Off, you can only power it On again at its physical location, or you must use an iDRAC connection to the DR Series system.

NOTE: To shutdown the DR Series system using a UPS after a power loss, refer to the following article for information on how to do this using the shutdown command in the IPMI interface: http://www.dell.com/downloads/global/power/ps4q04-20040204-murphy.pdf.

To shutdown your DR Series system, complete the following:

1. In the navigation panel, select **System Configuration**.

   The **System Configuration** page is displayed.

2. Click **Shutdown** on the **System Configuration** page options bar.

   The **Shutdown confirmation** dialog is displayed.

3. Click **Shutdown System** to proceed with shutting down the system (or click **Cancel** to return to the **System Configuration** page).

Rebooting the DR Series System

If needed, you can reboot the DR Series system by selecting the **Reboot** option in the **System Configuration** page. To reboot your system:

1. In the navigation panel, select **System Configuration**.

   The **System Configuration** page is displayed.

2. Click **Reboot** on the **System Configuration** page options bar.

   The **Reboot System** confirmation dialog is displayed.

3. Click **Reboot System** to proceed with rebooting the system (or click **Cancel** to return to the **System Configuration** page).

The **System has successfully rebooted** dialog is displayed after rebooting (system reboot may take up to 10 minutes to complete).

Configuring Active Directory Settings

You need to configure the Active Directory setting to direct your DR Series system to join or leave a domain that contains a Microsoft Active Directory Service (ADS). To join an ADS domain, complete steps 1 through 4 in the following procedure (to leave an ADS domain, skip to step 5). When you join the DR Series system to an ADS domain, this disables the Network Time Protocol (NTP) service and instead uses the domain-based time service.

NOTE: If you use the command line interface (CLI) to join the DR Series system into the domain, you might notice that Global View contains multiple, unnecessary entries. Dell recommends that you use the DR Series system GUI (and not CLI commands) for Global View related operations, including domain join/leave.

To configure the DR Series system for a domain using ADS, complete the following:

1. Select **System Configuration** → **Active Directory**.

   The **Active Directory** page is displayed.

   NOTE: If you have not yet configured ADS settings, an informational message is displayed in the **Settings** pane in the **Active Directory** page.
2. Click **Join** on the options bar.

   The **Active Directory Configuration** dialog is displayed.
3. Type the following values in the **Active Directory Configuration** dialog:

   - In **Domain Name (FQDN)**, type a fully qualified domain name for the ADS; for example, **AD12.acme.com**. *(This is a required field.)*

     NOTE: Supported domain names are limited to 64 characters in length and can only consist of a combination of A-Z, a-z, 0-9, and three special characters: a dash (-), a period (.), and an underscore (_).
   - In **Username**, type a valid user name that meets the user name guidelines for the ADS. *(This is a required field.)*

     NOTE: Supported user names are limited to 64 characters in length and can only consist of a combination of A-Z, a-z, 0-9, and three special characters: a dash (-), a period (.), and an underscore (_).
   - In **Password**, type a valid password that meets the password guidelines for the ADS. *(This is a required field.)*
   - In **Org Unit**, type a valid organizational name that meets the organization name guidelines for the ADS. *(This is an optional field.)*
4. Click **Join Domain** to configure your system with these ADS settings (or click **Cancel** to display the **Active Directory** page).

   The **Successfully Configured** dialog is displayed when successful.

   NOTE: If you configure CIFS container share paths, these will be displayed in a CIFS Container Share Path pane in the **Active Directory** page.
5. To leave an ADS domain, click **Leave** in the **Active Directory** page.

   The **Active Directory Configuration** dialog is displayed.
6. Leaving the configured ADS domain requires that you enter the following:

   a. In **Username**, enter a valid user name for the ADS domain.

   b. In **Password**, enter a valid password for the ADS domain.
7. Click **Leave Domain** to direct your DR Series system to leave the ADS domain (or click **Cancel** to display the **Active Directory** page).

   The **Successfully Configured** dialog is displayed when successful.

Configuring Local Workgroup Users Settings

You need to configure settings to create a local workgroup of CIFS authenticated users. This capability lets you create a local workgroup (Local Workgroup Users) to which you can add new users, edit existing users, or delete users from the workgroup.

To configure the DR Series system for a Local Workgroup Users, complete the following:

1. Select **System Configuration** → **Local Workgroup Users**.

   The **Local Workgroup Users (CIFS)** page is displayed.

2. To create a new CIFS user in this local workgroup of users, click **Create** on the option bar.

   The **Create a local workgroup user for CIFS authentication** dialog is displayed.

   a. In **User Name**, enter a valid user name for this user.
   b. In **Password**, enter a valid password for this user.
   c. Click **Add CIFS User** to create the new user in the Local Workgroup Users for the system (or click **Cancel** to return to the **Local Workgroup Users (CIFS)** page).

   An **Added CIFS user** confirmation dialog is displayed when successful.

3. To edit an existing CIFS user in this local workgroup of users, click **Select** to identify the user in the Local Workgroup Users summary table that you want to modify, and click **Edit** in the option bar.

   The **Edit a local workgroup user for CIFS authentication** dialog is displayed.

   a. In **Password**, enter a different valid password for this user.

      You cannot modify the **User Name** for this user, you can only modify the **Password**. If you want a user with a different **User Name**, you must delete this user and create a new user with the desired **User Name**.

   b. Click **Edit CIFS User** to modify the password for existing user in the Local Workgroup Users for the system (or click **Cancel** to return to the **Local Workgroup Users (CIFS)** page).

4. To delete an existing CIFS user from the local workgroup of users, click **Select** to identify the user in the Local Workgroup Users summary table that you want to delete, and click **Delete** in the option bar.

   The **Delete user** confirmation dialog is displayed.

   a. Click **OK** to delete the selected user from the Local Workgroup Users summary table (or click **Cancel** to return to the **Local Workgroup Users (CIFS)** page).

   A **Deleted CIFS user** confirmation dialog is displayed when successful.

Configuring Email Alert Settings

You can create and manage recipient email addresses for users to which you want to send DR Series system email alerts. The **Email Alerts** page contains options that let you add new, edit or delete existing recipient email addresses, and send a test message to the recipient email addresses listed in the **Recipient Email Address** pane.

NOTE: The **Email Alerts** page contains all the options you need for managing the recipient email addresses and testing the send message capability.

Adding a Recipient Email Address

To configure and add a new recipient email address, complete the following:

1. Select **System Configuration** → **Email Alerts.**

   The **Email Alerts** page is displayed.

2. Click **Add** on the options bar.

   The **Add Recipient Email Address** dialog is displayed.

3. In **Email Address**, type a valid email address using the address format that your email system supports.
4. Click **Submit** to configure the recipient email address (or click **Cancel** to display the **Email Alerts** page).

   The **Email Alerts** page is displayed, and an **Added email recipient** dialog is displayed when successful.
5. To create additional recipient email addresses, repeat steps 2 through 4.

NOTE: For information about sending an email alerts message to test one or more email recipients, see Sending a Test Message.

Editing or Deleting a Recipient Email Address

To edit or delete an existing recipient email address:

1. Select **System Configuration→ Email Alerts**.

   The **Email Alerts** page is displayed.

   NOTE: To edit or delete an existing recipient email address, you must first click **Select** in the Recipient Email Address pane to indicate the address that you want to edit or delete. To edit an existing email address, proceed to step 2, or to delete an existing email address, skip to step 4. For more information about adding email recipients, see Adding a Recipient Email Address.
2. To edit an existing recipient email address, click **Select** to indicate the recipient email address entry that you want to change, and click **Edit** on the options bar.

   The **Edit Recipient Email Address** dialog is displayed.
3. Modify the existing email address you selected as needed, and click **Submit**.

   The **Email Alerts** page is displayed, and a **Successfully updated email recipient** dialog is displayed when successful. To edit additional recipient email addresses, repeat steps 2 and 3.
4. To delete an existing recipient email address, click **Select** to indicate the recipient email address entry that you want to delete, and click **Delete** on the options bar.

   The **Delete Confirmation** dialog is displayed.
5. Click **OK** to delete the selected email recipient address (or click **Cancel** to display the **Email Alerts** page).

   The **Email Alerts** page is displayed, and a **Deleted email recipient** dialog is displayed when successful. To delete additional recipient email addresses, repeat steps 4 and 5.

Sending a Test Message

The DR Series system provides the means for sending test messages to all configured recipient email addresses. This process lets you manage the sending of system alert messages, at which point you can verify that all of the configured email recipients received these messages.

NOTE: If needed, ensure that you have a configured email relay host. For more information about email relay hosts, see Adding an Email Relay Host.

1. Select **System Configuration → Email Alerts**.

   The **Email Alerts** page is displayed.
2. Click **Send Test Message** on the options bar.

   The **Send Test Email** confirmation dialog is displayed.
3. Click **OK** (or click **Cancel** to display the **Email Alerts** page).

   The **Email Alerts** page is displayed, and a **Successfully sent email** dialog is displayed when successful.
4. Verify that all of the intended recipient email addresses received the test email.

Configuring Administrator Contact Information

You can configure the administrator contact information to identify the person who is actively managing or responsible for your DR Series system acting as its administrator. To do this, enter contact information for the administrator on the **Administrator Contact Information** page using the **Edit Contact Information** option.

In the navigation panel on the **Dashboard** page, click **System Configuration** → **Admin Contact Info** to display the **Administrator Contact Information** page.

For more information about contact information for the administrator, see Editing Administrator Contact Information, and Adding Administrator Contact Information.

The following information categories are displayed in the **Contact Information** and **Notification** panes on the **Administrator Contact Information** page, and this is information sent with all system alert emails:

- Contact Information
  - Administrator Name
  - Company Name
  - Email
  - Work Phone
  - Comments
- Notification
  - Status of **Notify me of [DR Series] appliance alerts** check box (enabled or disabled)
  - Status of **Notify me of [DR Series] software updates** check box (enabled or disabled)
  - Status of **Notify me of [DR Series] daily container statistics** check box (enabled or disabled)

Adding Administrator Contact Information

To configure contact information for the system administrator, complete the following:

1. Select **System Configuration** → **Admin Contact Info**.

   The **Administrator Contact Information** page is displayed.
2. Click **Add Contact Information** on the options bar.

   The **Add Administrator Contact Information** dialog is displayed.
3. In **Administrator Name**, type the name of the administrator for this appliance.
4. In **Company Name**, type the company name associated with the administrator.
5. In **Email**, type the email address of the administrator (using the email address format that your email system supports).
6. In **Work Phone**, type the telephone number associated with the administrator.
7. In **Comments**, type some information or add comments that uniquely identify this administrator.
8. Click the **Notify me of [DR Series] appliance alerts** check box to be notified about system alerts.
9. Click the **Notify me of [DR Series] software updates** check box to be notified about system software updates.
10. Click the **Notify me of [DR Series] daily container statistics** check box to receive your container statistics summary report on a daily basis.
11. Click **Submit** (or click **Cancel** to display the **Administrator Contact Information** page).

    The **Administrator Contact Information** page is displayed, and an **Updated administrator contact information** dialog is displayed when successful.

Editing Administrator Contact Information

To edit the contact information for an existing system administrator, complete the following:

1. Select **System Configuration→ Admin Contact Info**.

   The **Administrator Contact Information** page is displayed.
2. Click **Edit Contact Info** on the options bar.

   The **Edit Administrator Contact Information** dialog is displayed.
3. Modify the notification selections as needed.
4. Click **Submit**.

   The **Administrator Contact Information** page is displayed, and an **Updated administrator contact information** dialog is displayed when successful.

Managing Passwords

You can edit the system password and system password reset configuration on this page.

Modifying the System Password

To configure a new password or to modify an existing password for logging in to the DR Series system, complete the following:

1. To change the system password, do one of the following:.

   - In the navigation panel, select **System Configuration**, the **System Configuration** page is displayed. Click **Password Management**.
   - In the navigation panel, select **System Configuration → Password**, the **Password Management** page is displayed.
2. Click **Edit Password**.

   The **Edit Password** dialog is displayed.
3. In **Current password**, type the current password for the system.
4. In **New password**, type the new system password.
5. In **Confirm password**, retype the new password to confirm this as the new password replacing the existing system password.
6. Click **Change Password** (or click **Cancel** to display the **System Configuration** page).

   If successful, a **Password change was successful** dialog is displayed.

Modifying Password Reset Options

To modify the password reset options:

1. Select **System Configuration → Password.**

   The **Password Management** page is displayed.
2. Click **Edit Password Reset Options**.

   The **Edit Password Reset Options** dialog is displayed.
3. To use service tag only, select **Service Tag Only** and click **Submit**.

   NOTE: To select the option **Service Tag and Administrator Email**, you must first configure the e-mail relay host and administrator contact e-mail.

4. To use the service tag and administrator e-mail, select **Service Tag and Administrator Email**.

   The optional security questions area is displayed.
5. To set the optional security questions, under **Optional Security Question 1** and **Optional Security Question 2** in **Question** enter the security question.
6. In **Answer** , enter the answer to your security question.

   NOTE: Save the answer in a secure location, you will need these answers to reset the DR Series system password.
7. Click **Submit**.

Configuring an Email Relay Host

If needed, you can configure an external email relay host to serve your DR Series system if the network email system requires one. The email relay host is typically an external mail server that relays any email alerts from the DR Series system to each of the designated recipient email addresses.

To do this on the **Email Relay Host** page, click **Add Relay Host** to define a new email relay host (or to edit an existing email relay host, click the **Edit Relay Host**) on the options bar. For more information on editing an existing email relay host, see Editing an Email Relay Host.

Adding an Email Relay Host

To configure a new email relay host for your DR Series system, complete the following:

NOTE: To edit an existing email relay host, see Editing an Email Relay Host.

1. Select **System Configuration** → **Email Relay Host**.

   The **Email Relay Host** page is displayed.
2. Click **Add Relay Host** on the options bar.

   The **Add Relay Host** dialog is displayed.
3. In **Relay Host**, type the hostname or IP address of an external mail server that will act as the email relay host for your DR Series system.
4. Click **Submit** (or click **Cancel** to display the **Email Alerts** page).

   The **Email Relay Host** page is displayed, and an **Updated external email server information** dialog is displayed when successful.
5. Send a test message to verify that the email relay host is working properly.

   For more information, see Sending a Test Message.
6. Verify that all of the intended recipient email addresses received the test email.

Editing an Email Relay Host

To edit an existing email relay host for your DR Series system, complete the following:

1. Select **System Configuration**→ **Email Relay Host**.

   The **Email Relay Host** page is displayed.
2. Click **Edit Relay Host** on the options bar.

   The **Edit Relay Host** dialog is displayed.
3. In **Relay Host**, modify the email relay hostname or IP address of the external mail server as needed.
4. Click **Submit** (or click **Cancel** to display the **Email Alerts** page).

The **Email Relay Host** page is displayed, and an **Updated external email server information** dialog is displayed when successful.

Configuring System Date and Time Settings

If you need to configure or manage the date and time settings used by your system that synchronize it with other DR Series systems or clients running in your domain, navigate to the **Date and Time** page, and click **Edit**. The **Date and Time** page displays a Settings pane that contains the following date and time-related settings (by default, the system has the following date and time settings as default values in an initial system startup):

- **Mode**—select from two types: Manual and Network Time Protocol (NTP).

  NOTE: Dell recommends using NTP when the DR Series system is part of a workgroup and not part of a domain. When the DR Series system is joined to a domain, such as the Microsoft Active Directory Services (ADS) domain, NTP is disabled and the DR Series system uses the domain time.
- **Time Zone**—when in NTP mode, select from a list of time zone options based on Greenwich Mean Time (GMT); for example, GMT-8:00, Pacific Time (US and Canada).
- **NTP Servers**—when in NTP mode, select from an Internet pool of NTP servers (you can define up to three NTP servers) when using the NTP mode. If this setting is not visible in the Settings pane, verify that the **Mode** indicates it is joined to an Active Directory Services (ADS) domain. When joined to a domain, NTP is disabled for the DR Series system.
- **Set Date and Time**—when in Manual mode, click the calendar icon, and configure the date and time by making month, day, and time in a 24-hour time format selections. Use the controls on the calendar to select the month, the day of the month, and the hours and minutes using the slider controls. To set the current time, click **Now**. When done with setting your date and time values, click **Done** (and the time appears for example, as 12/12/12 14:05:45). When all date and time settings are configured, click **Submit** for the DR Series system to accept the new values.

NOTE: System synchronization is critical for proper data archiving and replication service operations.

By using the NTP mode, you synchronize your system clock whereby NTP ensures that your system has a reliable time stamp. This is critical for successful file exchanges, network log coordination and validation, and resource access requests within a workgroup.

NOTE: Dell recommends that you use the NTP mode to ensure better replication service operations when part of a workgroup. You can set or modify existing date and time settings for your DR Series system by using the **Edit** option in the **Date and Time** page. However, the NTP service is disabled when you join a domain, at which point the domain time management is used and you cannot enable NTP.

Editing System Date and Time Settings

To modify the default time and date settings for your DR Series system, complete the following:

1. Select **System Configuration** → **Date and Time**.

   The **Date and Time** page is displayed.
2. Click **Edit** on the options bar.

   The **Edit Date and Time** dialog is displayed.

NOTE: If the DR Series system is joined to a Microsoft Active Directory Services (ADS) domain, the **Edit** option will be disabled (grayed out) and the **Mode**, **Time Zone**, or **Date and Time** values cannot be changed in the Settings pane. This is because whenever a DR Series system is joined to a domain, the Network Time Protocol (NTP) is disabled and the DR Series system uses the domain-based time service. NTP is used in the **Mode** setting when the DR Series system is part of a workgroup and not joined to a domain. To be able to modify or edit any of the Settings pane values when the DR Series system is joined to an ADS domain, you would first need to leave the ADS domain before you could modify any of the date and time settings. For more information, see Configuring Active Directory Settings.

3. In **Mode**, select either **Manual** or **NTP**.

   If you select **Manual**, continue on with the tasks in step 3.

   If you select **NTP**, skip to step 4.

   a. Select **Manual**.

      The **Edit Date and Time** dialog is displayed.

   b. Click the **Time Zone** drop-down list and choose the desired time zone.

   c. Click the **Calendar** icon (adjacent to **Set Date and Time**), and select the desired day in the month (the system prevents the selection of unsupported days).

   d. Adjust the **Hour and Minute** sliders to the desired time (or click **Now** to set the date and time to be the current date and time in hours and minutes).

   a. Click **Done**.

      The **Edit Date and Time** dialog is displayed with your new settings.

4. Select **NTP**.

   The **Edit Date and Time** dialog is displayed.

   - Click the **Time Zone** drop-down list and select the desired time.
   - Edit or revise the NTP servers as desired (you are limited to selecting only three NTP servers).

5. Click **Submit** (or click **Cancel**).

   The **Date and Time** page is displayed, and an **Enabled NTP service** dialog is displayed when successful (and this was your selected mode).

Understanding Containers

After initialization, the DR Series system contains a single default container named *backup* for storing backup data. You can create additional containers as needed for storing your data. For more information about creating storage containers, see Creating Storage Containers.

Containers function like a shared file system. These types of containers can be assigned a specific type of connection type, for example, NFS/CIFS or RDA (includes both OST and RDS clients) depending on the type of container. These containers are then accessed using NFS, CIFS, or RDA. You can also create virtual tape library (VTL) type containers, which are accessed via NDMP and iSCSI protocols.

Configuring Share-Level Security

The DR Series system supports setting up share-level permissions for CIFS shares using the standard Microsoft Windows administrative tool, Computer Management. Computer Management is a component that is built into the Microsoft Windows 7, Vista, and XP operating systems.

NOTE: Any user that is part of BUILTIN\Administrators can edit ACLs on CIFS shares. The local DR Series system administrator is included in the BUILTIN\Administrators group. To add additional domain groups to the BUILTIN \Administrators group, you can use the Computer Manager tool on a Windows client to connect to the DR Series system as Domain administrator and add any groups you want. This capability allows users other than the Domain administrator to modify an ACL as needed.

This administrative tool lets you control access to shares and also configure read-only or read-write access to user groups or individual users within the Active Directory Service (ADS) when joined to an ADS domain.

To implement share-level security on a DR Series system that has been joined to an ADS domain, make sure that you have mapped a drive on the DR Series system using an account with DOMAIN\Administrator credentials (or by using an account that is equivalent to a domain administrator). For more information about joining to an ADS domain, see Configuring Active Directory Settings.

NOTE: If you do not use an account with sufficient privileges, you will not be able to see the shares or you may experience other problems.

1. Click **Start** → **Control Panel** → **Administrative Tools** → **Computer Management**.

   The **Computer Management** page is displayed.
2. Click **Action** → **Connect to another computer...** .

   The **Select Computer** dialog is displayed.
3. Click **Another computer**, type the hostname or IP address for this DR Series system, and click **OK**.

   The **Computer Management** page is displayed with the designated DR Series system listed in the left pane.
4. Click **System Tools**, and click **Shared folders**.

   The **Shares**, **Sessions**, and **Open Files** folders are displayed in the main pane of the **Computer Management** page.
5. Click **Shares** to display a list of the shares managed by the DR Series system.
6. Right-click on the share of interest, and select **Properties**.

   The specified share **Properties** page is displayed.
7. Click the **Share Permissions** tab in the specified share **Properties** page.

   The **Share Permissions** view in the **Properties** page is displayed.
8. To remove existing access permissions to the share, or add additional groups or user that can access the share, complete the following:

   - To add access for a new group or user, click **Add...** to display the **Select Users or Groups** dialog.
   - Click **Object Types...**, choose the object types you want to select (**Built-in security principals**, **Groups**, or **Users**), and click **OK**.
   - Click **Locations...** and define the root location from which to begin your search, and click **OK**.
   - In the **Enter the object names to select** list box, enter any object name(s) you want to find.

     NOTE: You can search for multiple objects by separating each name with a semicolon, and by using one of the following syntax examples: DisplayName, ObjectName, UserName, ObjectName@DomainName, or DomainName\ObjectName.
   - Click **Check Names** to locate all matching or similar object names that are listed in the **Enter the object names to select** list box, by using the object types and directory locations you selected.
9. Click **OK** to add the object to the **Group or user names** list box.
10. In the Permissions pane for the selected object, select the **Allow** or **Deny** check box to configure the following permissions:

    - Full Control
    - Change
    - Read
11. Click **OK** to save the selected share permission settings associated with the selected object.

5

Managing DR Series Storage Operations

This chapter describes how to use the DR Series system to perform data storage operations, including creating and managing containers, setting up and managing replication, viewing detailed client information, and setting up and managing encryption.

Understanding the Storage Page and Options

To open the **Storage** page, click **Dashboard** → **Storage**. This page displays system-related storage information in the following panes:

NOTE: The DR Series system polls and updates statistics every 30 seconds.

- **Storage Summary**:
  - Number of Containers
  - Number of Containers Replicated
  - Total Number of Files in All Containers
  - Compression Level
- **Capacity**:
  - Used and free system physical capacity in both percentages and Gibibytes (GiB) or Tebibytes (TiB)
- **Storage Savings**:
  - Total savings (deduplication and compression) graphed in percentages and based on time in minutes; you can display the statistics in 1–hour (1h), 1–day (1d), 5–day (5d), 1–month (1m), and 1–year (1y); 1–hour is the default.
- **Throughput**:
  - Read and write rates graphed in Mebibytes per second (MiB/s) and based on time in minutes; you can display the statistics in 1–hour (1h), 1–day (1d), 5–days (5d), 1–month (1m), and 1–year (1y); 1–hour is the default.
- **Physical Storage**:
  - Type: internal or external storage (external is the expansion shelf enclosure)
  - Raw Size (storage capacity listed in Gigabytes or Terabytes)
  - % Used (represents the percent of capacity used)
  - Service Tag (tag is a unique 7–digit Dell ID)
  - Configured (status is listed as yes, no, add, or detect)
  - State (storage status is ready, reading, initializing, rebuilding, or not detected)

NOTE: To refresh the values listed in **Storage Savings** and **Throughput** , click ⟳. To refresh an expansion shelf enclosure, click **Detect** under the Configured column in the Physical Storage summary table (the **Enclosure Detect** dialog is displayed with this message: *If the enclosure is undetected, please wait five minutes and try again. If the enclosure still remains undetected after an attempt, keep the enclosure powered On and reboot the appliance*).

For more information about DR Series system container operations, see Managing Container Operations.

Understanding the Storage Options

The DR Series system stores backed up and deduplicated data that has been ingested by the system into easily accessible storage containers. A number of system storage operations are available in the DR Series system graphical user interface (GUI) that simplify the process for storing this type of data. The **Storage** section of the navigation panel of the DR Series system GUI contains the following areas of functionality:

- **Containers**
- **Replication**
- **Encryption**
- **Clients**

Containers

To display the **Containers** page, click **Storage→ Containers**. This page displays the total number of containers (**Number of Containers**) and the container path (**Container Path: /containers**). On this page, you can perform the following tasks:

- **Create** — Create new containers
- **Edit** — Edit existing containers
- **Delete** — Delete existing containers
- **Display Statistics** — Display container, connection, and replication statistics

The **Containers** page also displays a Containers summary table that displays the following types of container-related information:

- **Containers** — lists containers by name
- **Files** — lists the number of files in each container
- **Marker Type** — lists the marker type that supports your DMA
- **Access Protocol** — lists the connection type/access protocol per container:
  - Network File System (NFS)
  - Common Internet File System (CIFS)
  - Rapid Data Access (RDA)
  - Network Data Management Protocol (NDMP) (for VTL containers)
  - Internet Small Computer System Interface (iSCSI) (for VTL containers)
- **Replication** — lists the current replication state per container:
  - Not Configured
  - Stopped
  - Disconnected
  - Trying to Connect
  - Online
  - N/A
  - Marked for Deletion

NOTE: For newly created OST or RDS containers, the Replication status displays **N/A**. When replication data has been deleted from an existing OST or RDS container, the Replication status also displays **N/A**. For existing containers that are in the process of deleting a large amount of data, the Replication status displays **Marked for Deletion** to indicate that the data deletion process has not yet completed.

NOTE: Use **Select** to identify the container on which you want to perform an action. For example, click **Select**, and click **Display Statistics** to display the **Container Statistics** page for the container you selected.

Replication Page

To display the **Replication** page, click **Storage** → **Replication**. The **Replication** page displays the number of source replications, the names of the local and remote containers, the peer state, and the bandwidth selected per container. The **Replication** page lets you perform the following tasks:

- Create a new replication relationship (source and target pair or cascaded replication) and select the type of encryption to use.
- Edit or delete an existing replication relationship.
- Start or stop replication.
- Set the bandwidth (or speed limit) for the replication process.
- Display statistics for an existing replication relationship.

The **Replication** page contains a Replication summary table that lists the following replication-related information:

- **Source Container Name**—SRC container name (IP address or hostname)
- **Replica Container Name**—Target in the replication process (IP address or hostname)
- **Cascaded Replica Container Name**—Remote container name (IP address or hostname) (optional)
- **Bandwidth**—Settings include Kibibytes per second (KiB/s), Mebibytes per second (MiB/s), Gibibytes per second (GiB/s), or default (an unlimited bandwidth setting)

  NOTE: Mouse over status for Peer State—Online, Offline, Paused, or Disconnected. When started the Peer State displays the status as Online for the selected container. When stopped, the Peer State initially displays the status as Paused, and then changes to Offline.

Encryption

To display the **Encryption** page, click **Storage**→ **Encryption**. This page displays current encryption settings for the stored data on the DR Series system.

On this page, you can perform the following tasks:

- **Set or Change Passphrase** — Set a new passphrase or change the current passphrase
- **Manage Encryption Settings** — Manage encryption settings, such as enabling or turning off encryption and setting the encryption mode.

Clients

To open the **Clients** page, click **Storage** → **Clients**. This page displays the total number of clients that are connected to the DR Series system, which can be a combination of NFS, CIFS, RDS, OST, NDMP, iSCSI, and DR2000v clients. The total number of clients is listed above the tabs (**NFS**, **CIFS**, **RDA**, **NDMP**, **iSCSI**, and **DR2000v** tabs).

Depending on the tab you select, the number of clients for each connection type is displayed, as well as other information about the clients. For example, if you select the **RDA** tab, the number of current OST or RDA clients (OpenStorage Technology or Rapid Data Storage clients) that are connected to the system are displayed. The RDA tab also provides the following types of client-related information:

- **Number of RDA Clients** — The number of OST and RDS clients.
- **Name** — Each client referenced by name.
- **Type** — The type of RDA clients.

- **Plug-In** — The plug-in type installed on each client.
- **Backup Software** — The backup software used with each client.
- **Idle Time** — The idle time (non-activity) for each client.
- **Connection** — The number of connections for each client. For a definition of connections and streams, see Streams_vs_Connections.
- **Mode** — The current mode type for each client.

For more information about using this page and related tabs, see Clients Page (Using the NFS or CIFS Tab), Clients Page (Using the RDA Tab), Clients Page (Using the NDMP tab), and Clients Page (Using the iSCSI Tab).

Clients Page (Using the NFS or CIFS Tabs)

On the **Clients** page (**Storage→ Clients)**, click the **NFS** or **CIFS** tab to view the following information for NFS or CIFS clients. (For more information about the Clients page, see Clients.)

- **Number of NFS (or CIFS) Clients** — lists number of NFS (or CIFS) clients.
- **Name** — lists each client by name.
- **Idle Time** — lists idle time (nonactivity) for each client.
- **Connection Time** — lists connection time for each client.

Clients Page (Using the RDA Tab)

To display the **Clients** page, click **Storage→ Clients**. This page displays the total number of clients that are connected to the DR Series system, and this number reflects all of the clients based listed under the **Clients** tab (NFS, CIFS, and RDA). Using this page and the **RDA** tab lets you perform the following tasks for RDS or OST clients:

- Update a client (you are limited to modifying the mode type)
- Edit a client password

This page displays an RDS or OST Clients Summary table that lists the following types of RDS or OST client-related information:

- Name — lists client by name
- Type — lists client type
- Plug-In — lists plug-in version that is installed on the client

  NOTE: The RDA plug-in is installed by default if you are running the latest version of Dell NetVault Backup (NVBU). You must download and install the RDA plug-in for NVBU only if there is a plug-in version mismatch between the DR Series system software and NVBU.
- Backup Software — lists backup software used with this client
- Idle Time — lists the idle time for this client
- Connection — lists the number of connections for this client
- Mode — lists the mode types that can be set for this client:
  - **Auto:** DR will set the deduplication to Dedupe or Passthrough, based on the client's number of cores and whether it is 32– or 64–bit.
  - **Passthrough:** The client will pass all data to DR for deduplication processing (appliance-side deduplication).
  - **Dedupe:** The client will process hashing on data, so deduplication processing occurs on the server side (client-side deduplication).

If an OST or RDS client has four or more CPU cores, it is considered to be dedupe-capable. However, the OST or RDS client operating mode depends upon how it is configured in the DR Series system (**Dedupe** is the default RDA client mode).

- If the administrator did not configure an OST or RDS client to operate in a specific mode and it is dedupe-capable, it will run in the **Dedupe** mode.
- If an OST or RDS client is not dedupe-capable (meaning the OST or RDS client has less than four CPU cores), and the administrator sets it to run in the **Dedupe** mode, it will only run in the **Passthrough** mode.
- If an OST or RDS client is set to run in **Auto** mode, the OST or RDS client will run in the mode setting determined by the media server.

The following table shows the relationship between the configured OST or RDS client mode types and the supported client mode based on client architecture type and corresponding number of CPU cores. For information about Rapid NFS and Rapid CIFS supported client modes based on architecture and CPU cores, see Best Practices: Rapid NFS and Best Practices: Rapid CIFS.

Table 1. Supported OST or RDS Client Modes and Settings

OST or RDS Client Mode Settings	32–Bit OST or RDS Client (4 or more CPU cores)	64–Bit OST or RDS Client (4 or more CPU cores)	32–Bit OST or RDS Client (Less than 4 CPU cores)	64–Bit OST or RDS Client (Less than 4 CPU cores)
Auto	Passthrough	Dedupe	Passthrough	Passthrough
Dedupe	Not Supported	Supported	Not Supported	Not Supported
Passthrough	Supported	Supported	Supported	Supported

Clients Page (Using the NDMP Tab)

On the **Clients** page (**Storage** > **Clients**), click the **NDMP** tab. On this tab, you can view the following information for NDMP clients. (for more information about the Clients page, see Clients).

- **Number of current NDMP sessions active** — Lists the number of NDMP sessions that are currently active.
- **ID** — NDMP session ID.
- **Duration** — The duration of the current active session.
- **State** — The current status, for example, Active.
- **Source** — IP address of the source filer.
- **Target** — The target tape drive being used for the current NDMP session.
- **Throughput** — The current and average throughput.
- **Transfer size** — The total size of data transferred in this backup session.
- **DMA** — The IP address of the DMA initiating the backup.
- **NDMP Completed Sessions Statistics** — Shows the above information for any completed NDMP sessions.

Clients Page (Using the iSCSI Tab)

On the **Clients** page (**Storage** > **Clients**), click the **iSCSI** tab. On this tab, you can view the following information for iSCSI clients. (for more information about the Clients page, see Clients).

- **Number of current iSCSI sessions active** — The number of currently active iSCSI sessions.
- **Container Name** — The container name for each iSCSI VTL container.
- **Container IQN** — The iSCSI Qualified Name for each iSCSI VTL container..
- **Initiators Connected** — The initiators connected to this iSCSI VTL container..

On this tab, you can also set or change the CHAP password for the CHAP account.

To do so, click **Edit CHAP Password**.

Managing Container Operations

This topic describes using the DR Series system to manage your data storage and container operations. Data storage operations include tasks such as creating new containers, managing or deleting existing containers, moving data into containers, and displaying current container statistics.

Creating Storage Containers

By default, the DR Series system provides a container named **backup** for your use after you complete the basic system configuration and initialization process. You can create additional containers to store your data as needed.

NOTE: The DR Series system does not support container names that begin with a number.

Containers function like a shared file system that can be accessed using the following connection types:

- **NFS**
- **CIFS**
- **NDMP** (for VTL type containers)
- **iSCSI** (for VTL type containers)
- **RDA** (Rapid Data Access)
  - **OST** (OpenStorage Technology)
  - **RDS** (Rapid Data Storage)
- **No Access** (an unassigned connection type)

Choosing the **No Access** or unassigned connection type lets you create containers that can be configured later as needed. To modify a container configured with a **No Access** connection type, select the container, click **Edit**, and start configuring it as desired.

Creating an NFS or CIFS Connection Type Container

To create an NFS or a CIFS connection type container, complete the following steps:

1. Select **Storage** → **Containers**.

   The **Containers** page is displayed, which includes a Containers summary table listing all existing containers.
2. Click **Create**.

   The **Container Wizard — Create New Container** dialog box appears.
3. For **Container Name**, type the name of the container, and then click **Next**.

   Container names cannot exceed 32 characters in length, must start with a letter, and can be composed of any combination of the following characters:

   - A-Z (uppercase letters)
   - a-z (lowercase letters)
   - 0-9 (numbers). Do not start a container name with a number.
   - dash (-) or underscore (_) special characters

   NOTE: The DR Series system does not support the use of the following special characters in container names: /, #, or @.
4. On the next page of the wizard, for **Storage Access Protocol**, select **NAS (NFS, CIFS)**, and then click **Next**.
5. On the next page of the wizard, next to **Enable Access Protocols**, select **NFS** or **CIFS** as appropriate.

   (Use NFS to back up UNIX or LINUX clients. Use CIFS to back up Windows clients.)

6. For **Marker Type**, select the appropriate marker that supports your DMA.

   - **None** — Disables marker detection for the container.
   - **Auto** — Automatically detects CommVault, Tivoli Storage Manager (TSM), ARCserve, and HP Data Protector marker types. In addition, select this option if you need to support EMC Networker 2.0.
   - **Networker** — Supports EMC Networker 3.0. If you need to support EMC Networker 2.0, select **Auto**.
   - **Unix Dump** — Supports the Amanda marker, among others.
   - **BridgeHead** — Supports the BridgeHead HDM marker.
   - **Time Navigator** — Supports the Time Navigator marker.

   Improper marker selection can result in non-optimal savings. As a best practice, if you have only one type of DMA with traffic directed to a container, it is best to select the marker type that supports your DMA (for example, **BridgeHead**, **Auto**, or another). Conversely, as a best practice, if you have traffic from a DMA that is not one of the supported marker types, it is best to disable marker detection for the container by selecting the **None** marker type.
7. Click **Next**.
8. If you selected NFS as the connection type, configure NFS access as follows.

   - **NFS Options** — Defines the type of access to the container. Select one of the following options.
     - **Read Write Access** — To allow read-write access to the container.
     - **Read Only Access** — To allow read-only access.
   - **Insecure** — Select this option to allow replies to be made to requests before the changes in the request are committed to disk.

     NOTE: The DR Series system always commits writes to NVRAM first before committing any changes to disk.
   - **Map Root To** — Select one of the following options from the drop-down list to define the user level you want mapped to this container.
     - **nobody** — to specify a user on the system without root access permissions.
     - **root** — to specify a remote user with root access to read, write, and access files on the system.
     - **administrator** — to specify the system administrator.
   - **Client Access** — Define the NFS client(s) that can access the NFS container or manage the clients that can access this container by selecting one of the following options.
     - **Open (allow all clients) —** To allow open access for all clients to the NFS container you create. (Select this option *only* if you want to enable access for all clients to this NFS container.)
     - **Create Client Access List** — To define specific clients that can access the NFS container. In the **Client FQDN or IP** text box, type the IP address (or FQDN hostname) and click **Add.** The “added” client appears in the **allow access clients** list box. (To delete an existing client from this list box, select the IP address (or FQDN hostname) of the client you want to delete, and click **Remove**. The “deleted” client disappears from the list box.)
9. If you selected CIFS as the connection type, configure CIFS access as follows.

   - **Client Access** — Define the CIFS client(s) that can access the container or manage the clients that can access this container by selecting one of the following options.
     - **Open (allow all clients) —** To allow open access for all clients to the container you create. (Select this option *only* if you want to enable access for all clients to this container.)
     - **Create Client Access List** — To define specific clients that can access the container. In the **Client FQDN or IP** text box, type the IP address (or FQDN hostname) and click **Add.** The “added” client appears in the **allow**

access clients list box. (To delete an existing client from this list box, select the IP address (or FQDN hostname) of the client you want to delete, and click **Remove**. The “deleted” client disappears from the list box.)

> **NOTE:** The DR Series system administrator that manages the system has a different set of privileges than does the CIFS administrator user. Only the DR Series system administrator can change the password for the CIFS administrator user. To change the password that allows access for the CIFS administrator user, use the **authenticate --set --user administrator** commands. For more information, see the *Dell DR Series System Command Line Reference Guide*.

10. Click **Next**.

    A Configuration Summary of the options you selected for creating the container appears.

11. Click **Create a New Container**.

    A progress dialog box appears and then the **Containers** page is displayed, with a **Successfully Added** message. The list of containers in the Containers summary table is now updated with your new container.

Creating a Virtual Tape Library (VTL) Type Container

To create a VTL type container, complete the following steps:

> **NOTE:** The creation of VTL type containers is supported on the DR4X00 and DR6000.

1. Select **Storage** → **Containers**.

   The **Containers** page is displayed, which includes a Containers summary table listing all existing containers.

2. Click **Create**.

   The **Container Wizard — Create New Container** dialog appears.

3. For **Container Name**, type the name of the container.

   > **NOTE:** The DR Series system does not support spaces or the following special characters in container names: /, #, or @. VTL container names cannot exceed 32 characters in length, must start with a letter, and can be composed of any combination of the following characters:

   - A-Z (uppercase letters)
   - a-z (lowercase letters)
   - 0-9 (numbers). (Do not start a container name with a number.)
   - underscore (_) special characters

   > **NOTE:** iSCSI VTL containers do not support the following characters:

   - ASCII CONTROL CHARACTERS and SPACE through ,
   - ASCII /
   - ASCII ; through @
   - ASCII [through `
   - ASCII { through DEL

4. Select the **Virtual Tape Library (VTL)** check box.
5. Click **Next**.
6. In the **Container Wizard – Create New Container** dialog box, if you want to create the Dell OEM VTL container type, select the **Is OEM** checkbox.

   > **NOTE:** The Dell OEM type VTL is supported only with Symantec Backup Exec and Netbackup data management applications (DMAs).

7. For **Tape Size**, select the size of the tapes for your tape library from one of the following options.

- 800 GB
- 400 GB
- 200 GB
- 100 GB
- 50 GB
- 10 GB

  NOTE: Creating a VTL container type creates a tape library of type Storage Tek L700 with 10 tape drives of type IBM Ultrium LTO-4 and 10 tape slots holding 10 tapes. Additional tapes can be added as required. For more information, see the topic, VTL and DR Series Specifications.

8. For **Access Protocol**, select one of the following options.

   - NDMP
   - iSCSI
   - No Access (select this option if you are not ready to select a protocol.)

     NOTE: The DR Series system allows you to create a VTL container type without configuring it with a specific protocol (that is, by selecting No Access). When you are ready to configure the container at a later date, select it in the Containers summary table, click **Edit**, and then configure it with the proper protocol.

9. For **Access Control**, do one of the following:

   - If you selected NDMP as the access protocol, type the DMA's FQDN or IP address that will access the VTL container.
   - If you selected iSCSI as the access protocol, type the FQDN, IQN, or IP address of the iSCSI initiator that can access the VTL container.

10. If you selected NDMP as the access protocol, for **Marker Type**, select the appropriate marker that supports your DMA from one of the following options.

    - **None** — Disables marker detection for the container.
    - **Unix Dump** — Supports the Amanda marker, among others.

11. If you selected iSCSI as the access protocol, for **Marker Type**, select the appropriate marker that supports your DMA from one of the following options.

    - **None** — Disables marker detection for the container.
    - **Auto** — Automatically detects CommVault, Tivoli Storage Manager (TSM), ARCserve, and HP Data Protector marker types. In addition, select this option if you need to support EMC Networker 2.0.
    - **Networker** — Supports EMC Networker 3.0. If you need to support EMC Networker 2.0, select Auto.
    - **Unix Dump** — Supports the Amanda marker, among others.
    - **BridgeHead** — Supports the BridgeHead HDM marker.
    - **Time Navigator** — Supports the Time Navigator marker.

    NOTE: Improper marker selection can result in non-optimal savings. As a best practice, if you have only one type of DMA with traffic directed to a container, it is best to select the marker type that supports your DMA. Conversely, as a best practice, if you have traffic from a DMA that is not one of the supported marker types, it is best to disable marker detection for the container by selecting the **None** marker type.

12. Click **Next**.

    A Configuration Summary of the options you selected for creating the container appears.

13. Click **Create a New Container**.

    The **Containers** page is displayed with a message stating the container was successfully added and enabled. The list of containers in the Containers summary table is updated to show your new container.

For iSCSI, you should configure the CHAP password for the system-wide CHAP account. To do so, you can use the CLI or navigate to **Storage > Clients**, and then click **Edit CHAP Password**.

You can add additional tapes to the library after container creation by editing the container in the GUI or by using the following CLI command:

```
vtl --update_carts --name <name> --add --no_of_tapes <number>
```

NOTE: For more information about using the command line interface, see the *Dell DR Series Command Line Reference Guide*.

Creating an OST or RDS Connection Type Container

To create an OST or RDS connection type container, follow these steps:

1. Select **Storage** → **Containers**.

   The **Containers** page displays all existing containers.
2. Click **Create**.

   The **Container Wizard — Create New Container** dialog box appears.
3. For **Container Name**, type the name of the container, and then click **Next**.

   Container names cannot exceed 32 characters in length, must start with a letter, and can be composed of any combination of the following characters:

   - A-Z (uppercase letters)
   - a-z (lowercase letters)
   - 0-9 (numbers). Do not start a container name with a number.
   - dash (-) or underscore (_) special characters

   NOTE: The DR Series system does not support the use of the following special characters in container names: /, #, or @.
4. For **Connection Type**, select **Dell Rapid Data Storage (RDS)** or **Symantec OpenStorage (OST)** as appropriate, and then click **Next**.
5. For **LSU Capacity**, select one of the following options allowed per container:

   - **Unlimited** — To define the allowed amount of incoming raw data per container (based on the physical capacity of the container). If you selected **RDS**, by default, **Unlimited** is selected.
   - **Quota**: To define a set limit in Gibibytes (GiB) for incoming raw data allowed per container.
6. Click **Next**.

   A Configuration Summary of the options you selected for creating the container appears.
7. Click **Create a New Container**.

   A progress dialog box appears and then the **Containers** page is displayed, with a **Successfully Added** message. The list of containers in the Containers summary table is now updated with your new container.The Marker Type for the newly created container is displayed as None. The list of containers in the Containers summary table is updated with your new container.

Editing Container Settings

To modify any of the settings for an existing container, complete the following:

1. Select **Storage**→ **Containers**.

   The **Containers** page is displayed, and lists all current containers.
2. Click **Select** to identify the container in the list that you want to modify, and click **Edit**.

   The **Edit Container** dialog is displayed.

3. Modify the marker type for the selected container as needed. For details, see Creating Storage Containers.

   CAUTION: If you are changing the marker type on a DR6000 and you are using Rapid CIFS, you must remount the share on the client after you change the marker type.

4. Modify the connection type options for the selected container as needed.

   - If you want to modify an existing NFS/CIFS, NFS, or CIFS connection type container settings, see the NFS/CIFS, NFS-only, and CIFS-only options available in Creating an NFS or CIFS Connection Type Container, and make the corresponding changes.
   - If you want to modify an existing VTL container type settings, see the options available in the topic, Creating a VTL Type Container, and make the corresponding changes.
   - If you want to modify the existing OST or RDS connection type container settings, see the options available in Creating an OST or RDS Connection Type Container , and make the corresponding changes.
   - If you want to modify the existing unassigned (No Access) connection type container settings, see the options available in Creating An Unassigned Connection Type Container, and make the corresponding changes.

   NOTE: If you select **Open Access** in the **Client Access** pane, the **Add clients (IP or FQDN Hostname)** and **Clients** panes are hidden and you cannot create or modify these options.

   NOTE: The DR Series system always commits writes to NVRAM first before committing any changes to disk.

   NOTE: The DR Series system administrator who manages the DR Series system has a different set of privileges than the CIFS administrator user. Only the DR Series system administrator can change the password for the CIFS administrator user. To change the password that allows access for the CIFS administrator user, use the DR Series system CLI **authenticate --set --user administrator** command. For more information, see the *Dell DR Series System Command Line Reference Guide* at **dell.com/powervaultmanuals**.

5. After the container type settings have been modified, click **Modify this Container** .

   The **Successfully updated container** dialog is displayed. The list of containers in the Containers summary table is updated with the newly modified container.

Deleting Containers

Before deleting a container, Dell recommends that you first carefully consider whether or not you need to preserve the data in the container. To delete an existing container that contains data, complete the following:

CAUTION: Before deleting any DR Series container that contains deduplicated data, Dell recommends that you take steps to preserve this data using another means of long-term retention. Once a container is deleted, the deduplicated data cannot be retrieved. The DR Series system allows you to delete any specified container and all of its contents in one operation.

1. Select **Storage** → **Containers**.

   The **Containers** page is displayed, and lists all current containers.

2. Click **Select** to identify the container you want to delete, and click **Delete**.

   A **Delete Confirmation** dialog is displayed, which prompts you about the specific container by name that you selected to delete.

3. Click **OK** in the **Delete Confirmation** dialog.

   The **Successfully removed container** dialog is displayed. The list of containers in the Containers summary table is updated and no longer displays the deleted container.

Moving Data Into a Container

To move data into an existing DR Series system container, complete the following:

1. Click **Start** → **Windows Explorer** → **Network**.

   The **Network** page is displayed, which lists all current computers.
2. In the browser **Address bar**, click **Network** to select your DR Series hostname or IP address.

   The **Network** page is displayed, which lists all current storage and replication containers.

   NOTE: However, if your DR Series system is not listed, you can enter its hostname or IP Address preceded by "https://" and followed by the container name in the **Address bar** to access it (for example in this format, https://10.10.20.20/container-1). The DR Series system only supports the Hypertext Transfer Protocol Secure (HTTPS) form of IP addressing.
3. Move data from the source location to the destination container using your regular DMA or backup application process.

   NOTE: If any file ingested by the DR Series system by a DMA or backup application is renamed or deleted without using the DMA or backup application's process, the corresponding catalog must be updated accordingly. Failure to do so may prevent the DMA or backup application from being able to access the data.
4. Verify that the data recently moved now resides in the destination container (or click **Dashboard** → **Container Statistics**, select the destination container in the **Container Name** drop-down list, and view the following information panes for recent container activity:

   - **Backup Data**
   - **Throughput**
   - **Connection Type**
   - **Connection Configuration**

Displaying Container Statistics

To display the current statistics for an existing container that stores your data, complete the following:

NOTE: An alternate method to display statistics for any current container is to select that container by name in the **Container Name** drop-down list in the **Container Statistics** page (**Dashboard** → **Container Statistics**).

1. Select **Storage** → **Containers**.

   The **Containers** page is displayed, and the Containers summary table lists all of the current containers in the system.
2. Click **Select** to identify the container to display, and click **Display Statistics** in the options bar.

   The **Container Statistics** page is displayed which shows the current backup data (number of active files and active bytes ingested in the Backup Data pane), and read and write throughput (in the Throughput pane). The system polls for and updates the displayed statistics every 30 seconds.

   NOTE: To display statistics for another container, select that container by name in the **Container Name** drop-down list.

   This page also displays the marker type and connection type for the selected container, and whether the container is using Rapid CIFS or Rapid NFS (DR6000 only). For more information, see Monitoring Container Statistics.

   In addition, you can also display the set of system statistics by using the DR Series system CLI **stats --system** command to show the following categories of system statistics:

   - Capacity Used (system capacity used in Gibibytes or GiBs)

- Capacity Free (system capacity free in GiBs)
- Read Throughput (read throughput rate in Mebibytes or MiB/s)
- Write Throughput (write throughput rate in MiB/s)
- Current Files (current number of files in system)
- Current Bytes (current number of ingested bytes in system)
- Post Dedupe Bytes (number of bytes after deduplication)
- Post Compression Bytes (number of bytes after compression)
- Post Encryption Bytes
- Post Encryption Bytes in GiB
- Compression Status (current compression status)
- Cleaner Status (current space reclamation process status)
- Encryption Status
- Total Inodes (total number of data structures)
- Bytes decrypted
- Dedupe Savings (deduplication storage savings by percentage)
- Compression Savings (compression storage savings by percentage)
- Total Savings (total storage savings by percentage)

Displaying DR Series System Statistics Using the CLI

An alternate method for checking the current DR Series system statistics is using the DR Series system CLI **stats --system** command to show the following categories of system statistics:

- Capacity Used (system capacity used in Gibibytes or GiBs)
- Capacity Free (system capacity free in GiBs)
- Read Throughput (read throughput rate in Mebibytes or MiB/s)
- Write Throughput (write throughput rate in MiB/s)
- Current Files (current number of files in system)
- Current Bytes (current number of ingested bytes in system)
- Post Dedupe Bytes (number of bytes after deduplication)
- Post Compression Bytes (number of bytes after compression)
- Post Encryption Bytes
- Post Encryption Bytes in GiB
- Compression Status (current compression status)
- Cleaner Status (current space reclamation process status)
- Encryption Status
- Total Inodes (total number of data structures)
- Bytes decrypted
- Dedupe Savings (deduplication storage savings by percentage)
- Compression Savings (compression storage savings by percentage)
- Total Savings (total storage savings by percentage)

For more information on DR Series system CLI commands, see the *Dell DR Series System Command Line Reference Guide*.

Displaying Container-Specific Statistics Using the CLI

You can display the set of container-specific statistics by using the DR Series system CLI **stats --container --name <container name>** command to show the following categories of statistics:

- Container Name (name of the container)
- Container ID (ID associated with container)
- Total Inodes (total number of data structures in container)
- Read Throughput (read throughput rate in Mebibytes or MiB/s for container)
- Write Throughput (write throughput rate in MiB/s for container)
- Current Files (current number of files in container)
- Current Bytes (current number of ingested bytes in container)
- Cleaner Status (current space reclamation process status for the selected container)

For more information on DR Series system CLI commands, see the *Dell DR Series System Command Line Reference Guide*.

Managing Replication Operations

This topic describes using the DR Series system to manage data replication operations. Replication operations include various tasks, such as creating new replication relationships, managing or deleting existing replication relationships, starting and stopping replication, setting a replication bandwidth limit per host, displaying current replication statistics, and setting a replication schedule.

The Replication page displays current information about replication relationships for the DR Series system. It lists the following information for all current replication relationships:

- Storage Container Name
- Replica Container
- Cascaded Replica Container (if one exists)
- Status of each container
- Peer State, Estimated time to Sync, Network Savings, Encryption, Bandwidth and Schedule Status

NOTE: Bandwidth is the replication bandwidth limit that you can set as Kibibytes per second (KiBps), Mebibytes per second (MiBps), Gibibytes per second (GiBps), or as an unlimited bandwidth (default).

If no existing containers, replication relationships, or any scheduled replication operations have been added for the DR Series system, the only Replication-related option that is enabled on the Replication page is **Create.**

TCP Port Configuration

If you plan to perform replication operations across a firewall, the DR Series system replication service requires that the following fixed TCP ports be configured to support replication operations:

- port 9904
- port 9911
- port 9915
- port 9916

Before you Begin

Refer to the following important notes for understanding and using replication with the DR Series system.

- **DMAs and Domain Relationships**

  — To allow replication storage information to be viewed by a corresponding data management application (DMA), the target DR Series system must reside in the same domain as the source DR Series system in the replication relationship.
- **Replication Limits** —
  The DR Series system supports 64:1 replication of data (32:1 for DR4X00). This means that up to 64 source DR Series systems can write data to different individual containers on a single, target DR Series system. Replication can use up to 16 streams over a single port using one connection. For a definition of connections and streams, see Streams_vs_Connections.
- **Version Checking** — The DR Series system software includes version checking that limits replication only between other DR Series systems that run the same system software release version. If versions are incompatible, the administrator will be notified by an event, and replication will not continue.
- **Storage Capacity and Number of Source Systems** — Be aware that the storage capacity of the target DR Series system is directly affected by the number of source systems writing to its containers, and also by the amount being written by each of these source systems.
- **Replication for VTL Containers**—Replication for virtual tape library (VTL) container types is not currently supported; however, it is planned for a future release of the DR Series system.

Creating Replication Relationships

To create a new replication relationship, complete the following steps.

1. Select **Storage** → **Replication**.
2. Click **Create** in the options bar.

   The **Create Replication** page is displayed.
3. Under **Source Container**, define the source container by doing the following.
   a. Click **Select container from local system** or **Select container from remote system**, and select a container. (For a remote system, you will need to provide user credentials for the remote system.)
   b. Under **Source Container** > **Replica Container**, for **Encryption**, select one of the following encryption options: **None**, **128–bit**, or **256–bit**.
   c. For **Bandwidth Speed Rate**, select the bandwidth as **Default** or specify a rate.

   NOTE: Bandwidth is the replication bandwidth limit that you can set as Kibibytes per second (KiBps), Mebibytes per second (MiBps), Gibibytes per second (GiBps), or as an unlimited bandwidth (default). The minimum allowed replication bandwidth that you can set is 192 KiBps.
4. Under **Replica Container**, define the target replica container by doing the following.
   a. Click **Select container from remote system** and then select a container for the replication from the remote system.
   b. Enter the user logon credentials of the remote system.
   c. Click the **Retrieve Remote Container** button and, in the drop-down list, select a remote container from the list of available containers.
5. To set up cascaded replication (optional), define the cascaded replication by doing the following.
   a. Under **Cascaded Replica Container**, click **Select a container from the remote system** to select the container you will be using for the cascaded replica.
   b. Enter the logon credentials of the remote system.

c. Click the **Retrieve Remote Container** button, and, in the drop-down list, select a remote container from the list of available containers.

d. Under **Replica > Cascaded Replica Container**, for **Encryption**, select one of the following encryption options: **None**, **128–bit**, or **256–bit**.

e. For **Bandwidth**, select the **Bandwidth Speed Rate** as **Default** or specify a rate.

6. Click the **Create Replication** button.

Modifying Replication Relationships

You can modify the following replication settings: bandwidth, encryption, and remote container’s IP address/host name settings. To modify settings for an existing replication relationship, complete the following steps.

CAUTION: Exercise care when configuring the direction of replication for source and target containers. For example, target containers can have their contents deleted if they contain existing data.

NOTE: Because you cannot modify an existing defined role (source or target replica) for a replication relationship, if necessary, you must delete the existing replication relationship, and then recreate a new relationship with the specific source and target roles that you want.

1. Select **Storage→ Replication**.

   The **Replication** page is displayed, which lists all current replication entries

2. **Select** the replication relationship that you want to modify, and click **Edit** in the options bar.

   The **Edit Replication** dialog is displayed.

3. Modify the settings/values for the Source, Replica, or Cacscaded Replica containers as needed.

   a. To modify the bandwidth rate, next to **Bandwidth Speed Rate**, select the bandwidth as **Default** or specify a rate.

      Bandwidth is the replication bandwidth limit that you can set as Kibibytes per second (KiBps), Mebibytes per second (MiBps), Gibibytes per second (GiBps), or as an unlimited bandwidth (default). The minimum allowed replication bandwidth setting that you can configure is 192 KiBps.

   b. To modify the encryption setting, select one of the following **Encryption** values for the Source Container > Replica Container or Replica > Cascaded Replica Container as needed: **None**, **128–bit**, or **256–bit**.

   c. To modify a remote container’s IP address/host name settings, under Replica Container or Cascaded Replica Container, modify the user logon credentials of the remote system as needed.

4. Click **Save Replication**.

   The **Successfully updated replication** dialog is displayed when updates have been saved.

Deleting Replication Relationships

To delete an existing replication relationship, complete the following:

1. Select **Storage → Replication**.

   The **Replication** page is displayed.

2. **Select** the replication relationship that you want to delete, and click **Delete** in the options bar.

   The **Delete Replication** dialog is displayed.

3. Select the relationships you want to delete for the Source Container > Replica Container and/or the Replica Container > Cascaded Replica Container, and then click **OK** in the **Delete replication** dialog (or click **Cancel** to display the **Replication** page).

   The **Successfully deleted replication** dialog is displayed when successful.

   NOTE: If the deletion fails, you can use the Force option to force removal of the relationship.

Starting and Stopping Replication

To start or stop replication in an existing replication relationship, complete the following:

NOTE: For more information about setting up a Replication schedule, see Creating a Replication Schedule.

1. Select **Storage** → **Replication**.

   The **Replication** page is displayed.
2. Click **Select** to select the replication relationship for which you want to stop (see step 3) or start (see step 4) the replication process.
3. To stop the scheduled replication process, click **Stop**, and click **OK** to stop replication (or click **Cancel** to display the **Replication** page).

   The **Successfully stopped replication** dialog is displayed.
4. To start the scheduled replication process, click **Start**, and click **OK** to start replication (or click **Cancel** to display the **Replication** page).

   The **Successfully started replication** dialog is displayed.

Adding a Cascaded Replica

To add a cascaded replica to an existing replication relationship, complete the following steps.

1. Select **Storage**→ **Replication**.
2. On the Replication page, **select** the replication relationship for which you want to add a cascaded replica, and then click **Edit**.

   The Edit Replication dialog opens.
3. Under **Cascaded Replica Container**, click **Select a container from the remote system** to select the container you will be using for the cascaded replica.
4. Enter the logon credentials of the remote system.
5. Click the **Retrieve Remote Container** button, and, in the drop-down list, select a remote container from the list of available containers.
6. Under **Replica** > **Cascaded Replica Container**, select one of the following Encryption options: **None**, **128–bit**, or **256–bit**.
7. For **Bandwidth**, select the **Bandwidth Speed Rate** as **Default** or specify a rate.

   NOTE: Bandwidth is the replication bandwidth limit that you can set as Kibibytes per second (KiBps), Mebibytes per second (MiBps), Gibibytes per second (GiBps), or as an unlimited bandwidth (default). The minimum allowed replication bandwidth setting that you can configure is 192 Kbps.
8. Click **Save Replication** to save your changes.

Displaying Replication Statistics

To display the statistics for an existing replication relationship, complete the following:

1. Select **Storage** → **Replication**.

   The **Replication** page is displayed.
2. Select the replication relationship for which you want to display replication statistics, and then click **Display Statistics**, The **Replication Statistics** page is displayed, which contains the following information:

   - **Source —>Replica** — Indicates the Source->Replica replication segment.
   - **Replica—>Cascaded Replica** — Indicates the Replica->Source replication segment if one exists.

- **Hostname** — Displays the hostname of the source or target.
- **Container**—Displays the container on the related host for the replication.
- **Status**—Displays the percentage of the active replication in progress, if applicable.

3. To sort a column on this page, click a column heading by which you want to sort. Only one column can be sorted at a time, and sorting can be either ascending and descending. If you set a sort order, the sort will be remembered the next time you return to the Replication Statistics page.
4. To show replication details, click the "+" icon in the first column for a selected replication, which expands to show replication details. The replication details update every 20 seconds. These details include the following statistics for both Source->Replica and Replica->Cascaded Replica replication segments as appropriate:

   - Peer State—indicates the current peer status (Insync, Paused, or Replicating)
   - Replication Transfer Rate—in KB/s
   - Replication Peak Transfer Rate—in KB/s
   - Network Average Transfer Rate—in KB/s
   - Network Peak Transfer Rate—in KB/s
   - Network Bytes Sent
   - Estimated Time to Sync
   - Dedupe Network Savings
   - Compression Network Savings
   - Last INSYNC Time—indicates the last time system synchronization occurred.
   - Schedule Status
5. To apply filtering, in the upper right corner, select **Filter**. In the **Replication Filter** dialog box, select the replication segment hostname(s) by which you want to filter statistics, and then click **Apply Filter**. The Replication filter results will be displayed.

   For more information, see Displaying the Statistics: Replication Page.

Creating a Replication Schedule

Replication schedules can only be set on individual replication-enabled source containers.

NOTE: If there is no Replication schedule set, but there is pending data that can be replicated, replication will run when it detects three (3) minutes of idle time for any newly written files in the replicated container.

NOTE: The **Replication Schedule** page displays the current DR Series system time zone and current timestamp (using this format: US/Pacific, Tue Oct 28 14:53:02 2012).

To create a Replication schedule on a replication-enabled source container, complete the following steps.

1. Select **Schedules** → **Replication Schedule**.

   The **Replication Schedule** page is displayed.
2. Click to select the replication-enabled source container in the **Container** drop-down list.

   The Replication schedule table is displayed with columns that identify the week day, start time, and stop time.
3. Click **Schedule** to create a new schedule (or click **Edit Schedule** to modify an existing Replication schedule).

   The **Set Replication Schedule** page is displayed.
4. Select (or modify) the **Start Time** and **Stop Time** setpoint values using the **Hour** and **Minutes** pull-down lists to create a Replication schedule. For an example, see Daily Replication Schedule Example and Weekly Replication Schedule Example.

   NOTE: You must set a corresponding **Stop Time** for every **Start Time** in each Replication schedule you set. The DR Series system will not support any Replication schedule that does not contain a **Start Time/Stop Time** pair of setpoints (daily or weekly).

5. Click **Set Schedule** for the system to accept your Replication schedule (or click **Cancel** to display the **Replication Schedule** page).

   NOTE: To reset all of the values in the current Replication schedule, click **Reset** in the **Set Replication Schedule** dialog. To selectively modify values in the current schedule, make your changes to the corresponding hours and minutes pull-down lists for the **Start Time** and **Stop Time** you wish to modify, and click **Set Schedule**.

   Dell recommends that you do not schedule the running of any Replication operations during the same time period when Cleaner or ingest operations will be running. Failure to follow this practice will affect the time required to complete the system operations and/or impact your DR Series system performance.

Daily Replication Schedule Example

The daily Replication schedule example in this topic illustrates the process for setting up a replication schedule that uses a 24-hour clock (the time keeping convention where time of day is defined on a 24–hour basis). You set or view a Replication schedule in the **Replication Schedule** page. For more information, see Creating a Replication Schedule.

NOTE: Replication schedules can only be set on individual replication-enabled source containers.

To set a daily replication schedule that starts at 16:00 hours (which is 4:00 PM in a 12–hour clock format) and stops at 23:00 hours (which is 11:00 PM in a 12–hour clock format) on Mondays, click **Edit Schedule** (if modifying an existing schedule) or **Schedule** (if creating a new schedule):

- Select 16 in the hours pull-down list and 00 in the minutes pull-down list to set a **Start Time** of 16:00 on Monday.
- Select 23 in the hours pull-down list and 00 in the minutes pull-down list to set a **Stop Time** of 23:00 for Monday.
- Set the **Start Time** and **Stop Time** setpoints for any remaining days of the week on which you want to schedule replication.

NOTE: You must set a corresponding **Stop Time** for every **Start Time** in each Replication schedule you set. The DR Series system will not support any Replication schedule that does not contain a **Start Time/Stop Time** pair of setpoints (daily or weekly).

Weekly Replication Schedule Example

The following example shows how to set up a weekly Replication schedule with a start time at 01:00 am on Saturday and a stop time at 01:00 am on Sunday. The DR Series system uses the 24-hour clock convention for its time keeping in which each day is divided into twenty-four 1-hour segments.

NOTE: Replication schedules can only be set on individual replication-enabled source containers that you select from the **Container** drop-down list.

- Select 01 in the hours pull-down list and 00 in the minutes pull-down list to set a Start Time of 01:00 for Saturday.
- Select 01 in the hours pull-down list and 00 in the minutes pull-down list to set a Stop Time of 01:00 for Sunday

NOTE: You need to click **Set Schedule** for the DR Series system to accept your Replication schedule.

For more information on Replication schedules, see Creating a Replication Schedule.

Managing Encryption Operations

This topic describes using the DR Series system to manage encryption settings and operations. Encryption operations include tasks, such as enabling or turning off encryption, setting or changing the passphrase, and setting the encryption mode. For more information about recommended guidelines for setting up encryption, see the topic, Configuring and Using Encryption at Rest.

Setting or Changing the Passphrase

A passphrase is a very important part of the encryption process on the DR Series system as the passphrase is used to encrypt the content encryption key or keys. It is mandatory to define a passphrase to enable encryption. If the passphrase is compromised or lost, the administrator should change it immediately so that the content encryption keys do not become vulnerable.
To set or change the encryption passphrase, complete the following steps:

1. Select **Storage** → **Encryption**.

   The Encryption page is displayed, which displays the current encryption status of the DR Series system.
2. Click **Set or Change Passphrase**.

   The **Set or Change Passphrase** dialog box opens.
3. In the **Passphrase** and **Confirm Passphrase** text boxes, enter the passphrase to be used to encrypt content encryption keys.

   When creating a passphrase, follow these guidelines:

   - The passphrase string can take up to 256 characters.
   - Alphanumeric and special characters can be entered as part of the passphrase string.

   NOTE: Input/output operations for the DR Series system will halt during passphrase configuration, and the system will resume after passphrase submission.
4. Click the **Submit** button.

Enabling Encryption

To enable encryption for the DR Series system, complete the following steps:

1. Select **Storage** → **Encryption**.

   The **Encryption** page is displayed, which shows the current status of encryption of the DR Series system.
2. Click **Encryption Settings**.

   The **Encryption Settings** dialog box opens.
3. Next to **Encryption**, click **ON**.
4. Next to **Mode**, select the mode of key lifecycle management from one of the following options:

   - **Static** — A global, fixed key is used to encrypt all data.
   - **Internal** — Content encryption keys are generated and rotated on a specified period of days.
5. If you selected Internal as the mode of key management, next to **Key Rotation Interval in Days**, enter the number of days for key rotation when a new key is to be generated.

   In internal mode there is a maximum limit of 1023 keys. The default key rotation period is set to 30 days by default when the passphrase is set and/or encryption is turned on. You can later change the key rotation period from 7 days to 70 years for internal mode.
6. Click the **Submit Encryption Settings** button.

After encryption is enabled, all of the data that is backed up is encrypted and is kept encrypted until it is expired and cleaned by the system cleaner. Note that encryption is an irreversible process.

Changing Encryption Settings

NOTE: Key modes can be changed at any time during the lifetime of the DR Series system; however, changing the key mode can be a significant operation to undertake as all encrypted data must be re-encrypted.

To change current encryption settings, complete the following steps:

1. Select **Storage** → **Encryption**.

   The **Encryption** page is displayed, which lists the current status of encryption on the DR Series system.
2. Click **Encryption Settings**.

   The **Encryption Settings** dialog box opens.
3. Next to **Mode**, you can change the mode of key lifecycle management from one of the following options:

   - **Static** — A global, fixed key is used to encrypt all data.
   - **Internal** — Content encryption keys are generated and rotated on a specified period of days.
4. If you selected Internal as the mode of key management, next to **Key Rotation Interval in Days**, enter the number of days for key rotation when a new key is to be generated.

   The minimum number of days before the content encryption key can be rotated, and a new key is generated is seven days.
5. Click the **Submit Encryption Settings** button.

For information about disabling encryption, see the topic, Disabling Encryption.
For information about changing the passphrase, see the topic, Setting or Changing the Passphrase.

Disabling Encryption

To disable encryption, complete the following steps:

1. Select **Storage** → **Encryption**.

   The Encryption page is displayed, which shows the current status of encryption on the DR Series system.
2. Click **Encryption Settings**.

   The **Encryption Settings** dialog box opens.
3. Next to **Encryption**, select **OFF**.
4. Click the **Submit Encryption Settings** button.

   After turning off encryption, no further data will be encrypted.

6

Monitoring the DR Series System

NOTE: The topics in this section apply to physical DR Series systems. The virtual DR Series system, DR2000v, may have different options available. For details, see the *Dell DR2000v Deployment Guide* for your specific VM platform and the *Dell DR Series System Interoperability Guide*. For more information on the DR Series system CLI commands, see the *Dell DR Series System Command Line Reference Guide*.

This topic introduces the ways in which you monitor the current state of DR Series system operations using the **Dashboard** page options in the navigation panel. The **Dashboard** page displays a summary of current system status categories (**System State**, **HW State**, **Number of Alerts**, and **Number of Events**. In addition, this page displays **Capacity**, **Storage Savings**, and **Throughput**), and includes the **System Information** pane. There are links to other system pages (the **Health**, **Alerts**, and **Events** pages) that you can use to display the current state of the system health (by the status of its components), display the current system alerts, and current system events for your DR Series system.

Monitoring Operations Using the Dashboard Page

The **Dashboard** page contains system status indicators for the current state of the DR Series system (**System State**), current hardware state (**HW State**), current number of system alerts (**Number of Alerts**), and current number of system events (**Number of Events**). The **Dashboard** page also contains data graphs that display:

- **Capacity**—used space, free space, and used and encrypted space in percentage (graphical) and total (in Gibibytes or Tebibytes).
- **Storage Savings**—total savings in percentage based on time (in minutes), which can be displayed in 1h (1–hour, which is the default), 1d (1–day), 5d (5–day), 1m (1–month), or 1y (1–year) durations.
- **Throughput**—for reads and writes in volume based on time (in minutes), which can be displayed in 1h (1–hour, which is the default), 1d (1–day), 5d (5–day), 1m (1–month), or 1y (1–year) durations.

The **Dashboard** page also displays a System Information pane that lists key information about this DR Series system (such as product name, system name, software version, and a number of other key categories). For details about the System Information pane, see System Information Pane.

System Status Bar

The **Dashboard** page contains a System Status pane with icons that indicate the current system status and provide links for more DR Series system status information:

- **System State**
- **HW State** (with a link to the **Health** page)
- **Number of Alerts** (with a link to the **Alerts** page)
- **Number of Events** (with a link to the **Events** page)

For more detailed information about the System Status pane icons:

- **System State**, see Monitoring System Usage.
- **HW State**, see Monitoring System Health.

- **Number of Alerts**, see Monitoring System Alerts.
- **Number of Events**, see Monitoring System Events.

Location	Status Icon	Description
System Status bar	✓	Represents an optimal state.
System Status bar	⚠	Represents a warning state (a non-critical error was detected).
System Status bar	✖	Represents an actionable state (a critical error was detected).

NOTE: To display specific information about the current **HW State**, click the link to display the **Health** page. The **Health** page displays the current status of the DR Series system hardware and expansion shelf enclosures (if installed): front and rear chassis views, showing hard drive, power supply, cooling fan, and connection locations. The System Hardware Health pane for the DR Series system provides status for the power supplies, cooling fans, temperature, storage, voltage, network interface cards (NIC), CPU, DIMM, and NVRAM. The System Hardware Health pane for the external expansion shelf enclosures provides status for the power supplies, cooling fans, temperature, storage, and the Enclosure Management Module (EMM).

NOTE: To display more information about the current **Number of Alerts**, click the link to display the **Alerts** page. The **Alerts** page displays the total number of alerts, and lists each system alert by index number, timestamp, and message that briefly describes alert status.

NOTE: To display more information about the current **Number of Events**, click the link to display the **Events** page. The **Events** page displays the total number of events, and lists each system event by index number, severity (critical, warning, and informational), timestamp, and a message that briefly describes event status.

DR Series System and the Capacity-Storage Savings-Throughput Panes

There are three central panes in the **Dashboard** page that display data graphs which illustrate the current DR Series system status for **Capacity**, **Storage Savings**, and **Throughput**:

- **Capacity**—displays the used and free physical storage capacity in percentages and volume in Gibibytes and Tebibytes (GiBs and TiBs).
- **Storage Savings**—displays a total savings in percentages (combining both deduplication and compression) over a time period (in minutes).
- **Throughput**—displays the throughput volume in Mebibytes/second (MiB/s) for read and write operations over a time period (in minutes).

NOTE: For both the **Storage Savings** and **Throughput** data graphs, you can choose to display the current values in 1h (1-hour, the default), 1d (1-day), 5d (5-days), 1m (1-month), and 1y (1-year) durations.

System Information Pane

Located in the lower part of the **Dashboard** page, the System Information pane displays the following categories of current system information:

- **Product Name**
- **System Name**
- **Software Version**

- **Current Date/Time**
- **Current Time Zone**
- **Cleaner Status**
- **Total Savings** (in percentage)
- **Total Number of Files in All Containers**
- **Number of Containers**
- **Number of Containers Replicated**
- **Active Bytes** (total bytes before optimization)
- **Advanced Data Protection** (status of data integrity check)
- **Encryption Status** (such as Done, Running, Pending, or Disabled)

NOTE: To display additional information about certain elements in the DR Series system GUI, click the corresponding Question Mark (?) icon.

Monitoring System Alerts

You can monitor the DR Series system alerts and display the current state of the system using the navigation panel, the **Dashboard** page, and its options:

- Using the **Dashboard** page, you can access the **Alerts** page via the **Number of Alerts** link.
- Using **Dashboard**→ **Alerts**, you can access the **Alerts** page from the navigation panel.
- The Alerts page lists the number of system alerts, the current time zone, and provides a summary table of alerts defined by index number, timestamp of the system alert, and a brief message describing the alert. For more information, see Displaying System Alerts.

Using the Dashboard Alerts Page

To use the **Dashboard** page to display the current number of system alerts, complete the following:

NOTE: This method in convenient when you are already at the **Dashboard** page and want to quickly display more information about system alerts.

1. Click **Number of Alerts** on the **Dashboard** page.

   The **Number of Alerts** in the System Status bar provides a link (which indicates the number of alerts, in this case 2 alerts, which are listed in the **Number of Alerts: 2** link).
2. Click the **Number of Alerts** link (in this example, **2**).

   The **Alerts** page is displayed.
3. View the list of system alerts in the System Alerts summary table, identified by index number, timestamp, and a brief message that describes the alert.

   For more information, see Dashboard Page and Options and Displaying System Alerts.

Viewing the System Alerts

To use the DR Series navigation panel to display the current number of system alerts, complete the following:

1. Click **Dashboard** → **Alerts** in the navigation panel.

   The **Alerts** page is displayed, which lists the number of system alerts in the System Alerts summary table, and provides the current timezone (for example, US/Pacific).
2. Review the system alerts listed in the System Alerts summary table, which identifies each alert by:

- Index number (for example: 1, 2, ...).
- Timestamp (in yyyy-mm-dd hh:mm:ss format; for example, 2012–10–30 10:24:53).
- Message (a brief description of the alert; for example, *Network Interface Controller Embedded (LOM) Port 2 disconnected. Connect it to a network and/or check your network switches or routers for network connectivity issues*).

Monitoring System Events

You can monitor the DR Series system events, and filter events you want to display using the Event Filter pane in the **Events** page. This page can display **All** system events, or you can restrict the events to only one of the following types: **Info** (Informational), **Warning**, or **Critical** events.

The **Events** page lets you search for system events and monitor the current state of the DR Series system based on the system events that match your search criteria. For more information about using the Event Filter pane, see Using the Event Filter.

To monitor the system, using either of the following methods to display the **Events** page:

- In **Dashboard** page, click the **Number of Events** link in the **Events** page.
- In the navigation panel, click **Dashboard** → **Events** to display the **Events** page.

Using the Dashboard to Display System Events

To use the **Dashboard** page to display the current number of system events (**Number of Events**), complete the following:

NOTE: This method in convenient when you are already at the **Dashboard** page and want to display the current system events.

1. In the **Dashboard** page, click the **Number of Events** link in the System Status bar (for example, **Number of Events: 2**).

   The **Events** page is displayed and lists the total number of current events, the Event Filter, the Events summary table, and the current time zone.
2. In the Event Filter pane, you can select to filter events by using the **Event Severity** pull-down list, and setting the **Timestamp From** and **Timestamp To** starting and ending setpoints.
3. In the **Event Severity** pull-down list, select the severity level of events that you want to filter and display (**All**, **Critical**, **Warning**, or **Info**).
4. In **Message Contains**, enter a word or string of words you want to search for in the **Message** text field, and the DR Series system will perform a case-insensitive match for your entry (no other search options are supported). Matches are displayed in the Events summary table.
5. In **Timestamp From**, click in the field or click the calendar icon to display the current month and day.
   - Click and select a day in the current month schedule (or use the left and right arrows in the month title to select a previous or later month, respectively).
   - Use the **Hour** and **Minute** sliders to set the desired time in hours and minutes, or click **Now** to use the current time.
   - When configured, click **Done**.
6. In **Timestamp To**, click in the field or click the calendar icon to display the current month and day.
   - Click and select a day in the current month schedule (or use the left and right arrows in the month title to select a previous or later month, respectively).
   - Use the **Hour** and **Minute** sliders to set the desired time in hours and minutes, or click **Now** to use the current time.
   - When configured, click **Done**.
7. Click **Start Filter** to display system events in the Events summary table based on the settings you selected.

The Events summary table displays system events based on **Index**, **Severity**, **Timestamp**, and **Message** (a brief description of event). To navigate and display results in the Events summary table, complete the following:

- Set the number of events to display per page: click **Events per page** at the lower-right corner of the table and select either **25** or **50** events to display per page.
- Use the scroll bar to display each full page of system events.
- To display other pages of system events, click **prev** or **next**, click on a specific page number, or enter a page number in the **Goto page** and click **Go** to display that page of system events.

8. To clear the current filter settings, click **Reset** and set new filter values using the process described in steps 3 through 6.

   For more information about using the Event Filter on the **Events** page, see Using the Event Filter.

Using the Dashboard Events Option

To use the DR Series navigation panel to display the current number of system events, complete the following:

1. Click **Dashboard**→ **Events** in the navigation panel.

   The **Events** page is displayed, which lists the total number of system events in the System Events summary table, and provides the current timezone (for example, US/Pacific).
2. View the list of current system events in the System Events summary table, which are grouped by index number, severity, timestamp, and a brief description of the event message.
3. Use the **Event Filter** to search for events that match the criteria you select (event severity, message content, timestamp from, and timestamp to ranges).

   For more information on using the **Event Filter**, see Using the Event Filter and Using the Dashboard to Display System Events.

Using the Event Filter

The **Events** page contains an Event Filter pane that lets you filter the type of system events you want to display in the Events summary table. Event filtering is done by selecting the severity level and using a timestamp. Choose the severity level by selecting it in the **Event Severity** drop-down list, and refine your search by selecting specific start and end setpoints in **Timestamp from** and **Timestamp to**.

To filter the system events you want to display in the Events summary table, complete the following:

1. Click **Dashboard** → **Events** (or access the **Events** page via the **Number of Events** link).

   The **Events** page is displayed, which lists the number of current events and the current time zone set for the system.
2. In the Event Filter pane, select the desired severity to display from the **Event Severity** drop-down list.

   System event severity levels include:

   - **All**—displays all four types of system events (All, Critical, Warning, and Info)
   - **Critical**—displays only critical events (in red)
   - **Warning**—displays only warning events (in yellow)
   - **Info**—displays only informational events
3. In **Message Contains**, enter a word or string of words that you want to search for in the **Message** text field, and the DR Series system will perform a case-insensitive match for your entry (no other search options are supported). Matches are displayed in the Events summary table.
4. Click the **Calendar** icon (adjacent to **Timestamp From**) to configure a start setpoint.

   To configure a start setpoint, complete the following:

   - Select the desired day in the current month, or click the left or right arrow in the month title bar to select a previous or later month.

- Adjust the **Hour** and **Minute** sliders to the desired time (or click **Now** to set the date and time as the current date and time in hours and minutes).
- Click **Done**.

5. Click the **Calendar** icon (adjacent to **Timestamp To**) to configure an end setpoint.

   To configure an end setpoint, complete the following:

   - Select the desired day in the current month, or click the left or right arrow in the month title bar to select a previous or later month.
   - Adjust the **Hour** and **Minute** sliders to the desired time (or click **Now** to set the date and time to be the current date and time in hours and minutes).
   - Click **Done**.

6. Click **Start Filter** (or click **Reset** to return all values to default values).

   The search results based on your filter choices are displayed in the Events summary table.

For more information about using the Events summary table, see Using the Dashboard to Display System Events.

Monitoring System Health

Monitor and display the current state of your system hardware status using the following methods in the DR Series system:

- Using **Dashboard→ Health** , you can access the **Health** page from the navigation panel.
- In the **Dashboard** page, you can access the **Health** page via the **HW State** link.

For more information about the **Health** page, see Health.

Using the Dashboard Page to Monitor System Health

To use the **Dashboard** page to display and monitor the current DR Series system hardware status, complete the following:

1. Click **Dashboard** in the navigation panel.

   The **Dashboard** page is displayed and provides a **HW State** link in the System Status bar (for example, **HW State: optimal**). (You can also access the **Health** page when you click **Dashboard→ Health**.)

2. Click the **HW State** link (in this example, optimal) to display the **Health** page.

   The **Health** page provides a **System** tab, which is the default displayed on this page. If you have installed at least one enclosure, your system will also include an **Enclosure** tab. The **System** tab displays front and rear views of the chassis showing the disk drive locations in the front view (0–11), the OS internal drives (12–13), and the fans, system connectors, and power supplies in the rear view. If installed and clicked, the **Enclosure** tab displays front and rear views of the enclosure chassis showing the physical disk locations (0–11) in the front view, and the enclosure connectors, fans, and pluggable drive locations in the rear view. In addition, the service tag of the expansion shelf is displayed. Both the **System** and **Enclosure** tabs display the System Hardware Health summary table that lists the current status of all major components in the DR Series system or its expansion shelf, respectively.

   NOTE: This method is convenient when you are already at the **Dashboard** page and want to display more information about current System Status.

   DR Series system — System Hardware Health components

   - Power Supplies
   - Fans

- Temperature
- Storage
- Voltage
- NIC
- CPU
- DIMM
- NVRAM

Enclosure — System Hardware Health components

- Power Supplies
- Fans
- Temperature
- Storage
- Enclosure Management Module (EMM)

Using the Dashboard Health Options

To use the navigation panel to display the current system status of the DR Series system components (or any expansion shelf enclosure) that are installed, complete the following:

1. Click **Dashboard** → **Health**.

   The **Health** page is displayed.
2. Mouse over the chassis front and rear panel views on the **Health** page to display a dialog with the status, name, and state for the DR Series system disk drives and OS drives.

   Use the same process to display a similar dialog with the status and name for the power supplies and rear panel connectors for an expansion shelf enclosure.
3. View the status in the System Hardware Health summary table for all of the DR Series system or expansion shelf components (depending upon the tab selected, **System** or **Enclosure**).

   To display additional information, click to expand each component in the corresponding summary table.

For more information about the system components and the **Health** page, see Health, Monitoring System Health, and Using the Dashboard Page to Monitor System Health.

Understanding DR Series System NICs And Ports

The DR Series system supports the use of the following types of NICs:

- 1-Gigabit Ethernet (GbE) two-port (10-Base T); Dell recommends using CAT6a copper cabling
- 10-GbE two-port (100-Base T); Dell recommends using CAT6a copper cabling
- 10-GbE SFP+ two-port using LC fiber-optic transceivers or twin-axial cabling

The 1-GbE, 10-GbE, and 10-GbE SFP+ NICs configurations bond multiple Ethernet ports into a single interface by default:

- For the 1-GbE ports, this means that the four ports in the DR4000 system (or the six ports in the DR4100/DR6000 system) are bonded together to form one interface connection.
- For the 10-GbE and 10-GbE SFP+ ports, this means that to operate at maximum speed, only the two high-speed Ethernet ports are bonded together to form one interface connection.

The DR Series system supports configuring the NICs to use either of the following supported bonding configurations:

- **ALB**—adaptive load balancing (ALB) is the default; this configuration does not require special switch support, but it does require the data source machine to be on the same subnet as the DR Series system. The ALB is mediated by the Address Resolution Protocol (ARP).
- **802.3ad**—also known as Link Aggregation Control Protocol (LACP) is used for copper-wired Ethernet applications; this configuration does require special switch management (the requirement being that it be managed from the switch).

For more information, see Configuring Networking Settings.

ALB and the 802.3ad are link aggregation methods that aggregate or combine multiple network connections in parallel to increase throughput beyond what a single connection could support.

Link aggregation for Ethernet connections also provides redundancy, in case one of the links fails. The DR Series system also comes with a Serial-Attached SCSI (SAS) card for future enhancements.

The DR Series system ships equipped with the 1-GbE, I-GbE, or 10-GbE SFP+ NIC. To visually differentiate between the NIC types, observe the markings on the NICs installed in the rear chassis of the DR Series system:

- 1-GbE NIC is labeled as GRN=10 ORN=100 YEL=1000
- 10-GbE NIC is labeled as 10G=GRN 1G=YLW

NOTE: There are two key requirements to meet if you use the 10-GbE NIC configuration: 1) use only CAT6a copper cabling, and 2) you must have two switch ports capable of supporting 10-GbE NICs.

NOTE: There are two key requirements to meet if you use the 10-GbE SFP+ NIC configuration: 1) use only Dell-supported SFP+ transceivers, and 2) you must have two switch ports capable of supporting 10-GbE SFP+ NICs (and LC fiber-optic or twin-axial cabling).

To verify the types of NICs that are installed in your system, click **System Configuration** → **Networking** to display the NIC information. For more information, see Configuring Networking Settings. In addition, you can also use the DR Series system CLI **network --show** command to display other NIC-related information.

Monitoring System Usage

To display the current DR Series system usage, click **Dashboard** → **Usage** to display the **Usage** page. This page allows you to monitor system status and the currently displayed system usage status is based on the **Latest Range** or **Time Range** settings that are in effect. These settings define the output for the following tab categories on the **Usage** page:

- **CPU Load**
- **System**
- **Memory**
- **Active Processes**
- **Protocols**
- **Network**
- **Disk**
- **All** (displays all system status categories)

Displaying Current System Usage

To display the current usage for a DR Series system, complete the following:

1. Click **Dashboard** → **Usage**.

The **Usage** page is displayed.

2. View the current system usage based on the current **Latest Range** or **Time Range** values in effect (the default is the last 1-hour period). By default, the **CPU Load** is always the first tab that displays when the **Usage** page is selected.

   The tabs you can display in the **Usage** page include: **CPU Load**, **System**, **Memory**, **Active Processes**, **Protocols**, **Network**, **Disk**, and **All**. For more information, see System Usage.

3. Click any of the system usage tabs to display the current status for that tab category (or click **All** to display all of the system usage tab results).

   For example, click **Protocols** to display the current results for the **NFS Usage - Total**, **CIFS Usage - Total**, and **RDA Usage - Total** for the system.

Setting a Latest Range Value

To set a **Latest Range** value and display system status results based on this setting, complete the following:

1. Click **Dashboard** → **Usage**.

   The **Usage** page is displayed.

2. Click **Latest Range**.
3. Select the desired duration period (**Hours**, **Days**, or **Months**) in the **Range** drop-down list.

   By default, **Hours** is the first displayed duration option in the drop-down list.

4. Select a value in the **Display last...** drop-down list that matches the **Range** duration time period you selected.

   For example, **Hours** (the default display period shown) lists choices between 1-24. If **Days** is selected, the choices listed are between 1-31, and if **Months** is selected, the listed choices are between 1-12.

5. Click **Apply**.
6. Click the tab that corresponds to the usage type you want to view based on the selected settings (or click **All** to display all of the system results based on the selected settings).

Setting a Time Range Value

To set a **Time Range** value and display system status results based on these settings, complete the following:

1. Click **Dashboard** → **Usage**.

   The **Usage** page is displayed.

2. Click **Time Range**.
3. In **Start Date**, click the **Start Date** field (or **Calendar** icon) to display the current month.

   To select a previous month, click the left arrow in the month title bar to select the desired month in the current year (or previous year).

4. To choose the **Start Date** day in the selected month, you have two options:

   - Choose a specific day in the selected month (only the available days are displayed). Future days are considered unavailable (and appear dimmed out).
   - Click **Now** to select the current date and time in **Hours** and **Minutes** (or use the **Hour** and **Minute** sliders to select a desired time value).

5. Click **Done** to display your date and time settings in **Start Date**.

   The date and time settings you set appear in an mm/dd/yyyy hh:mm AM/PM format.

6. In **End Date**, perform the same process that you did for setting the **Start Date** to specify an end date (or select **Set "End Date" to current time**).
7. Click **Apply**.
8. Click the tab that corresponds to the usage type you want to monitor using your choice of settings (or click **All** to display all of the system usage tab results based on your choice of settings).

9. Observe the DR Series system usage results based on the criteria selected.

Monitoring Container Statistics

Click **Dashboard** → **Container Statistics** to monitor statistics for a selected container. Current statistics are displayed in the following panes on this page:

- **Backup Data**
- **Throughput**
- **Marker Type**
- **Connection Type**
- **Replication** (if enabled)
- **Library/Slots/Access Control List** (for VTL type containers only)

For more information, see Editing Container Settings.

Displaying the Container Statistics Page

To display container statistics for a selected container, complete the following:

1. Click **Dashboard**→ **Container Statistics**.

   The **Container Statistics** page is displayed.
2. In the **Container Name:** drop-down list, select the container for which you want to view statistics.

   NOTE: When you select a container, all statistics displayed on the **Container Statistics** page represent specific information about the backup data, throughput, replication, marker type, and connection type for the selected container. The displayed statistics will vary depending upon the connection type used by the specified container.
3. View the current statistics in the Backup Data and Throughput panes.

   The Backup Data pane displays the number of active files ingested based on time (in minutes), and the number of active bytes ingested based on time (in minutes). The Throughput pane displays the number of read data in Mebibytes/per second (MiB/s) based on time (in minutes), and the number of write data in MiB/s based on time (in minutes).

   NOTE: The Current Time Zone for the DR Series system is displayed below the Backup Data pane (for example, System Time Zone: US/Pacific).
4. In the Backup Data and Throughput panes, click **Zoom** to select the duration period you want to display from the following options:

   - 1h (1-hour is the default duration displayed)
   - 1d (1-day)
   - 5-d (five-day)
   - 1m (1-month)
   - 1y (1-year)

   NOTE: To refresh the values listed in the Backup Data and Throughput panes, click ⟳ .
5. The Marker Type pane displays the marker type associated with the container. For details, see Creating Storage Containers.

6. In the Connection Type pane, you can view information about the configured connection type for the selected container which can be NFS, CIFS, NDMP, iSCSI, RDS, or OST. The type of information displayed can be different depending on the connection type. For example, the following information is displayed:

    - NFS Connection Configuration pane—NFS access path, Client Access, NFS Options, Map root to, and NFS Write Accelerator (DR6000 only).
    - CIFS Connection Configuration pane—CIFS share path, Client Access, and CIFS Write Accelerator (DR6000 only).
    - For VTL containers with a connection type of NDMP or iSCSI, the Connection Type pane displays the tape size and also contains the following three tabs:
        - **Library** — displays information in a table about the vendor and model information for medium changer and tape drives. The Info Column in the first row of the table indicates the total number of tapes and tape size of the VTL container.
        - **Access Control List** — For NDMP connection types, displays the IP address or the FQDN of the DMA that has access to this VTL container, or, for iSCSI connection types, displays the "Inititators Allowed" for the container.
    - If the container is an RDA connection type container, the Connection Type OST pane or Connection Type RDS pane displays the following three tabs:
        - **Capacity** — displays a Capacity pane with Status, Capacity, Capacity Used, and Total Images
        - **Duplication**
          — displays a Duplication Statistics pane with Inbound and Outbound statistics in the following categories: Bytes Copied (logical), Bytes Transferred (actual), Network Bandwidth Settings, Current Count of Active Files, and Replication Errors.
        - **Client Statistics** — displays a Client Statistics pane with Images Ingested, Images Complete, Images Incomplete, Images Restored, Bytes Restored, Image Restore Errors, Image Ingest Errors, Bytes Ingested, Bytes Transferred, and Network Savings.

7. In the Replication pane (if enabled for NFS/CIFS connection types), you can click the link for a container to view the replication information for that container. When you click the link, the Replication Statistics page opens for the selected container.

Monitoring Replication Statistics

Click **Dashboard** → **Replication Statistics** to display and monitor replication statistics for one (or more) containers, and one (or more) peer DR Series systems selected in the Replication Filter pane. Depending upon the configured settings, you can monitor and display replication statistics for:

- All containers
- One or more specific containers
- One or more peer DR Series systems

The Replication Filter pane contains 10 Headers check boxes that when selected display replication statistics for the container(s) or other peer DR Series system(s) you select in **Container Filter**.

After selecting the container(s), peer system(s), and the replication statistic categories, click **Apply Filter** to display the replication statistics results based on the search criteria you selected.

Using the **Replication Statistics** page, you can selectively filter and display specific types of related replication statistics for all, one or more than one container, or one or more other peer DR Series systems.

For more information about Replication statistics, see Displaying Replication Statistics, Container Filter, and Displaying the Replication Statistics Page.

Displaying the Replication Statistics Page

To display system replication container statistics for a selected container or another DR Series system, complete the following:

1. Click **Dashboard→ Replication Statistics**.

   The **Replication Statistics** page is displayed.
2. To select a container or another peer DR Series system, choose the appropriate **Container Filter** option.

   - Click **All** to choose all of the replication containers.
   - Click **Name**, press **Ctrl**, and select the containers in the list box to select one or more containers in the list that you want to display.
   - Click **Peer System**, press **Ctrl**, and select the peer systems in the list box to select one or more peer DR Series systems in the list that you want to display.

   NOTE: Only one of the **Container Filter** options can be active at any one time (they are mutually exclusive).
3. Select the **Header** check box(es) for the replication statistics categories for which you want to filter and display in the Replication Statistics summary table:

   - **Peer Status**
   - **Replication Status**
   - **Time to Sync**
   - **Progress %** (percentage)
   - **Replication Throughput**
   - **Network Throughput**
   - **Network Savings**
   - **Last Sync in Time**
   - **Peer Container**
   - **Peer Status**

   NOTE: The following five types of replication statistics are enabled by default: **Peer Status**, **Replication Status**, **Network Throughput**, **Network Savings**, and **Progress %**. If you choose more than five types of statistics (when you select additional check boxes), a horizontal scroll bar appears at the bottom of the Replication Statistics table. Use this scroll bar to display the columns of additional statistics that may not display within the main window.
4. Click **Apply Filter** to display the replication statistics types you selected to filter for your container or other peer DR Series system choices.

   The Replication Statistics summary table displays the replication statistics types you selected in the Replication Filter pane.

   To reset the default settings in the Replication Filter pane, click **Reset**.

   To update the Replication Filter table after making a change, click **Apply Filter** to display an updated set of replication statistics.

   NOTE: Use the horizontal and vertical scroll bars to navigate through the columns of replication statistics displayed in the Replication Statistics summary table.

NOTE: You can set up nightly replication statistics notification mails using the `alerts --email --daily_report yes` command. For more information, see the *Dell DR Series Systems Command Line Interface Guide* at **dell.com/support/manuals**.

Displaying Replication Statistics Using the CLI

In addition to using the DR Series system GUI to display replication statistics, you can also display statistics for a specific replication container by using the DR Series system CLI **stats --replication --name <container name>** command to view the following replication container statistics categories:

- Container Name (name of the replication container)
- Replication Source Container (name that identifies the data source)
- Replication Source System (IP address or host name of the data source)
- Peer Status (current status of replication peer; for example, paused)
- Replication State (current state of replication relationship; for example, insync)
- Schedule Status (current status in days, hours, minutes, seconds)
- Replication Average Throughput (in Kebibytes per second, KiB/s)
- Replication Maximum Throughput (in KiB/s)
- Network Average Throughput (average throughput rate in KiB/s)
- Network Maximum Throughput (maximum throughput rate in KiB/s)
- Network Bytes Sent (total network bytes sent in Mebibytes/MiB)
- Dedupe Network Savings (total deduplication network savings in percentage)
- Compression Network Savings (total compression network savings in percentage)
- Last INSYNC Time (date of last sync operation in yyyy-mm-dd hh:mm:ss format)
- Estimated time to sync (time until next sync operation in days, hours, minutes, and seconds)

Data replication history is also displayed on a file-by-file basis, with a replication timestamp, and other file related information.

For more information about DR Series system CLI commands, see the *Dell DR Series System Command Line Reference Guide*.

7

Using Global View

This topic describes how to monitor and navigate to multiple DR systems in your enterprise using the Global View feature, which provides a real-time view of multiple DR systems in your enterprise.

About Global Views

The Global View is a dashboard that provides a holistic picture of all DR Series systems added to it, making it easy to monitor and manage remote systems. For example, suppose you are an administrator in a headquarters office with a DR Series system. You have three branch offices, each with two DR units that replicate to the headquarters office. You can use Global View to monitor all of the branch office units (as well as your headquarters unit) on a single page. A drop-down list and links provide easy navigation to any DR system in the view.

Following are tips and constraints for using Global View:

- For streamlined navigation, your location in the GUI is saved when you navigate between DR systems in the dashboard. For example, suppose you are on the **Software Upgrade** page in one DR system. When you navigate to another DR system from the Global View page, the **Software Upgrade** page of the new DR system appears.
- The Global View dashboard on a DR Series system is local to that system; the Global View information is maintained in a physical file on the system. If the machine goes down or is otherwise unavailable, the Global View is unavailable. In addition, if a factory refresh is performed on the machine, the Global View information will be lost and you must re-add the machines to the Global View dashboard.
- You can define an identical Global View on another DR system in your domain to serve as a backup if the DR system that contains the original Global View is down or otherwise unavailable. For example, suppose you have three DR Series systems: A, B, and C. All of these are on the same Active Directory Services (ADS) domain and have identical login credentials. You log in to DR Series system A, and on its Global View page, you add DR Series systems B and C (resulting in A, B, and C being in the view). Then you log in to DR Series system B and add A and C to its Global View page (also resulting in A, B, and C being in the view).
- You cannot import or export a Global View dashboard configuration. To create a Global View, you must manually define it by adding machines to the Global View dashboard. For details, see Adding a DR Series System to Global View .
- The DR2000v is able to be monitored in Global View by the hardware DR Series appliances to which is it registered.

NOTE: If you are using Internet Explorer 10, it is recommended that you disable the pop-up blocker to allow DR units to open in new browser windows when you navigate to them within Global View.

Prerequisites

The Global View feature is available on all DR Series systems that have version 3.0.0.1 (or newer) software installed. The system to which you are currently logged in is automatically included by default in the **Global View** page; however, any other systems must be explicitly added. For details, see Adding a DR Series System to Global View.

Following are the prerequisites that must be met in order to successfully add and view your DR Series systems in the **Global View** page.

- All DR Series systems must have the same version of 3.x software installed. Systems running older software versions cannot be added to the **Global View** page.

- All DR Series systems must be in the same Active Directory Services (ADS) domain, in the same login group, and have identical login credentials. This includes the system to which you are currently logged in. For details, see the procedures that follow.
- When you use Global View, you must log in to the DR Series system using your domain credentials; for example, you must log in as DOMAIN\Administrator instead of Administrator.

Configuring Active Directory Settings

You need to configure the Active Directory setting to direct your DR Series system to join or leave a domain that contains a Microsoft Active Directory Service (ADS). To join an ADS domain, complete steps 1 through 4 in the following procedure (to leave an ADS domain, skip to step 5). When you join the DR Series system to an ADS domain, this disables the Network Time Protocol (NTP) service and instead uses the domain-based time service.

NOTE: If you use the command line interface (CLI) to join the DR Series system into the domain, you might notice that Global View contains multiple, unnecessary entries. Dell recommends that you use the DR Series system GUI (and not CLI commands) for Global View related operations, including domain join/leave.

To configure the DR Series system for a domain using ADS, complete the following:

1. Select **System Configuration** → **Active Directory**.

   The **Active Directory** page is displayed.

   NOTE: If you have not yet configured ADS settings, an informational message is displayed in the **Settings** pane in the **Active Directory** page.
2. Click **Join** on the options bar.

   The **Active Directory Configuration** dialog is displayed.
3. Type the following values in the **Active Directory Configuration** dialog:

   - In **Domain Name (FQDN)**, type a fully qualified domain name for the ADS; for example, **AD12.acme.com**. *(This is a required field.)*

     NOTE: Supported domain names are limited to 64 characters in length and can only consist of a combination of A-Z, a-z, 0-9, and three special characters: a dash (-), a period (.), and an underscore (_).
   - In **Username**, type a valid user name that meets the user name guidelines for the ADS. *(This is a required field.)*

     NOTE: Supported user names are limited to 64 characters in length and can only consist of a combination of A-Z, a-z, 0-9, and three special characters: a dash (-), a period (.), and an underscore (_).
   - In **Password**, type a valid password that meets the password guidelines for the ADS. *(This is a required field.)*
   - In **Org Unit**, type a valid organizational name that meets the organization name guidelines for the ADS. *(This is an optional field.)*
4. Click **Join Domain** to configure your system with these ADS settings (or click **Cancel** to display the **Active Directory** page).

   The **Successfully Configured** dialog is displayed when successful.

   NOTE: If you configure CIFS container share paths, these will be displayed in a CIFS Container Share Path pane in the **Active Directory** page.
5. To leave an ADS domain, click **Leave** in the **Active Directory** page.

   The **Active Directory Configuration** dialog is displayed.
6. Leaving the configured ADS domain requires that you enter the following:

   a. In **Username**, enter a valid user name for the ADS domain.

   b. In **Password**, enter a valid password for the ADS domain.
7. Click **Leave Domain** to direct your DR Series system to leave the ADS domain (or click **Cancel** to display the **Active Directory** page).

   The **Successfully Configured** dialog is displayed when successful.

Adding a Login Group in an ADS Domain

After you configure your DR systems within the same ADS domain, you must ensure that a login group exists and add it to the domain.
Adding a login group is only possible when the DR Series system is already joined to a domain. Also, you must be logged in as a domain user that is part of an enabled login group.
To add a login group in an ADS domain, complete the following:

1. Select **System Configuration** → **Active Directory**.

   The **Active Directory** page is displayed. Under **Settings**, “Active Directory is configured” should be displayed; if not, you must configure your ADS domain before proceeding.
2. Click **Add Login Group** on the options bar.

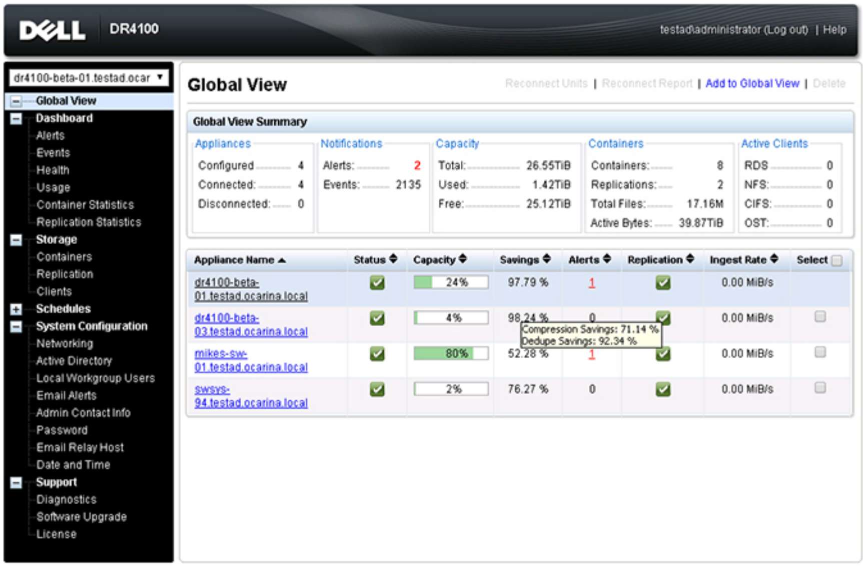
   The **Active Directory Configuration** dialog is displayed.
3. In **Login Group**, type the name of the login group including the domain name; for example, **Domain\Domain Admins**. If your login group name contains spaces, you must not enclose it in quotation marks. (This differs from the equivalent CLI command.)
4. Click **Add Login Group** to add the login group (or click **Cancel** to display the **Active Directory** page).

   If the addition is successful, a confirmation message displays.

Changes made to the login group take effect on the next log in attempt (no active checking is done on the group, which matches how Windows ADS works).

About the Global View Page

The **Global View** page displays a dashboard of operating statistics for all of the DR Series systems that you have added to the view. From this page, you can monitor the status of your enterprise as well as easily navigate to any DR Series system in your enterprise.



Global View

Global View Summary

Appliances
Configured 4
Connected: 4
Disconnected: 0

Notifications
Alerts: 2
Events: 2135

Capacity
Total: 26.55TiB
Used: 1.42TiB
Free: 25.12TiB

Containers
Containers: 8
Replications: 2
Total Files: 17.16M
Active Bytes: 39.87TiB

Active Clients
RDS 0
NFS: 0
CIFS: 0
OST: 0

Appliance Name	Status	Capacity	Savings	Alerts	Replication	Ingest Rate	Select □
dr4100-beta-01.testad.ocarina.local	☑	24%	97.79 %	1	☑	0.00 MiB/s	
dr4100-beta-03.testad.ocarina.local	☑	4%	98.24 %	0	☑	0.00 MiB/s	□
mikes-sw-01.testad.ocarina.local	☑	80%	52.28 %	1	☑	0.00 MiB/s	□
swsys-94.testad.ocarina.local	☑	2%	76.27 %	0	☑	0.00 MiB/s	□

Compression Savings: 71.14 %
Dedupe Savings: 92.34 %

Figure 9. Global View Page (DR4100 System)

Global View Summary

NOTE: If an alert is displayed with a message that "Member units will fail to connect because non-Active Directory credentials were used", see Prerequisites.

The following table describes the statistics available in the **Global View Summary**:

NOTE: The statistical values refresh every 15 seconds.

NOTE: If you used the command line interface (CLI) to join the DR Series system into the Active Directory domain, you may notice Global View contains multiple, unnecessary entries. Dell recommends that you use the DR Series system GUI (and not CLI commands) for Global View related operations, including domain join/leave.

Table 2. Global View Summary

Item	Description
Appliances	
Configured	Displays the number of appliances that were added to the Global View (including the system that contains the Global View dashboard)..
Connected	Displays the number of appliances that are currently connected in Global View.
Disconnected	Displays the number of appliances that were added to the Global View, but are unable to be reached. To troubleshoot, see Reconnecting DR Series Systems.
Notifications	
Alerts	Displays the total number of alerts in all appliances in the Global View.
Events	Displays the total number of events in all appliances in the Global View.
Capacity	
Total	Displays the total physical capacity in all appliances in the Global View.
Used	Displays the total physical capacity bytes that are used across all appliances in the Global View.
Free	Displays the total physical capacity bytes that are free across all appliances in the Global View.
Containers	
Containers	Displays the total number of containers in all appliances in the Global View.
Replications	Displays the total number of containers replicated in all appliances in the Global View.
Total Files	Displays the total number of files in all containers in all appliances in the Global View.

Item	Description
Active Bytes	Displays the total bytes before optimization in all appliances in the Global View.
Active Clients	Displays the total clients configured in all appliances in the Global View, organized by container connection type.

Appliance List

This section lists all appliances in the Global View with a high-level snapshot of their status. By default, appliances are listed in alphabetic order by **Appliance Name**. You can sort the list by a particular column by clicking the column header, which toggles between ascending and descending sort order. This sort order is retained even if you leave the page and return later.

NOTE: The information in the appliance list refreshes every 15 seconds.

The following table describes the information displayed in the appliance list:

Item	Description
Appliance Name	Lists the Active Directory fully-qualified domain name (FQDN), and contains links to each respective DR Series system. Hover your mouse over the appliance name to display the following information: • Model • Service Tag • Software Version • Expansion Shelves • iDRAC IP • Management IP • Administrator Contact Information
Status	Displays the system operational state by using an icon. • A green icon ✓ indicates that the system is operational. Hovering your mouse over a green**Status** icon displays the message **Operational**. • A red icon ✖ indicates that the system is not connected. Hovering your mouse over a red **Status** icon displays the message **Connect Failed**. This can occur if the DR Series system is removed from the Active Directory Services (ADS) domain, if it is down, or being rebooted. **NOTE:** If the system administrator re-adds the DR Series system back into the ADS domain, the logged out DR Series system will not automatically be logged back in. In this case, the **Reconnect Units** link will be enabled, and you must manually log in to the DR Series system.
Capacity	Displays the used and free physical storage capacity in percentages and volume in Gibibytes and Tebibytes (GiBs and

Item	Description
	TiBs). The capacity appears as a progress bar with a percentage shown. When the capacity is less than 90%, the capacity bar is green. After the capacity used reaches 90%, the capacity bar is shown in red. Hover your mouse over the **Capacity** percentage bar to display the following information: • Used Capacity (GiB) • Free Capacity (GiB) • Total Capacity (GiB)
Savings	Displays the total savings as a percentage (combining both deduplication and compression) over a time period (in minutes). Hover your mouse over the Savings column value to display the following individual measures: • **Compression Savings:** The percentage of compression savings that was achieved on the data that could not be deduplicated. • **Dedupe Savings:** The percentage of data that was deduplicated.
Alerts	Displays the alert count as a link to the DR Series system's **Alert** page.
Replication	Displays the replication state by using an icon. • A green icon ✓ indicates that replication is operational. Hovering your mouse over a green **Replication** icon displays the number of **Total Containers**, **Configured Replications**, and **Failed Replications**. • A red icon ✗ indicates that replication has failed. Hovering your mouse over a red **Replication** icon displays the message **Replication Failed**.
Ingest Rate	Displays the rate of data being written to the DR Series system across your network. Hover your mouse over the Ingest Rate to display the **Read Throughput** in Megabytes per second.

Navigating in Global View

You can use the Global View navigation features to easily view DR Series systems in your enterprise without having to log out and log on using new browser sessions. To navigate to different DR Series systems in your Global View dashboard, do one of the following:

- In the left navigation pane above **Global View**, use the drop-down list to select the DR Series system that you want to view.
- In the appliance list on the **Global View** page, click the link of the DR Series system in the **Appliance Name** column.

The selected DR Series system is displayed in a new browser window. If you are using Internet Explorer 10, make sure the pop-up blocker is disabled in order to have the selected DR Series system open in a new browser window.

NOTE: When you initially navigate to a DR Series system, you will need to accept a browser certificate exception. After you accept it, the exception does not appear again unless you clear your browser cache.

Adding a DR Series System to Global View

You can add up to 64 machines to your Global View dashboard. This number includes the system on which you are logged in.

Before you add a system to the Global View dashboard, you must have logged in to the system using your domain credentials and have added a login group in the domain. For details, see Prerequisites.

To add a DR Series system to Global View, complete the following:

1. In the left navigation pane, click **Global View**.
2. On the **Global View** page, click **Add to Global View**.

   The Add to Global View dialog box is displayed.
3. In **DR Unit FQDN or IP address**, enter the fully-qualified domain name (FQDN) or IP address of the DR Series system that you want to add. Keep in mind that the system must be in the same ADS domain, in the same login group, and have identical credentials to the system on which you are working.
4. In **Domain Name (FQDN)**, the fully-qualified domain name should be already completed. If not, enter it.
5. In **Username**, enter the domain username for the DR Series system that you want to add. For example, DOMAIN \administrator. This should be identical to the credentials used in all other systems in the Global View.
6. In **Password**, enter the domain password for the DR Series system that you want to add. This should be identical to the credentials used in all other systems in the Global View.
7. Click **Add and Connect**.

   If successful, the Add to Global View dialog box displays “Successfully added DR unit: [name]” and remains open.
8. If you want to add additional systems, repeat the steps. If not, click **Close**.

Removing a DR Series System from Global View

You can remove any DR Series system from your Global View dashboard except the system that contains the Global View dashboard. All other systems are available to be removed from your Global View page.

Keep in mind that when you remove a DR Series system from a Global View dashboard on one system, it does **not** remove it from any other Global View dashboards you may have added it to on other systems.
To remove a DR Series system from Global View, complete the following:

1. In the left navigation pane, click **Global View**.
2. On the **Global View** page, in the appliance list, click the **Delete** checkbox next to the system you want to delete. Note that there is no checkbox next to the system that contains the Global View; it is not available to be removed.
3. At the top of the page, click **Delete**.

   A confirmation prompt is displayed.
4. Click **OK** to confirm the deletion.

   The system is deleted from the Global View dashboard.

Reconnecting DR Series Systems

If a system administrator removes a member DR Series system from the ADS domain or if authentication to a member DR Series system fails (such as when the system is down), then the Global View dashboard displays a red icon in the **Status** column next to the appliance. If one or more red icons are displayed, the **Reconnect Units** link is enabled on the Global View page. To reconnect a DR Series system to the Global View, complete the following:

1. On the Global View page, click **Reconnect Units**.

   The **Reconnect DR Units** dialog box appears.
2. In **Domain Name (FQDN)**, enter the fully-qualified domain name (FQDN) in which the DR Series system resides. Keep in mind that the system must be in the same login group and have identical credentials to the system on which you are working.
3. In **Username**, enter the domain username for the DR Series system. For example, DOMAIN\administrator. This should be identical to the credentials used in all other systems in the Global View.
4. In **Password**, enter the domain password for the DR Series system. This should be identical to the credentials used in all other systems in the Global View.
5. Click **Reconnect**.

   The DR Series system attempts to reconnect only those DR Series systems that are currently disconnected.

The **Reconnect DR Units Report** is displayed, indicating whether the reconnection was successful or unsuccessful. If the reconnect action is successful, the **Status** of the connected DR Series system displays a green icon. However, if there are unresolved underlying issues such as issues with the network connection, issues with a WAN connection, or issues with the DR Series system that prevent a good connection, then the **Reconnect DR Units Report** indicates failure.

Using the Reconnect Report

The Reconnect DR Units Report provides information about your most recent attempt to reconnect DR Series systems. The link to access the Reconnect DR Units Report is only enabled after you attempt to reconnect DR Series systems. To view the Reconnect DR Units Report, complete the following:

1. On the **Global View** page, click **Reconnect Report**.

   The **Reconnect DR Units Report** is displayed. If all DR Series systems were successfully reconnected the last time you clicked **Reconnect Units**, then the report indicates that all DR Series systems were successfully connected. However, if the reconnect failed, then the **Reconnect DR Units Report** displays the FQDNs of the disconnected DR Series systems with a message indicating the issue. For example, the message **No route to host** indicates that the system was unable to ping the DR Series system from the current location because either the system is down, or the router is unable to route traffic to the system.
2. After you review the **Reconnect DR Units Report**, click **Close** to return to the **Global View** page.

8

Using the DR Series System Support Options

You can use the **Support** page and its **Diagnostics**, **Software Upgrade**, and **License** options to maintain the state of your DR Series system. To access these options, use the DR Series system navigation panel (for example, click **Support**→ **Diagnostics** to display the **Diagnostics** page) or use the **Diagnostics**, **Software Upgrade**, or **License** links on the **Support** page.

Support Information Pane

The **Support** page displays the Support Information pane, which provides the following information about the DR Series system:

- **Product Name**—DR Series system product name
- **Software Version**—DR Series system software version installed
- **Service Tag**—DR Series system appliance bar code label
- **Last Diagnostic Run**—timestamp of latest diagnostics log file (for example, Tue Nov 6 12:39:44 2012)
- **BIOS Version**—current version of installed BIOS
- **MAC Address**—current address in standard two-digit hexadecimal grouping format
- **iDRAC IP Address**—current IP address of iDRAC (if applicable)
- **Ethernet Ports**—displays information about bonded ports only (if the 10-GbE NICs are installed, it only displays information about the two supported 10–GbE ports):
  - Eth0 MAC address and port speed
  - Eth1 MAC address and port speed
  - Eth2 MAC address and port speed in
  - Eth3 MAC address and port speed in

  NOTE: This example shows four Ethernet ports bonded (such as if a DR4000 system with 1–GbE ports as a single interface). For more information on possible port configurations, see the system chassis descriptions in Local Console Connection.

NOTE: The Support Information pane contains important information that may be needed if you contact Dell Support for any technical assistance.

NOTE: For additional system information, click **Dashboard** in the navigation panel to display its System Information pane, which lists **Product Name**, **System Name**, **Software Version**, **Current Date/Time**, **Current Time Zone**, **Cleaner Status**, **Total Savings** (in percentage), **Total Number of Files in All Containers**, **Number of Containers**, **Number of Containers Replicated**, and **Active Bytes**.

Diagnostics Page and Options

The options on the **Diagnostics** page allow you to generate new diagnostics log files that capture the current state of your system (**Generate**), download diagnostics log files to the local system (**Download**), or delete existing diagnostics log files (**Delete**).

NOTE: For more information about diagnostics log files, log file directories, and the Diagnostics service, see About The Diagnostics Service.

A DR Series diagnostics log file is a bundle that contains a variety of file types that record the latest system settings, and saves them in a compressed .lzip file format. The **Diagnostics** page identifies each diagnostics log file by the following attributes:

- File name—in this format, <*hostname*>_<*date*>_<*time*>.lzip, as in this example: **acme-sys-19_2012-10-12_13-51-40.lzip**

  NOTE: Diagnostic log file names are limited to 128 characters.
- Size—in Megabytes (for example, 58.6 MB).
- Time—timestamp when log file was created (for example, Fri Oct 12 13:51:40 2012).
- Reason for generation—describes reason log file was generated (for example, [admin-generated]: generated by Administrator).

  NOTE: Diagnostic reason descriptions are limited to 512 characters, and the descriptions can only be added using the DR Series system CLI.
- Status—indicates status of log file (for example, Completed).

There are two methods to display the **Diagnostics** page:

- Using the **Support** page (to access the **Diagnostics** page via the **Diagnostics** link).
- Using **Support** → **Diagnostics** (to access the **Diagnostics** page from the navigation panel).

If you have multiple pages of diagnostics log files, you can navigate to another page by using the controls are the foot of the Diagnostics summary table:

- Click **prev** or **next** to move back or forward one page.
- Double-click the listed page number (adjacent to **Goto** page).
- Enter a page number in **Goto** page, and click **Go**.
- Use the scroll bar at the right side of Diagnostics summary table to view all of the diagnostics log files available to display.

NOTE: You can also set how many entries you want to display per page in the Diagnostics summary table. In the **View per page** drop-down list, click **25** or **50** to select the desired number of entries to display.

Generating a Diagnostics Log File

A DR Series diagnostics log file is a bundle that contains a variety of file types that record the latest system settings, and saves them in a compressed .lzip file format. The **Diagnostics** page identifies each diagnostics log file by the following attribute types:

- File name
- Size
- Time
- Reason for generation
- Status

NOTE: When you generate a diagnostics log file bundle, it contains all of the DR Series system information that may be needed when contacting Dell Support for technical assistance.

The diagnostics log file bundle collects the same type of hardware, storage, and operating system information collected by the Dell System E-Support Tool (DSET) from the Dell DR Series system hardware.

The diagnostics log file bundle is identical to one created using the DR Series system CLI **diagnostics --collect --dset** command. System diagnostics information can assist Dell Support when troubleshooting or evaluating your DR Series system.
To generate a diagnostics log file bundle for your system, complete the following:

1. Select **Support** → **Diagnostics** in the navigation panel.

   The **Diagnostics** page is displayed, and this page lists all current diagnostics log files.
2. Click **Generate**.

   A **New log file is scheduled** dialog is displayed.
3. To verify that a new diagnostics log file is being generated, check the status of the diagnostics log file by selecting **Support** → **Diagnostics**.

   The **Diagnostics** page is displayed, and a status showing **In-progress** indicates that a new diagnostics log file is being generated.

Once completed, the new diagnostics log file resides at the top of the File Name column in the table. To verify, check its timestamp (using its date and time), to ensure this is the latest diagnostics file created.

NOTE: When you generate a diagnostics log file bundle, it contains all of the DR Series system information that may be needed when contacting Dell Support for technical assistance. This also includes all the previous auto-generated diagnostics log files, which are then deleted from the DR Series system.

The diagnostics log file bundle collects the same type of hardware, storage, and operating system information collected by the Dell System E-Support Tool (DSET) from the Dell DR Series system appliance hardware:

- To collect a DSET log file, use the DR Series system CLI command, **diagnostics --collect --dset**.
- To collect the comprehensive DR Series system diagnostics log file bundle (which also includes DSET information), use the DR Series system CLI command, **diagnostics --collect**.

Downloading Diagnostics Log Files

To display the **Diagnostics** page and open or download an existing diagnostics log file, complete the following:

1. Click **Support**→ **Diagnostics** in the navigation panel.

   The **Diagnostics** page is displayed, which lists all current diagnostics log files allowed by the system.
2. Click **Select** to identify the diagnostics log file you want to download, and click **Download** (or single-click the diagnostics log file name link).

   The **File Download** dialog is displayed.

   NOTE: When a new diagnostics log file is in the process of being generated (and its **Status** displays as In-progress), the diagnostic log file name link is not active, and if you attempt to select this file the **Download** option is disabled.
3. Download the file to the desired location, depending upon the following:

   a. If accessing the DR Series system GUI from a Linux-based system: click **Save File** and navigate to a different folder location, define a new file name (or retain the existing file name), and click **Save** to save the diagnostics log file to a specified folder location.

   b. If accessing the DR Series system GUI from a Windows-based system: click **Save** (or **Save As**), and navigate to the **Downloads** folder and retrieve the diagnostics log file.

Deleting a Diagnostics Log File

To delete an existing diagnostics log file from the Diagnostics summary table on the **Diagnostics** page, complete the following:

1. Select **Support** → **Diagnostics**.

   The **Diagnostics** page is displayed.
2. Click **Select** to select the diagnostics file you want to delete, and click **Delete**.

   The **Delete Confirmation** dialog is displayed.
3. Click **OK** to delete the selected diagnostics log file (or click **Cancel** to display the **Diagnostics** page).

   The **Log file was removed successfully** dialog is displayed when successful.

DR Series System Software Upgrade

When you initiate a DR Series system software upgrade, the navigation panel displays only the **Support** page and the **Software Upgrade** options.

The administrator that initiated the software upgrade (considered the initiator administrator) will see a System Information pane that displays an alert that reads `IMPORTANT: Please do not navigate out of this screen until the upgrade is finished`, and displays the upgrade status as `Upgrade in Progress... Please wait....` The Current Version and Upgrade History versions of the DR Series system software are listed in the **Software Info** pane.

All other administrators that may be logged into DR Series system (with the exception of the initiator administrator who started the software upgrade), will only see a dialog that displays `Status: The system is being upgraded. Wait for it to become operational.`

There are only three possible outcomes during a DR Series system software upgrade operation:

- The upgrade operation completed successfully—no reboot is required.
- The upgrade operation completed successfully—but a reboot is required (click **Reboot** in the **Software Upgrade** page).
- The upgrade operation failed.

Software Upgrade Page and Options

Use the **Software Upgrade** page to verify the current installed version of the DR Series system software in the **Software Information** pane, or to apply updates to the system. There are two methods you can use to display the **Software Upgrade** page:

- Using the **Support** page, click **Software Upgrade**.
- Using the navigation panel, select **Support** → **Software Upgrade**.

Both methods display the **Software Upgrade** page where you can verify the current installed version, check the upgrade history of previously installed software versions, verify the iDRAC IP address (if one is in use), start the upgrade process, or reboot the DR Series system using the options on this page.

NOTE: During the DR Series system software upgrade, the upgrade status "starting" remains displayed during almost the entire duration of the software upgrade process. It is not until the DR Series system upgrade status changes to "almost done" that the system upgrade process has fully completed.

Verifying the Current Software Version

To verify the currently installed version of the DR Series system software, complete the following:

NOTE: You can verify the version of the installed DR Series system software in the **Dashboard** page (in the System Information pane), the **Support** page (in the Support Information pane), and the **Software Upgrade** page (in the Software Information pane).

The following procedure documents the process from the **Software Upgrade** page.

1. In the navigation panel, select **Support** and click **Software Upgrade** (or select **Support→ Software Upgrade**).

   The **Software Upgrade** page is displayed.
2. Verify the currently installed DR Series system software version listed as **Current Version** in the Software Information pane (all previously installed versions are listed under **Upgrade History**, showing the version number and timestamp when installed).

Upgrading the DR Series System Software

To upgrade the DR Series system software, complete the following:

NOTE: The DR Series system only supports the copying of upgrade images and diagnostics files to and from the system using WinSCP. The DR Series system does not support the copying or deleting of any other file types using WinSCP. To use WinSCP to copy DR Series software upgrade and diagnostics log files, ensure that the File Protocol mode is set to SCP (Secure Copy) mode.

NOTE: You can use other SCP tools with the DR Series system, but you cannot use these other SCP tools to copy other types of files to or from the DR Series system.

1. Using the browser, go to **support.dell.com**, navigate to your DR Series product page, and enter your service tag.
2. Click **Get Drivers**, then **View All Drivers**.

   The **Drivers & Downloads** page displays a listing of downloadable firmware, utilities, applications, and drivers for the DR Series system.
3. Locate the IDM section of the **Drivers & Downloads** page, which includes the Dell-Utility (DR Series Upgrade File) in the format, **DR-UM-x.x.x.x-xxxxx.tar.gz**, and showing its release date and version.
4. Click **Download File**, click **For Single File Download via Browser**, and click **Download Now**.

   The **File Download** dialog is displayed.
5. Click **Save** to download the latest system software upgrade file to the DR Series system that is running the browser session started by the DR Series administrator.
6. Using the DR Series system GUI, select **Support**, and click the **Software Upgrade** link (or select **Support → Software Upgrade**).

   The **Software Upgrade** page is displayed.
7. Type the path of the software upgrade file in the **Select the upgrade file from local disk** (or click **Browse...**, and navigate to the location where you downloaded the system software upgrade file).
8. Select the software upgrade file, and click **Open**.
9. Click **Start Upgrade**.

   When you initiate a DR Series system software upgrade, the navigation panel displays only the **Support** page and the **Software Upgrade** option.

   The administrator that initiated the software upgrade (known as the initiator administrator) sees a System Information pane that displays an alert and upgrade status, and the Current Version and Upgrade History versions of the DR Series system software listed in the Software Info pane.

   All other administrators that may be logged into DR Series system (excluding the initiator administrator), only.

There are only three possible outcomes during a DR Series system software upgrade operation:

- Upgrade has completed successfully—no reboot is required.
- Upgrade has completed successfully—but a reboot is required (click **Reboot** in the **Software Upgrade** page).
- Upgrade has failed.

NOTE: If the DR Series system software upgrade operation fails, you can reboot the system and attempt another software upgrade operation using the DR Series system GUI. If this is unsuccessful, you can use the DR Series system CLI **system --show** command to view the current System State status. DR Series system software upgrades can also be performed using the DR Series system CLI. For details, see the *Dell DR Series System Command Line Reference Guide* at **dell.com/support/manuals/**. If both the DR Series system GUI and CLI attempts are unsuccessful, contact Dell Support for assistance.

SSL Page and Options

On the SSL page you can install a new SLL certificate. For additional security, the SSL Certificate feature for the DR Series system enables you to replace the self-signed, factory-installed Dell certificate with another certificate, for example, with one that is signed by a third-party CA. Once you have obtained your signed certificate, you can install it on the SSL page. Only one certificate can be installed on a DR Series system at any given point in time.

Installing an SSL Certificate

To install an SSL certificate, complete the following steps:

1. Select **Support** → **SSL Certificate** in the navigation panel.
   The **SSL Certificate** page is displayed.
2. Click **Browse** to locate and select the SSL certificate on your system that you want to install.

   NOTE: Only .pem formatted SSL certificates are supported.
3. On the SSL Certificate page, click **Install Certificate**.
   The Install SSL Certificate dialog box is displayed.
4. In the Install SSL Certificate dialog box, click **Continue**.
   Unless corrupted or expired, certificates files of .pem format type with less than 2048-bit encryption should successfully verify.
5. In the certificate Validation dialog box, click **Continue**.
   In the event you see the Certificate Verification Failed dialog box, clicking on “Continue” here will generate a connection reset in the browser. You will still be allowed to continue with certificate installation. Upon successful installation of a certificate, an HTTP server restart is performed, and the browser will move to a connection reset state.

   NOTE: If your browser cannot connect to a DR Series system after a certificate installation, you may need to reset the certificate from the command line interface (CLI) using “maintenance --configuration --reset_web_certificate”. Refer to the *Dell DR Series Command Line Reference Guide* for more information.
6. Click either the page reload icon or the back-arrow on the browser to restore the page.

Resetting the SSL Certificate

You can reset the certificate back to the factory-installed Dell, self-signed certificate. The “Reset SSL Certificate” link in the upper right corner of the SSL Certificate page will be enabled after a successful certificate installation.

To reset an SSL certificate, complete the following steps:

1. Select **Support** → **SSL Certificate** in the navigation panel.

   The **SSL Certificate** page is displayed.
2. In the upper right corner of the page, click **Reset SSL Certificate**.

   NOTE: You can also use the command line interface (CLI) command, "maintenance -- configuration -- reset_web_certificate". Refer to the *Dell DR Series Command Line Reference Guide* for more information.

Generating a CSR

You can generate a certificate signing request (CSR) from the SSL Certificate page. A certificate authority (CA) can use the CSR to create an SSL certificate for you. This CSR will contain information to be included in the certificate, such as organization name, common name (domain name), locality, and country. It also contains the public key that will be included in the certificate.

To generate a CSR, complete the following steps:

1. Select **Support** → **SSL Certificate** in the navigation panel.

   The **SSL Certificate** page is displayed.
2. Click **Generate CSR** in the upper right corner of the page.
3. In the Generate CSR and Private Key dialog box, enter the following required information in the form:

   - **Common Name** - The domain to be secured by the certificate.
   - **Organization Name** - The organization's legal business name.
   - **Organization Unit** - A department in the organization.
   - **Locality** - The business location.
   - **State Name** - The state/province of the business location
   - **Country Code** - The country of the business location.
   - **Email** - A contact email address.
   - **Encryption** - Select one of the following options: 2048-bit encryption or 4096 encryption. The default is 2048.
4. Click **Generate**.

   The Certificate request output will appear in the window. You can copy and paste the CSR to the CA's web site CSR page, or you can save the CSR to a file

   NOTE:

   Every time a CSR is generated, a new private key is generated and stored on the DR Series system. When the signed certificate is returned from the CA, and you attempt to install the signed certificate, a verification that the installed signed certificate matches the private key is performed. If the installed certificate does not match the private key, the certificate installation will fail due to private key match failure. You should be careful not to run a subsequent CSR generation while your initial CSR is being signed by a CA, as the returned certificate will no longer match the private key.
5. Click **Save to File** to save it to a file.

Restore Manager (RM)

The Dell **Restore Manager** (RM) utility can be used to restore the DR Series system software. RM can be used when a non-recoverable hardware or software failure prevents the DR Series system from functioning correctly.

RM can also be used to reset the system back to its initial factory settings when moving it from a test environment to a production environment. RM supports the following two modes:

- **Recover Appliance**—in Recover Appliance mode, RM reinstalls the operating system and attempts to recover the prior system configuration and the data residing in the containers.

  NOTE: To use the Recover Appliance mode, you must use an RM build that is compatible with the DR Series system software version that was running before the OS reset was attempted.

- **Factory Reset**—in a Factory Reset mode, RM reinstalls the operating system and resets the system configuration back to the original factory state. It is important to note that when doing a factory reset, all of the containers and the data in the containers gets deleted.

CAUTION: Using the Factory Reset mode deletes all of the DR Series system data. The Factory Reset mode must only be used when the container data is no longer needed.

Downloading the Restore Manager

The Dell **Restore Manager** (RM) utility runs from a USB boot key that contains the RM image, which must first be downloaded from the Dell Support site.

1. Using a supported web browser, navigate to **support.dell.com**.
2. Enter your DR Series system Service Tag to be directed to the DR Series system download page (or choose a product category, click **Get Drivers** and then **View All Drivers**).
3. In the **Category** drop-down list on the Drivers & Downloads page, select **IDM**.
4. If required, expand the **IDM** category to list the available IDM download files.
5. Locate, select, and download the **Restore Manager (RM) for DR4000 Series** file (listed in the following RM filename format, "DR-RM-x.x.x.xxxxx.img").

Creating the Restore Manager USB Key

To create a Restore Manager (RM) USB key, you must first download the RM image (.img) file from the Dell Support site, and then transfer this on to a USB key. The USB key must be a minimum of 4 GB (Gigabytes) in size or larger. Windows USB image tools can be used to transfer the RM image when they meet the following conditions:

- Support using the .img file format
- Support using a direct block-to-block device copy to ensure that the USB key is bootable

To transfer the RM image to the USB key on a Linux or Unix system, perform the following:

1. Copy the downloaded RM image file to a Linux or Unix system.
2. Insert the USB key into an available USB port on the Linux or Unix system.

   Make note of the device name that is reported by the operating system (for example, **/dev/sdc4**).
3. Do not locally mount the USB device to a file system at this time.
4. Copy the RM image to the USB key using the **dd** command:

   ```
   dd if=<path to .img file> of=<usb device> bs=4096k
   ```

   For example:

   ```
   dd if=/root/DR-RM-1.05.03.313-2.1.0851.2.img of=/dev/sdc4 bs=4096
   ```

Running the Restore Manager (RM)

To run the Dell **Restore Manager** (RM) utility, boot the DR Series system using the RM USB key created in Creating the RM USB key).

1. Insert the RM USB key into an available USB port on the system.

   You can also use the virtual media option of iDRAC to remotely load the RM USB key. For more information, see *Configuring and Using Virtual Media in the Integrated Dell Remote Access Controller 6 (iDRAC6) User Guide* at **support.dell.com/support/edocs/software/smdrac3/**.
2. Boot the DR Series system using the RM USB key.
3. During the time when the Power-On Self-Test (POST) screen displays, press **F11** to load the Boot Manager.
4. Within the Boot Manager, navigate to the system hard drive (C:), select the USB key as the boot device, and press **<Enter>**.
5. After a few minutes, **Restore Manager** loads and displays its main screen.
6. Select the desired Restore mode (either **Recover Appliance** or **Factory Reset**).
7. Enter the confirmation string, and press **<Enter>** to proceed.

   CAUTION: The Factory Reset mode deletes all DR Series data. The Factory Reset mode should only be used when the container data is no longer needed.

   NOTE: After **Restore Manager** completes, only the administrator account will remain enabled. To re-enable the root or service accounts, see the DR Series system CLI **user --enable --user** command in the *Dell DR Series System Command Line Reference Guide*.

   NOTE: If you had previously joined the DR Series system to any Active Directory Services (ADS) domain before running **Restore Manager**, after it completes you will need to manually rejoin the desired ADS domain. For information about joining an ADS domain, see Configuring Active Directory Settings.

Resetting the Boot LUN Setting in PERC H700 BIOS After Running RM

In the event that both of the 2.5-inch 300 GB 10K RPM 6 GB/s SAS internal drives (OS) in RAID1 are replaced, you must run the Dell **Restore Manager** (RM) utility to recover the DR Series system OS drives.

Following the RM recovery process, the boot logical unit number (LUN) has to be reset to VD0 RAID1. The DR Series system unsuccessfully attempts to boot from RAID6 instead of RAID1.

To resolve this issue, reset the Dell PERC H700 BIOS to revise the proper boot order setting to configure the proper boot LUN to be RAID1. To reset the proper LUN boot order, complete the following steps:

1. Start **Restore Manager**.
2. Select **Option 1** → **Recover My Appliance**.

   The **OS Virtual Disk is created: Warning Code 2002** dialog is displayed.
3. Click **Proceed**.

   The **Operating System installation was successful** dialog is displayed.
4. Click **Reboot**, and during reboot, press **Ctrl+R** to enter the PERC BIOS.

   The **PERC BIOS Configuration Utility** page is displayed.
5. Select **Controller 0: PERC H700** in the list.
6. Press **Ctrl+N** twice to select the **Ctrl Mgmt** (Controller Management) tab.
7. Select **Ctrl Mgmt**, click **Select bootable VD**, and select **VD 0** as the VD0 RAID1.
8. Click **Apply**, and reboot the DR Series system.

   The **RM Recover My Appliance** mode process will then complete.

Hardware Removal or Replacement

To properly remove or replace any DR Series system hardware, you must observe and use the best practice shut down and start up procedures. For a comprehensive set of removal and replacement procedures with step-by-step instructions, see the *Dell DR Series System Owner's Manual*.

For more information about the best practices, see DR Series System: Proper Shut Down and Start Up and Shutting Down the DR Series System.

DR Series System: Proper Shut Down and Start Up

Before you attempt to remove or replace any hardware component in the DR Series system, ensure that you observe the following best practices for properly shutting down and starting up the system.

NOTE: To shutdown the DR Series system using a UPS after a power loss, refer to the following article for information on how to do this using the shutdown command in the IPMI interface: http://www.dell.com/downloads/global/power/ps4q04-20040204-murphy.pdf.

1. Power off the DR Series system by selecting **Shutdown** in the **System Configuration** page.

   For more information, see Shutting Down the DR Series System. Another method you can use to shut down the system is the DR Series system CLI command, **system --shutdown**.
2. Allow the DR Series system to fully complete its power-down process.

   When the power-down process has completed, the Power Supply status indicator is unlit.
3. Disconnect the DR Series system power cables from the electrical power outlet.
4. Wait an additional period of time (up to 10 minutes), and/or verify that all of the green and amber NVRAM LEDs on the rear panel of the system chassis are unlit.

   NOTE: If you do not allow the NVRAM super capacitor sufficient time to discharge, the NVRAM status will report **DATA LOSS** when the DR Series system is subsequently powered up.
5. Unlatch the latch release lock and slide the DR Series system cover back and away to gain entry to the appliance internal components.

   To gain entry to the interior of the DR Series system, remove the cover. For more information, see the procedures in the *Dell DR Series System Owner's Manual*.
6. Remove and replace the system hardware components as needed.
7. Replace the cover, reconnect the system power cables to the electrical power outlet.
8. Power on the DR Series system by pressing the power-on indicator/power button.

DR Series System NVRAM

NVRAM is a field replaceable unit (FRU) in the DR Series system. The super capacitor that powers the NVRAM double-data rate (DDR) memory must be able to move its contents to the solid-state drive (SSD) during a power loss.

This data transfer requires maintaining the power to run the system for 3 minutes of operation (normally, it only takes approximately one minute). If a problem occurs during the data backup to the SSD, the subsequent system reboot detects this. NVRAM can experience backup failure when the following occurs:

- The NVRAM failed to backup the data during the power shutdown
- The super capacitor did not maintain sufficient power to backup the DDR contents into the SSD.
- The NVRAM/SSD encountered an end-of-line (EOL) or another error.

If any of these conditions occur, the NVRAM requires either a failure recovery or a replacement.

NOTE: Dell recommends the following supported method for flushing DR Series system data from the NVRAM to the RAID6 before replacing the NVRAM by using either of the following DR Series system CLI commands: **system --shutdown** or **system --reboot**.

NOTE: If you need to remove or replace the NVRAM in the DR Series system, see Shutting Down the DR Series System and NVRAM Field Replacement.

NVRAM Backup Failure Recovery

After you have physically replaced the NVRAM card in a PCIe x4 (or x8) slot in the DR Series system chassis, you can recover from an NVRAM backup failure by completing the following tasks:

CAUTION: You must wait a minimum of 20 minutes after powering on the DR Series system before using the DR Series system CLI maintenance --hardware --reinit_nvram command. This 20–minute post power-on waiting period allows the NVRAM card, the super capacitor calibration, and all solid state drive (SSD) processes to fully complete, which are necessary for the proper operation of the DR Series system.

During Maintenance mode, the DR Series system determines, detects, and repairs the data loss. During the system reboot process, it ensures that no valuable data remains on the NVRAM.

1. Enter the following DR Series system CLI command: **maintenance --hardware --reinit_nvram**.

   This formats the SSD and clears all of the backup and restore logs, by reinitializing the NVRAM.
2. Verify that the DR Series system enters its Maintenance mode.

   For more information about replacing the NVRAM, see NVRAM Field Replacement and DR Series System: Proper Shut Down and Start Up.

NVRAM Field Replacement

Whenever the DR Series system NVRAM is replaced in the field, you must observe this best practice procedure:

CAUTION: You must wait a minimum of 20 minutes after powering on the DR Series system before using the DR Series system CLI command: maintenance --hardware --reinit_nvram. This post power-on waiting period allows the NVRAM card, the super capacitor calibration, and the SSD processes to fully complete, which are necessary for the proper operation of the DR Series system.

NOTE: For more information, see DR Series System: Proper Shut Down and Start Up.

1. Verify that the DR Series system software detects the NVRAM as being new to the system.
2. Enter the following DR Series system CLI command: **maintenance --hardware --reinit_nvram**.

   This command initializes the NVRAM, creates new partitions, and updates information used internally by the DR Series system software.
3. Verify that the DR Series system enters its Maintenance mode.

   If properly initialized, the DR Series system will automatically enter Maintenance mode. The filesystem checker examines every blockmap and datastore to determine how much data was lost due to the failed NVRAM.

9

Configuring and Using Rapid NFS and Rapid CIFS

Rapid NFS and Rapid CIFS enable write operation acceleration on clients that use NFS and CIFS file system protocols. Similar to OST and RDS, these accelerators allow for better coordination and integration between DR Series system backup, restore, and optimized duplication operations with Data Management Applications (DMAs) such as CommVault, EMC Networker, and Tivoli Storage Manager. For the current list of supported DMAs, see the *Dell DR Series System Interoperability Guide*.

Rapid NFS is a new client file system type that ensures that only unique data is written to the DR Series system. It uses user space components and file system in user space (FUSE) to accomplish this. Metadata operations such as file creates and permission changes go through the standard NFS protocol, whereas write operations go through Rapid NFS.

Rapid CIFS is a Windows-certified filter driver that also ensures that only unique data is written to the DR Series system. All chunking and hash computations are done at the client level.

NOTE: The supported DMAs listed in the *Dell DR Series System Interoperability Guide* are the DMAs that have been **tested and qualified** with Rapid NFS and Rapid CIFS. You can use Rapid NFS and Rapid CIFS with other DMAs (such as Symantec products), but Dell has not tested and qualified Rapid NFS or Rapid CIFS on those products.

Rapid NFS and Rapid CIFS Benefits

When Rapid NFS and Rapid CIFS are used with the DR Series system, they offer the following benefits:

- Reduce network utilization and DMA backup time
  - Chunk data and perform hash computation on the client; transfer chunked hash files on the back-end
  - Reduce the amount of data that must be written across the wire
- Improve performance
- Support DMAs such as CommVault, EMC Networker, and Tivoli Storage Manager. For the current list of supported DMAs, see the *Dell DR Series System Interoperability Guide*.
- Compatible with existing NFS and CIFS clients — just need to install a plug-in (driver) on the client
  - Can use Rapid NFS and Rapid CIFS to accelerate I/O operations on any client — including a client that uses home-grown backup scripts
  - Can service multiple and concurrent media server backups

Best Practices: Rapid NFS

This topic introduces some recommended best practices for using Rapid NFS operations with the DR Series system.

Containers must be of type NFS/CIFS

RDA containers cannot use Rapid NFS. If you have existing NFS/CIFS containers, you do not need to create new containers to use Rapid NFS; you can install the plug-in (driver) to existing clients.

The Rapid NFS plug-in (driver) must be installed on client systems

After the plug-in is installed, write operations will go through Rapid NFS while metadata operations such as file creates and permission changes will go through the standard NFS protocol. Rapid NFS can be disabled by uninstalling the plug-in.

Markers must be set on the client, not in the DR Series GUI

If you are using a DMA that supports a marker, should explicitly set it. Your containers should have the marker type of **None** until you set the marker using the Mount command on the client (after installing the Rapid NFS plug-in). For existing containers, re-set the marker using the procedure that follows.

For example, if you wanted to set the CommVault marker (cv):

```
mount -t rdnfs 10.222.322.190:/containers/backup /mnt/backup -o
marker=cv
```

Mount command usage:

```
rdnfs [nfs mount point] [roach mount point] -o marker=[marker]
```

where:

```
nfs mount point = Already mounted nfs mountpoint
roach mount point = A new mount point
marker = appassure, arcserve, auto, cv, dump, hdm, hpdp, nw, or
tsm
```

Your DR Series system must meet the minimum configuration

Rapid NFS is available on a DR Series system and a client with a minimum of 4 CPU cores running at a minimum of 4 GHz cumulative processing power and 2 GB memory. Kernels must be 2.6.14 or later. For a list of supported operating systems, see the *Dell DR Series System Interoperability Guide*.

If you update your operating system, you must update your Rapid NFS plug-in as well. Updates are available on the Support site as well as within the GUI on the **Clients** page.

Rapid NFS is stateful

If the DR Series system goes down, the connection will terminate. DMAs will restart from the last checkpoint.

Rapid NFS and passthrough mode

If Rapid NFS mode fails for any reason, the DR Series system falls back to regular NFS mode automatically. For details, see Monitoring Performance.

Rapid NFS performance considerations

When using Rapid NFS on your client, Dell recommends that you do not run other protocols to the DR in parallel, as this will adversely affect your overall performance.

Rapid NFS acceleration constraints

Rapid NFS does not support:

- Direct I/O memory
- Mapped files
- File path size greater than 4096 characters
- File write locks across clients

NOTE: If the client and server do not have the same times, the times seen will not match typical NFS behavior due to the nature of file system in user space (FUSE).

Best Practices: Rapid CIFS

This topic introduces some recommended best practices for using Rapid CIFS operations with the DR Series system.

Containers must be of type NFS/ CIFS

RDA containers cannot use Rapid CIFS. If you have existing NFS/CIFS containers, you do not need to create new containers to use Rapid CIFS; you can install the plug-in (driver) to existing clients.

The Rapid CIFS plug-in (driver) must be installed on client systems

After the plug-in is installed, write operations will go through Rapid CIFS while metadata operations such as file creates and permission changes will go through the standard CIFS protocol. Rapid CIFS can be disabled by uninstalling the plug-in.

Your DR Series system must meet the minimum configuration

Rapid CIFS is available with a DR Series system and a client with a minimum of 4 CPU cores running at a minimum of 4 GHz cumulative processing power and 2 GB memory. For a list of supported operating systems, see the *Dell DR Series System Interoperability Guide*.

If you update your operating system, you must update your Rapid CIFS plug-in as well. Updates are available on the Support site as well as within the GUI on the **Clients** page.

Rapid CIFS is stateful

If the DR Series system goes down, the connection will terminate. DMAs will restart from the last checkpoint.

Rapid CIFS and passthrough mode

If Rapid CIFS mode fails for any reason, the DR Series system falls back to regular CIFS mode automatically. For details, see Monitoring Performance.

Rapid CIFS acceleration constraints

Rapid CIFS does not support:

- NAS functionality
  - Optlocks (but supported if a single client is writing)
  - Byte-range locks
- Optimization of very small files (less than 10 MB). File size can be adjusted using configuration settings.
- FILE_NO_IMMEDIATE_BUFFERING and FILEWRITE_THROUGH operations (sent via CIFS only).
- File path size greater than 4096 characters

Setting Client-Side Optimization

Client-side optimization is a process that can contribute to saving time performing backup operations and reducing the data transfer overhead on the network.

You can turn On or turn Off client-side optimization (also known as client-side deduplication) using the DR Series system CLI commands, **rda --update_client --name --mode**. For more information about DR Series system CLI commands, see the *Dell DR Series System Command Line Reference Guide*, available at **support.dell.com/manuals**.

Installing the Rapid NFS Plug-In

The Dell Rapid NFS plug-in must be installed on to the media server type you choose (for supported operating systems and DMAs, see the *Dell DR Series System Interoperability Guide*). The plug-in software enables integration between DR

Series system data storage operations and the supported data management applications (DMAs). Before you install, make sure you adhere to the Best Practices covered in another topic in this chapter.
The plug-in must be installed on the designated Linux-based media server in the following directory, **/usr/openv/lib/**. The plug-in is installed using a self-extracting installer that installs the Rapid NFS plug-in and all of its related components. The installer supports the following modes, with the default being Help (-h):

- Help (-h)
- Install (-install)
- Upgrade (-upgrade)
- Uninstall (-uninstall)
- Force (-force)

```
$> ./DellRapidNFS-xxxxx-xxxxx-x86_64.bin -help
Dell plug-in installer/uninstaller
usage: DellRapidNFS-xxxxx-xxxxx-x86_64.bin [ -h ] [ -install ] [ -uninstall ]
-h                    : Displays help
-install        : Installs the plug-in
-upgrade        : Upgrades the plug-in
-uninstall    : Uninstalls the plug-in
-force            : Forces the installation of the plug-in
```

You can download the plug-in installer via the Dell website:

- Navigate to **support.dell.com/** and locate the Drivers and Downloads location.
- Locate the Dell Rapid NFS plug-in and download it to your system.

After it is downloaded, follow the steps that follow to run the Plug-In Installer to install the plug-in on your designated Linux-based media server.

NOTE: The plug-in needs to be installed on client systems to support client-side deduplication.

1. Download `DellRapidNFS-xxxxx-xxxxx-x86_64.bin.gz` from the Dell website, as detailed previously.
2. Unzip the package.
   ```
   unzip DellRapidNFS-xxxxx-xxxxx-x86_64.bin.gz
   ```
3. Assign execute bit to change the permission of the binary package:
   ```
   chmod +x DellRapidNFS-xxxxx-xxxxx-x86_64.bin
   ```
4. Install the Rapid NFS package. Before installing, remove the stale NFS entry.
   ```
   DellRapidNFS-xxxxx-xxxxx-x86_64.bin -install
   ```
5. Load the file system in user space (FUSE) module, if not already loaded:
   ```
   modprobe fuse
   ```
6. Create a directory on the client. For example:
   ```
   mkdir /mnt/backup
   ```
7. Mount Rapid NFS as a file system type using the mount command. For example:
   ```
   mount -t rdnfs 10.222.322.190:/containers/backup /mnt/backup
   ```
   If you are using a DMA that supports a marker, set the marker by using -o in the mount command. For example, if you wanted to set the CommVault marker (cv):
   ```
   mount -t rdnfs 10.222.322.190:/containers/backup /mnt/backup -o marker=cv
   ```
   NOTE: If you want to do a mount on AIX, you must set the nfs_use_reserved_ports and portcheck parameters first. The parameters cannot be set to 0. For example: `root@aixhost1 / # nfso -po portcheck=1 root@aixhost1 / # nfso -po nfs_use_reserved_ports=1`

To ensure that the plug-in is running successfully, check the log file at: `tail -f /var/log/oca/rdnfs.log`.

Installing the Rapid CIFS Plug-In

The Dell Rapid CIFS plug-in must be installed on to the media server type you choose (for supported operating systems and DMAs, see the *Dell DR Series System Interoperability Guide*). The plug-in software enables integration between DR Series system data storage operations and the supported data management applications (DMAs). Before you install, make sure you adhere to the Best Practices covered in another topic in this chapter.

You can download the plug-in installer using the Dell website:

- Navigate to **support.dell.com/** and locate the Drivers and Downloads location.
- Locate the Dell Rapid CIFS plug-in and download it to your system.

After it is downloaded, follow the steps below to run the plug-in installer to install the plug-in on your designated media server.

NOTE: The plug-in needs to be installed on client systems to support client-side deduplication.

1. On the media server, map a network share to your CIFS-enabled container.
2. Download the plug-in installer from the Dell website, as detailed previously.
3. Open a command prompt with the “Run as Administrator” option selected. To do this using the Windows Start menu, click **Start** → **All Programs** → **Accessories**. Right-click **Command Prompt** and select **Run as Administrator**.

   This gives all the required privileges to install/copy the driver files to the Windows drivers folder.
4. Run `DellRapidCIFS-xxxxx.msi.`
5. Follow the installation prompts. All files are installed to Program Files\Dell\Rapid CIFS.

To ensure that the plug-in is running successfully, check the Windows Event log file.

Determining If Your System Is Using Rapid NFS or Rapid CIFS

Use this procedure to identify whether Rapid NFS or Rapid CIFS is installed and enabled on your DR Series system.
To determine if your system is using the Rapid NFS or Rapid CIFS accelerator:

1. In the GUI, go to the **Dashboard**, and then click **Container Statistics**.
2. In the **Container Name** drop-down list, select a NFS or CIFS container that is associated with your client.
3. In the **Connection Configuration** pane of the statistics page, locate the **NFS Write Accelerator** or **CIFS Write Accelerator** field, depending on the protocol selected.
4. Next to the **Write Accelerator** field is a value. **Active** indicates that the accelerator plug-in is installed and enabled. **Inactive** indicates that the plug-in is not installed or not working correctly.

Viewing the Rapid NFS and Rapid CIFS Logs

This topic contains information about locating and reviewing Rapid NFS and Rapid CIFS event logs in order to troubleshoot.

Viewing Rapid NFS Logs

The Rapid NFS log is located at /var/log/rdnfs.log. Statistics, throughput, and the plug-in version can be seen on the client by running the ru utility on the client, as follows:

```
ru --mpt=[rdnfs mount point] | --pid=[process ID of rdnfs] --show=[name|version|
parameters|stats|performance]
```

The configuration file is located /etc/oca.0/rdnfs.cfg.

Viewing Rapid CIFS Logs

If you want a high-level view of events and errors for the Rapid CIFS accelerator, open the Windows Event Log.

If you want to view more detailed event messages from Rapid CIFS, you can access a secondary log using the following Rapid CIFS utility command. The utility is located in Program Files\Dell\Rapid CIFS.

```
rdcifsctl.exe -collect
```

Monitoring Performance

This procedure describes how to monitor performance by viewing Rapid NFS and Rapid CIFS usage graphs.
Before you view usage graphs, make sure that the appropriate accelerator is active by viewing the **Connection Configuration** pane on the **Container Statistics** page.
To monitor Rapid NFS and Rapid CIFS performance:

1. Click **Dashboard**, and then click **Usage**.
2. Select a time range (if needed) and click **Apply**.
3. Click the **Protocols** tab.

   Under **NFS Usage** and **CIFS Usage**, there is an **XWrite** checkbox. This checkbox represents the accelerator activity.
4. In the desired usage graph pane, select the **XWrite** checkbox to view the accelerator performance over time.

If you have Rapid NFS enabled, you can use the command line to view statistics, throughput, and the plug-in version by running the ru utility on the client, as follows:

```
ru --mpt=[rdnfs mount point] | --pid=[process ID of rdnfs] --show=[name|version|
parameters|stats|performance]
```

If you have Rapid CIFS enabled, you can use the command line to view aggregate statistics (even while a backup job is running) using the following command:

```
\Program Files\Dell\Rapid CIFS\rdcifsctl.exe stats -s
```

Uninstalling the Rapid NFS Plug-In

Use the following procedure to remove the Dell Rapid NFS plug-in from a Linux-based media server. After you uninstall the plug-in, Rapid NFS will be disabled and “inactive” will be shown next to **NFS Write Accelerator** on the **NFS Connection Configuration** pane on the **Container Statistics** page.

NOTE: Dell recommends that you retain the Dell Rapid NFS plug-in installer on the media server in case you need to use it to reinstall the plug-in. It is usually located in /opt/dell/DR-series/RDNFS/scripts.

To uninstall the Rapid NFS plug-in on Linux:

1. Stop the Data Management Application (DMA) backup service before using the **-uninstall** option.

   The Rapid NFS plug-in installer returns an error if the DMA service is running when attempting to uninstall the plug-in.
2. Run the Rapid NFS plug-in installer (usually located in /opt/dell/DR-series/RDNFS/scripts) with the **-uninstall** option, which uninstalls the plug-in, using the following command:

   ```
   $> ./DellRapidNFS-xxxxx-x86_64.bin -uninstall
   ```

   NOTE: You must stop the DMA service before uninstalling the Rapid NFS plug-in (you are also required to use the Dell Rapid NFS plug-in installer to uninstall the plug-in).
3. Check that the plug-in is uninstalled by viewing the usage graph in the GUI; it should not indicate any **XWrite** activity.

Uninstalling the Rapid CIFS Plug-In

Use the following standard Microsoft Windows uninstall process to remove the Dell Rapid CIFS plug-in from a Windows-based media server. After you uninstall the plug-in, Rapid CIFS will be disabled and “inactive” will be shown next to **CIFS Write Accelerator** on the **CIFS Connection Configuration** pane on the **Container Statistics**page.
Alternatively, if you want to disable (but not uninstall) the plug-in, you can run the following Rapid CIFS utility command. The utility is located in Program Files\Dell\Rapid CIFS.

```
rdcifsctl.exe driver -d
```

NOTE: Dell recommends that you retain the Dell Rapid CIFS plug-in installer on the media server in case you need to use it to reinstall the plug-in.

To uninstall the Rapid CIFS plug-in on Windows:

1. Click **Start**, and click **Control Panel**.

   The **Control Panel** page is displayed.
2. Under **Programs and Features**, click **Uninstall a program**.

   The **Uninstall or change a program** page is displayed.
3. Locate the Dell Rapid CIFS plug-in in the listed of installed programs, right click and select **Uninstall**.

   The **Programs and Features** confirmation dialog is displayed.
4. Click **Yes** to uninstall the Dell Rapid CIFS plug-in.

10

Configuring and Using Rapid Data Access with Dell NetVault Backup and with Dell vRanger

Overview

Rapid Data Access (RDA) with Dell NetVault Backup and with Dell vRanger provides the logical disk interface that can be used with network storage devices. The Dell DR Series system requires a DR Rapid plug-in to integrate its data storage operations with NetVault Backup and vRanger. The plug-in is installed by default on the NetVault Backup and vRanger servers and the Dell DR Series system when the latest software updates are installed. Using the DR Rapid plug-in, the DMAs can take full advantage of key DR Series system features like replication and data deduplication.

When DR Rapid is used with the DR Series system, it offers the following benefits:

- RDA with NetVault Backup and RDA with vRanger protocols provide faster and improved data transfers:
  - Focus is on backups with minimal overhead
  - Accommodates larger data transfer sizes
  - Provides throughput that is better than CIFS or NFS
- DR Rapid and data management application (DMA) integration:
  - DMA-to-media server software communication
  - DR Series system storage capabilities can be used without extensive changes to DMAs
  - Backup and replication operations are simplified by using built-in DMA policies
- DR Series system and DR Rapid ports and write operations:
  - Control channel uses TCP port 10011
  - Data channel uses TCP port 11000
  - Optimized write operations enable client-side deduplication
- Replication operations between DR Series systems:
  - No configuration is required on the source or target DR Series system
  - Replication is file-based, not container-based
  - Replication is triggered by DMA optimized duplication operation
  - DR Series system transfers the data file (not the media server)
  - After duplication completes, DR Series system notifies DMA to update its catalog (acknowledging the second backup). This makes the DMA aware of the replication location. Restores from either the source or replication target can be used directly from the DMA.
  - Supports different retention policies between source and replica
  - Replication is set up in the DMA itself, not the DR Series system

Guidelines for using RDA with NetVault Backup and with vRanger

For best results, observe the following guidelines for optimal performance with your supported RDA with NetVault Backup and RDA with vRanger operations with the DR Series system:

- Backup, restore, and optimized duplication operations are performed using the RDA with NetVault Backup or RDA with vRanger plug-in

  NOTE: The plug-in is installed on client systems to support client-side deduplication.

- Backup:

  – Passthrough writes: Passthrough writes are when data is sent from a media server to the DR Series system without applying any optimization to the data. By contrast, dedupe writes are when data is sent from a media server to the DR Series system after optimization is applied to the data.

  – Dedupe writes

  NOTE: Dedupe mode requires four (4) GB of memory and passthrough requires 200 MB free memory.

- Restore
- Replication

Best Practices: RDA with NetVault Backup and vRanger and the DR Series System

This topic introduces some recommended best practices for using DR Rapid operations with the DR Series system.

RDS and non-RDS type containers can exist on the same DR Series system

The DR Series system supports having both RDS and non-RDS containers on the same appliance. However, this can cause incorrect capacity reporting as both container types share the same underlying storage.

RDS replication and non-RDS replication on the same DR Series system

Non-RDS replication must be configured, and it is replicated on a per-container basis. However, this type of replication will not replicate RDS containers. RDS replication is file-based and is triggered by the DMA.

Do not change the container connection type from NFS/CIFS to RDS

A non-RDS container must be deleted before this container can then be created as an RDS container using the same name.

Setting Client-Side Optimization

Client-side optimization is a process that can contribute to saving time performing backup operations and reducing the data transfer overhead on the network.

You can turn On or turn Off client-side optimization (also known as client-side deduplication) using the DR Series system CLI commands, **rda --update_client --name --mode**. For more information about DR Series system CLI commands, see the *Dell DR Series System Command Line Reference Guide*, available at **support.dell.com/manuals**.

Adding RDS Devices in NetVault Backup

To add RDS devices in NetVault Backup:

1. Start the NetVault Web user interface (UI), and log on to the NetVault Backup Server.
2. Start the configuration wizard by doing one of the following:
   - In the Navigation pane, click **Guided Configuration**, and then, on the NetVault Configuration Wizard page, click **Add Storage Devices**.
   - Alternatively, in the navigation pane, click **Manage Devices**, and then click **Add Device**.
3. Select the **Dell RDA Device** option, and click **Next**.

   The **Add Dell RDA Device** page is displayed.
4. In **Host**, enter the IP address or the system host name of the DR Series system.
5. In **Username**, enter **backup_user**.

   NOTE: The **Username**, **backup_user** is case-sensitive. You can configure RDS containers only while logged on the DR Series system with username **backup_user**.
6. In **Password**, enter the password used to access the DR Series system.
7. In **LSU**, enter the name of the RDS container.

   NOTE: The RDS container name in LSU is case-sensitive. Ensure that you enter the RDS container name exactly as it is on the DR Series system.
8. In **Block size**, enter the block size for data transfers. The block size is specified in bytes. The default block size is 131,072 bytes.
9. If the device is already added to another NetVault Backup Server with the same name, select the **Force add** check box. This option can be useful if you have performed a disaster recovery to rebuild the NetVault Backup Server.
10. Click **Next** to add the device.

    After the device is successfully added and initialized, a message is displayed.

Removing RDS Devices From NetVault Backup

Refer to the following steps to remove existing RDS devices from NetVault Backup.

NOTE: Removing an RDS device from NetVault Backup does not delete the data stored in the RDS container on the DR Series system.

1. Start the NetVault Web user interface (UI), and in the Navigation pane, click **Manage Devices**.
2. In the list of devices, locate the device, and click the corresponding **Manage Device** icon.
3. Click **Remove**, and then in the confirmation dialog box, click **Remove** again.

   NOTE: Ensure that you remove the RDA device from NetVault Backup before you delete the container from the DR Series system. You must force remove the RDS device from NetVault Backup, if you delete an RDS container from the DR Series system before removing it from the NetVault Backup server.
4. If NetVault Backup fails to remove the device, select the **Force Removal** check box in the confirmation dialog, and click **Remove**.

The selected RDS device is removed from NetVault Backup. The RDS container can now be removed from the DR Series system.

Backing Up Data on the RDS Container Using NetVault Backup

You must back up data on the RDS container (available on the DR Series systems) using NetVault Backup. Before you can back up data using the RDS protocol, you must create an RDS container on the DR Series system and then add that container as an RDA device on NetVault Backup. For more information see, Adding RDS Devices in NVBU.

To back up data on the RDS container:

1. Start the NetVault Web user interface (UI), and in the Navigation pane, click **Create Backup** Job.
2. In Job Name, type a name for the job. Assign a descriptive name that allows you to easily identify the job for monitoring its progress or restoring data. A job name can contain alphanumeric and non-alphanumeric characters, but it cannot contain non-Latin characters. There is no length restriction. However, a maximum of 40 characters is recommended on all platforms.
3. In the **Selections** list, select an existing Backup Selection Set, or click **Create New**, and select the items that you want to back up. The selection tree is plug-in specific. For more information about selecting data for backups, see the relevant NetVault Backup plug-in user's guide.
4. In the **Plugin Options** list, select an existing Backup Options Set, or click **Create New**, and configure the options that you want to use. These options are plug-in specific. For more information about these options, see the relevant NetVault Backup plug-in user's guide.
5. In the **Schedule** list, select an existing Schedule Set, or click **Create New**, and configure the schedule type and schedule method. For more information about these options, see the *Dell NetVault Backup Administrator's Guide*. To run the job as soon as it is submitted, use the "**Immediate**" set.
6. In the **Target Storage** list, select an existing Target Set, or click **Create New**, and configure the target device and media options for the job.

   To use a particular DR Series System, select the **Specify Device** option, and in the list of devices, clear the check marks for the devices that you do not want to use.

   For more information about these options, see the *Dell NetVault Backup Administrator's Guide.*.
7. In the **Advanced Options** list, select an existing Backup Advanced Options Set, or click **Create New**, and configure the options that you want to use.

   For more information about these options, see the *Dell NetVault Backup Administrator's Guide*.
8. To submit the job for scheduling, click **Save & Submit**.

The backup job may take a few minutes to complete depending on the amount of data that is backed up. You can view the progress of the backup job by using the Job Management section of NetVault Backup. For more information about using NetVault Backup, see the *Dell NetVault Backup Administrator's Guide.*

Replicating Data to a RDS Container using NetVault Backup

By using NetVault Backup with the DR Series system, you can run optimized replication jobs. You can replicate data in backup RDS containers on one DR Series system to a target RDS container that is on a different DR Series system. Both the source and target RDS containers must be added to the NetVault Backup server as RDA devices. You can complete optimized replication (or optimized duplication) of backups that you complete using NetVault Backup.

NOTE: You cannot replicate RDS containers using the DR Series system native replication feature.

NOTE: The source or backup container and the target container must use the RDS protocol.

To replicate the data available on the backup RDS container to a target RDS container:

1. In the **NetVault Backup Console**, click **Backup**.

   The **NetVault Backup** window is displayed.
2. From the **Server Location** list, select the relevant NetVault Backup server.

3. In **Job Title**, enter a relevant job title.
4. In the **Selections** tab, select **Data Copy** and then **Backups** or **Backup Sets**, and navigate to the backup job that you want to replicate.
5. Select the **Backup Options** tab, under **Data Copy Options** select the relevant options.

   NOTE: Under **Copy Type**, by default, options are set for **Copy and Optimized** replication for the DR Series systems.
6. Select the **Schedule** tab, under **Schedule Options** select one of the following:
   - **Immediate** — To start the backup operation as soon as you save the current backup job.
   - **Once** — To run the backup only once at a scheduled time and date.
   - **Repeating** — To run the backup at a scheduled time and date on a daily, weekly, or monthly basis.
   - **Triggered** — To run the backup if the system encounters a pre-specified **Trigger name**.
7. Under **Job Options** select the relevant options.
8. Select the **Source** tab, under **Device Options** select, **Specify Device**.

   The RDS devices added to NetVault Backup are displayed.
9. Select the relevant source RDS device from the list of displayed devices.

   You can select more than one device.
10. Select the **Target** tab, under **Device Options** select, **Specify Device**.

    The RDS devices added to NetVault Backup are displayed.
11. Select the relevant target RDS device from the list of displayed devices.

    You can select more than one device.
12. Under **Media Options** and **General Options**, select the relevant option.
13. Select the **Advanced Options** tab and select the relevant options.
14. To run the optimized replication job, click the **Submit** icon.

NOTE: For more information on Dell NetVault Backup, see the *Dell NetVault Backup Administrator's Guide*.

Restoring Data From a DR Series System using NetVault Backup

The following steps describe how to use NetVault Backup to restore data from a RDS container on a DR Series system.

To restore data from a DR Series system using NetVault Backup:

1. Start the NetVault Web user interface (UI), and in the Navigation pane, click **Create Restore Job**.
2. In the saveset table, select the saveset that you want to use, and click **Next**.
3. On the **Create Selection Set** page, select the items that you want to restore.

   The selection tree is plug-in specific. For more information about selecting data for restores, see the relevant NetVault Backup plug-in user's guide.
4. Click **Edit Plugin Options**, and configure the options that you want to use and then click **Next**.

   These options are plug-in specific. For more information about these options, see the relevant NetVault Backup plug-in user's guide.
5. On the **Create Restore Job** page, specify a name for the job. Assign a descriptive name that allows you to easily identify the job for monitoring its progress.

   A job name can contain alphanumeric and non-alphanumeric characters, but it cannot contain non-Latin characters. There is no length restriction. However, a maximum of 40 characters is recommended on all platforms.
6. In the **Target Client** list, select the restore target as follows:
   - To restore data to the same client (from which data was backed up), use the default setting.

- To restore data to an alternate client, select the target client in the list.
- Alternatively, click **Choose**. In the **Choose the Target Client** dialog box, select the client, and click **OK**.

7. In the **Schedule** list, select an existing Schedule Set, or click **Create New**, and configure the schedule type and schedule method. To run the job as soon as it is submitted, use the "**Immediate**" set.

   For more information about these options, see the *Dell NetVault Backup Administrator's Guide*.

8. In the **Source Options** list, select an existing Source Set, or click **Create New**, and configure the source device options. To use a particular DR Series System, select the **Specify Device** option, and in the list of devices, clear the check marks for the devices that you do not want to use.

   For more information about these options, see the *Dell NetVault Backup Administrator's Guide*.

9. Click **Submit** to submit the job for scheduling.

NOTE: For more information about using NetVault Backup, see the *Dell NetVault Backup Administrator's Guide*.

Supported DR Series System CLI Commands for RDS

The following are the supported DR Series system CLI commands for RDS operations:

```
administrator@DocTeam-SW-01 > rda
Usage:
        rda --show [--config]
                 [--file_history] [--name <name>]
                 [--active_files] [--name <name>]
                 [--clients]
                 [--limits]

        rda --setpassword
        rda --delete_client --name <RDA Client Hostname>

        rda --update_client --name <RDA Client Hostname>
                 --mode <auto|passthrough|dedupe>

        rda --limit --speed <<num><kbps|mbps|gbps> | default>
                 --target <ip address | hostname>

        rda --help

   rda <command> <command-arguments>
   <command> can be one of:
                --show            Displays command specific information.
                --setpassword     Updates the Rapid Data Access (RDA) user
password.
                --delete_client   Deletes the Rapid Data Access (RDA) client.
                --update_client   Updates attributes of a Rapid Data Access
(RDA) client.
                --limit           Limits bandwidth consumed by Rapid Data
Access(RDA) when replicating over a WAN link.

For command-specific help, please type rda --help <command>
        eg:
            rda --help show
```

NOTE: The **--files** in the **rda --show --file_history** command represents replicated files that were processed via the DMA optimized duplication operation. This command displays only up to the last 10 such files. The **--name** in the **rda --show --name** command represents the RDA container name. For more information about RDA-related DR Series system CLI commands, see the *Dell DR Series System Command Line Reference Guide*.

11

Configuring and Using RDA with OST

This topic introduces key RDA with OST tasks and provides links to other related topics that contain procedures that describe how to perform these tasks:

- Configuring the DR Series system for use with OST and the supported DMAs; for more information, see Configuring the DR Series System Using the Backup Exec GUI, and Configuring DR Series System Information Using NetBackup
- Configuring the Logical Storage Unit (LSU) using the DR Series system GUI; for more information, see Configuring an LSU
- Installing the RDA with OST plug-in to a supported media server (Linux or Windows)
- Using supported DMAs to perform backup and restore operations; for more information, see
  - Backing Up Data from a DR Series System Using NetBackup
  - Restoring Data from a DR Series System Using NetBackup
  - Duplicating Backup Images Between DR Series Systems Using NetBackup
  - Creating Backups on the DR Series System Using Backup Exec
  - Restoring Data from a DR Series System Using Backup Exec
  - Optimizing Duplication Between DR Series Systems Using Backup Exec

NOTE: This capability to use RDA with OST, also known as DR Rapid, adds tighter integration with backup software applications, such as the following Symantec OpenStorage-enabled backup applications: NetBackup and Backup Exec.

Understanding RDA with OST

OpenStorage Technology (OST) provides the logical disk interface that can be used with network storage devices, and the DR Series system appliance requires RDA with OST plug-in software to integrate its data storage operations with supported data management applications (DMAs). For details on the applications supported, see the *Dell DR Series System Interoperability Guide*.

The DR Series system integrates with supported DMAs using the RDA with OST plug-in, through which DMAs can control when backup images are created, duplicated, and deleted. Via the plug-in, the DMAs can take full advantage of key DR Series system features like replication and data deduplication.

The DR Series system accesses the OpenStorage API code through the RDA with OST plug-in, which can be installed on the supported media server platform type that you choose (Windows or Linux). When RDA with OST is used with the DR Series system, it offers the following benefits:

- RDA with OST protocol provides faster and improved data transfers:
  - Focus is on backups with minimal overhead
  - Accommodates larger data transfer sizes
  - Provides throughput that is significantly better than CIFS or NFS
- RDA with OST and DMA integration:
  - OpenStorage API enables the DMA-to-media server software communication

  - DR Series system storage capabilities can be used without extensive changes to DMAs
  - Backup and replication operations are simplified by using built-in DMA policies
- DR Series system and RDA with OST ports and write operations:
  - Control channel uses TCP port 10011
  - Data channel uses TCP port 11000
  - Optimized write operations enable client-side deduplication
- Replication operations between DR Series systems:
  - No configuration is required on the source or target DR Series system
  - Replication is file-based, not container-based
  - Replication is triggered by DMA optimized duplication operation
  - DR Series system transfers the data file (not the media server)
  - Once duplication completes, DR Series system notifies DMA to update its catalog (acknowledging the second backup)
  - Supports different retention policies between source and replica
  - Replication is set up in the DMA itself, not the DR Series system

Guidelines

For best results, observe the following guidelines for optimal performance with your supported RDA with OST operations with the DR Series system:

- Backup, restore, and optimized duplication operations need to be performed via the RDA with OST plug-in

  NOTE: The RDA with OST plug-in needs to be installed on client systems to support client-side deduplication.
- Backup:
  - Passthrough writes: Passthrough writes are when data is sent from a media server to the DR Series system without applying any optimization to the data.
  - Optimized writes: Optimized writes are when data is sent from a media server to the DR Series system after optimization is applied to the data.
- Restore
- Replication

Terminology

This topic introduces and briefly defines some basic RDA for OST terminology used throughout the DR Series system documentation.

Term	Description
BE	Symantec DMA, Backup Exec (BE)
DMA/DPA	Data Management Application (also known as Data Protection Application), which are terms for the role played by the backup applications used with RDA with OST; for example, Symantec NetBackup or Backup Exec.
LSU	Logical Storage Unit, which from the DR Series system perspective, represents any container created for data storage. *LSU* is a common storage term while *container* is a common term in DR Series systems that represents a location for storing data.

Term	Description
media server	This is the host running the DMA media server and is where the RDA with OST plug-in is installed. The RDA with OST plug-in can also be installed on a client.
NBU	Symantec DMA, NetBackup (NBU)
OST	The OpenStorage Technology from Symantec, which allows storage devices to deliver backup and recovery solutions with NetBackup. RDA with OST uses the OpenStorage API and a plug-in installed on either a Linux or a Windows-based media server platform.

Supported RDA with OST Software and Components

For the list of supported DMAs and DR Rapid plug-ins, see the *Dell DR Series System Interoperability Guide*, at **support.dell.com/manuals**.

The Dell DR Series system licensing is all-inclusive, so that no additional Dell licensing is required to use RDA with OST or the optimized duplication capability. The RDA with OST plug-in that gets installed on a supported Linux or Windows media server platform is a free download from Dell. However, if you are using Symantec backup applications, you may need to purchase additional licensing to enable OpenStorage Technology; refer to your Symantec documentation.

Best Practices: RDA with OST and the DR Series System

This topic introduces some recommended best practices for using RDA with OST operations with the DR Series system.

- OST and non-OST containers can exist on the same DR Series system. The DR Series system supports having both OST and non-OST containers on the same appliance. However, this can cause incorrect capacity reporting as both container types share the same underlying storage.
- OST replication and non-OST replication on the same DR Series system. Non-OST replication needs to be configured, and it is replicated on a per-container basis. However, this type of replication will not replicate OST containers. OST replication is file-based and is triggered by the DMA.
- Do not change the container connection type from NFS/CIFS to OST. A non-OST container must be deleted before this container can then be created as an OST container using the same name.

Setting Client-Side Optimization

Client-side optimization is a process that can contribute to saving time performing backup operations and reducing the data transfer overhead on the network.

You can turn On or turn Off client-side optimization (also known as client-side deduplication) using the DR Series system CLI commands, **ost --update_client --name --mode**. For more information about DR Series system CLI commands, see the *Dell DR Series System Command Line Reference Guide*, which is available at **support.dell.com/manuals**.

Configuring an LSU

You can configure a logical storage unit (LSU) as an OpenStorage Technology (OST) connection type container for data storage by using the DR Series system GUI. To configure an LSU as an OST connection type container, log in to the DR Series system and complete the following:

1. Navigate to the **Containers** page (in the **Dashboard** navigation panel).
2. Click **Create** to create a new container.

   The **Create New Container** dialog is displayed.

3. In **Container Name**, enter a name for the container.
4. In **Marker Type**, select the **None** marker type.

   For OST operations, only the NetBackup and Backup Exec media servers are supported.
5. In **Connection Type**, set the container type to **Rapid Data Access (RDA)**.

   The RDA pane is displayed.
6. In the **RDA** pane, set the RDA Type to **Symantec OpenStorage (OST)**.
7. In **Capacity**, select either the **Unlimited** or **Size** options to set the capacity for the OST connection type container.

   If you select **Size**, make sure to define the desired size in Gibibytes (GiB).
8. Click **Create a New Container** (or click **Cancel** to display the **Containers** page).

NOTE: For general information about creating DR Series system containers, see Creating Containers, and for creating an OST connection type container, see Creating an OST or RDS Connection Type Container.

NOTE: The capacity option in this command example sets the quota on the LSU. This is the maximum number of bytes (ignoring optimization) that can be written to an LSU and it is listed in the gigabytes (GB). If the capacity option is not specified (or if 0 is specified for the capacity), then the LSU will not have a quota. If this is the case, then this means that the amount of data that can be written to the LSU is limited only by the amount of free space on the disk.

Installing the RDA with OST Plug-In

Before you can start the installation process for the RDA with OST plug-in, you need to understand its role. The plug-in must be installed on to the media server type you choose. (For details on supported platforms, see the *Dell DR Series System Interoperability Guide*.) The RDA with OST plug-in software enables integration between DR Series system data storage operations and the supported data management applications (DMAs).

Understanding the RDA with OST Plug-In (Linux)

The plug-in must be installed on the designated Linux-based media server running the support Linux server operating system software in the following directory: **/usr/openv/lib/ost-plug-ins**. The RDA with OST plug-in is installed using a self-extracting installer that installs the plug-in and all of its related components. The installer supports the following modes, with the default being Help (-h):

NOTE: If no option is selected, the Help mode is displayed by default.

- Help (-h)
- Install (-install)
- Upgrade (-upgrade)
- Uninstall (-uninstall)
- Force (-force)

```
$> ./DellOSTPlugin-xxxxx-x86_64.bin -help
Dell plug-in installer/uninstaller
usage: DellOSTPlugin-xxxxx-x86_64.bin [ -h ] [ -install ] [ -uninstall ]
-h                     : Displays help
-install          : Installs the plug-in
-upgrade          : Upgrades the plug-in
-uninstall      : Uninstalls the plug-in
-force              : Forces the installation of the plug-in
```

You can download the RDA with plug-in installer in two ways:

- Using the DR Series system GUI:

  - Click **Storage** → **Clients**
  - Click the **RDA** tab in the **Clients** page, and click **Download Plug-In**
  - Select the appropriate plug-in in the **Download Plug-Ins** page, and click **Download**
- Using the Dell website:
  - Navigate to **support.dell.com/** and locate the Drivers and Downloads location
  - Locate the RDA with OST plug-in for Linux and download this to your system.

After it is downloaded, run the RDA with OST plug-in installer to install the plug-in on your designated Linux-based media server.

NOTE: The RDA with OST plug-in must be installed on client systems to support client-side deduplication.

Understanding the RDA with OST Plug-In (Windows)

The RDA with OST plug-in must be installed in the following directory on the designated Windows-based media server running the supported Microsoft Windows server operating system software: **$INSTALL_PATH\VERITAS\Netbackup\bin\ost-plug-ins** for NetBackup installations, and **$INSTALL_PATH\Symantec\Backup Exec\bin\** for Backup Exec installations. After it is downloaded, you can use **SETUP** to install the RDA with OST plug-in.

NOTE: The RDA with OST plug-in must be installed on client systems to support client-side deduplication.

Installing the RDA with OST Plug-In for Backup Exec on Windows

This topic describes how to install the RDA with OST plug-in within a Microsoft Windows environment for performing DR Series system operations via the plug-in.
Make sure that you meet all of the following prerequisites before installing the plug-in:

1. The Backup Exec installation must be running on one of the supported Windows media server platforms. For information on the supported versions of Backup Exec and operating systems, see the *Dell DR Series System Interoperability Guide*, available at **support.dell.com/manuals**.
2. The Windows RDA with OST installer must be downloaded. If not, download the Windows installer (DellOSTPlugin-xxxxx.msi), which is available at **support.dell.com/drivers**, to a network directory location you can access.

To install the RDA with OST plug-in, complete the following:

1. Launch the **Backup Exec Administrator** console, select **Tools**, and **Backup Exec Services...**.

   The **Backup Exec Services Manager** page is displayed.
2. Select the server on which you want to install the RDA with OST plug-in, and select **Stop all services**.

   The **Restarting Backup Exec Services** page is displayed, which lists the current status of services for the selected server.
3. Click **OK**.
4. Launch the **Dell Storage Plug-In for Symantec OST Setup Wizard** (and accept all default values).
5. In the **Welcome** page, click **Next** to continue.

   The **End-User License Agreement** page is displayed.
6. Click **I accept the terms in the License Agreement**, and click **Next**.
7. In the **Destination Folder** page, accept the default destination location, and click **Next**.
8. In the **Ready to Install Dell Storage Plug-In for Symantec OST** page, click **Install**.

   When the plug-in has been installed, the **Completed the Dell Storage Plug-In for Symantec OST Setup Wizard** page is displayed.
9. Click **Finish** to exit the wizard.

Installing the RDA with OST Plug-In for NetBackup on Windows

This topic describes how to install the RDA with OST plug-in on a media server running the supported Microsoft Windows server operating system software (and using the NetBackup DMA).
Ensure that you have downloaded the RDA with OST plug-in installer into the correct directory on the designated media server. The plug-in installer is saved as DellOSTPlugin64–xxxxx.msi (for 64–bit operating systems), or DellOSTPlugin-xxxxx.msi (for 32-bit operating systems). Ensure that the correct plug-in is downloaded to support your 64-bit or 32-bit system.

1. Stop the NetBackup services if they are running, by using the following command:
   ```
   $INSTALL_PATH\VERITAS\NetBackup\bin\bpdown.exe
   ```
2. Run **SETUP** to install the plug-in.
3. Check that the plug-in is installed by using the following NetBackup command on the Windows media server:
   ```
   $INSTALL_PATH\VERITAS\NetBackup\bin\admincmd\bpstsinfo.exe -pi
   ```

   This NetBackup command lists the plug-in details, as shown in the following example:

   - Plug-In Name: libstspiDellMT.dll
   - Prefix: DELL
   - Label: OST Plug-in that interfaces with the DR Series system
   - Build Version: 9
   - Build Version Minor: 1
   - Operating Version: 9
   - Vendor Version: Dell OST plug-in 10.1
4. Start the NetBackup services by using the following command:
   ```
   $INSTALL_PATH\VERITAS\NetBackup\bin\bpup.exe
   ```

Uninstalling the RDA with OST Plug-In for Windows

Use the following process if you need to uninstall the RDA with OST plug-in from a Windows-based media server.
Use the standard Microsoft Windows uninstall process to uninstall the RDA with OST plug-in from a Windows-based media server.

NOTE: Dell recommends that you retain the RDA with OST plug-in installer on the media server in case you need to use it to reinstall the plug-in.

1. Click **Start**, and click **Control Panel**.

   The **Control Panel** page is displayed.
2. Under **Programs and Features**, click **Uninstall a program**.

   The **Uninstall or change a program** page is displayed.
3. Locate the RDA with OST plug-in in the listed of installed programs, right-click and select **Uninstall**.

   The **Programs and Features** confirmation dialog is displayed.
4. Click **Yes** to uninstall the plug-in.

Installing the RDA with OST Plug-In for NetBackup on Linux

This topic describes how to install the RDA with OST plug-in on a media server running the supported Red Hat Enterprise Linux or SUSE Linux server operating system software (using the NetBackup DMA).
Ensure that you have downloaded the RDA with OST plug-in installer into the correct directory on the designated media server. The plug-in installer is saved as DellOSTPlugin-xxxxx-x86_64.bin.gz, where *xxxxx* represents its build number.

1. Unzip the RDA with OST plug-in installer file using the following command:

   ```
   $> /bin/gunzip DellOSTPlugin-xxxxx-x86_64.bin.gz
   ```

2. Configure the executable bit on the plug-in installer using the following command:

   ```
   $> /bin/chmod a+x DellOSTPlugin-xxxxx-x86_64.bin
   ```

3. Stop the NetBackup nbrmms service before using the **-install** option.

   The plug-in installer returns an error if the NetBackup nbrmms service is running when attempting to install the plug-in.

4. Run the plug-in installer using the **-install** option, and install the plug-in using the following command:

   ```
   $> ./DellOSTPlugin-xxxxx-x86_64.bin -install
   ```

   NOTE: The location for installing the plug-in is not user-configurable.

5. After the RDA with OST plug-in installer has stopped running, and the system prompt returns, verify that the plug-in has loaded properly by checking the output using the following NetBackup command on the Linux media server:

   ```
   $> /usr/openv/netbackup/bin/admincmd/bpstsinfo -plugininfo
   ```

   This NetBackup command lists the plug-in details as shown:

   - Plug-In Name: libstspiDellMT.so
   - Prefix: DELL
   - Label: Dell OpenStorage (OST) Plug-in
   - Build Version: 10
   - Build Version Minor: 1
   - Operating Version: 10
   - Vendor Version: (EAR-2.0.0) Build: 41640

6. Retain the plug-in installer on the media server so you can use it if needed to uninstall the plug-in.

Uninstalling the RDA with OST Plug-In for Linux

Use the following process if you need to uninstall the RDA with OST plug-in from a Linux-based media server:

1. Stop the NetBackup nbrmms service before using the **-uninstall** option.

   (The plug-in installer returns an error if the NetBackup nbrmms service is running when attempting to uninstall the OST plug-in.)

2. Run the RDA with OST plug-in installer with the **-uninstall** option, which uninstalls the plug-in, using the following command:

   ```
   $> ./DellOSTPlugin-xxxxx-x86_64.bin -uninstall
   ```

3. Check that the plug-in is uninstalled by using the following NetBackup command on the Linux media server:

   ```
   $> /usr/openv/netbackup/bin/admincmd/bpstsinfo -plugininfo
   ```

   NOTE: If the **-pluginfo** command returns any plug-in details, this means that the plug-in has not been uninstalled.

4. Retain the plug-in installer on the media server in case you need to use it to reinstall the plug-in.

Configuring DR Series System Information Using NetBackup

The topic introduces the concept of configuring the DR Series system information using the NetBackup media server command line interface (CLI) commands and graphical user interface (GUI) menus, tabs, and options. The NetBackup CLI commands and GUI menus, tabs, and options allow you to configure both the Linux or Windows media servers. In the *DR Series System Administrator Guide* documentation, you will find specific topics that address operations for using the NetBackup CLI, such as adding the DR Series system name to NetBackup on each Linux and Windows media server you intend to use with the DR Series system, using the NetBackup GUI to configure it to work with the DR Series system via OST, using the NetBackup GUI to configure disk pools from logical storage units (LSUs) on the DR Series system, and using the NetBackup GUI to create storage units using the disk pools on the DR Series system.

Related Links

Configuring NetBackup for the DR Series System

Configuring the DR Series System Using the Backup Exec GUI

Using NetBackup CLI to Add DR Series System Name (Windows)

Using NetBackup CLI to Add the DR Series System Name (Linux)

Using NetBackup CLI to Add DR Series System Name (Linux)

This topic describes how to use the NetBackup CLI to add the DR Series system name to each Linux-based media server you plan to use with the DR Series system.

1. Add the DR Series system name to NetBackup by using the following command:
   ```
   /usr/openv/netbackup/bin/admincmd/nbdevconfig -creatests
   -storage_server servername -stype DELL -media_server mediaservername
   ```
2. Log in to and authenticate with DR Series system by using the following command (for details, see Configuring an LSU).
   ```
   /usr/openv/volmgr/bin/tpconfig -add -storage_server servername -stype DELL -
   sts_user_id backup_user -password password
   ```

   NOTE: On the DR Series system, only one user account exists, and the user ID for that account is backup_user. You can only change the password for this account; you cannot create a new account nor can the existing account be deleted.

Using NetBackup CLI to Add DR Series System Name (Windows)

This topic describes how to use the NetBackup CLI to add the DR Series system name to each Windows-based media server you plan to use with the DR Series system.

1. Add the DR Series system name to NetBackup by using the following command:
   ```
   $INSTALL_PATH\VERITAS\NetBackup\bin\admincmd\nbdevconfig
   -creatests -storage_server servername -stype DELL -media_server
   mediaservername
   ```
2. Log in to and add the valid credentials for authentication by the DR Series system by using the following command (for details, see Configuring an LSU).
   ```
   $INSTALL_PATH\VERITAS\Volmgr\bin\tpconfig -add -storage_server servername -
   stype DELL -sts_user_id backup_user -password password
   ```

Configuring NetBackup for the DR Series System

Use the NetBackup graphical user interface (GUI) to configure it to work with the DR Series system via RDA with OST. This process is essentially the same type of operation for either the Linux or Windows platforms.
Log in to NetBackup, and complete the following:

1. In the main window of the **NetBackup Administrator** console, click **Configure Disk Storage Servers** to launch the **Storage Server Configuration Wizard**.

   The **Storage Server Configuration Wizard** page is displayed, which is where you can add a storage server.
2. Select **OpenStorage** to choose the type of disk storage that you want to configure in this window, and click **Next**.

   The **Add Storage Server** page is displayed.
3. Enter the following values to configure a storage server:

   - In **Storage server type**, enter **DELL**.
   - In **Storage server name**, enter the name of the DR Series system.
   - In the **Select media server** drop-down list, select the desired media server (the server on which you are configuring RDA with OST).
   - Enter values for the credential needed to authenticate with the DR Series system:
     - **User name**
     - **Password**
     - **Confirm password**

   The credentials should be the same as the credentials that are required for the DR Series system. For more information, see Configuring an LSU.
4. Click **Next**.

   The **Storage Server Configuration Summary** page is displayed, which lists the values you configured.
5. Click **Next**.

   The storage server you configured and the corresponding credentials are displayed in the **Storage Server Creation Status** page.
6. Click **Next** and click **Finish** to close the **Storage Server Configuration Wizard**.

   The **Storage server** *servername* **successfully created page** is displayed. NetBackup is now configured for use with the DR Series system.

Configuring NetBackup for Optimized Synthetic Backups

This procedure describes how to configure NetBackup so that it supports Symantec optimized synthetic backups. Optimized synthetic backups use RDA with OST to share data between images and synthesize the backup directly on the DR Series system without data being read to and written from the backup server. This saves time, expense, and space. The DR Series system supports optimized synthetic backups with NetBackup 7.1 and 7.5. The NetBackup storage server inherits the Optimized Image attribute during storage server configuration (nbdevconfig - creatests).
To configure NetBackup to use optimized synthetic backups:

1. Use the following command to add the OptimizedImage flag to each NetBackup storage server that needs to support optimized synthetic backups:

   ```
   nbdevconfig -changests -stype PureDisk -storage_server ss_name -setattribute
   OptimizedImage
   ```

   For `ss_name`, make sure to type the name of the storage server as you configured it in NetBackup.
2. Use the following command to add the OptimizedImage flag to each NetBackup disk pool that needs to support optimized synthetic backups:

```
nbdevconfig -changedp -stype PureDisk -dp dp_name -setattribute
OptimizedImage
```

For `dp_name`, make sure to type the name of the disk pool as you configured it in NetBackup. Make sure to add the OptimizedImage flag to the storage server first, and then to the disk pool.

Creating Disk Pools From LSUs

Use the NetBackup graphical user interface (GUI) to configure disk pools from logical storage units (LSUs) on the DR Series system.
Log in to NetBackup, and complete the following:

1. In the main window of the **NetBackup Administrator** console, click **Configure Disk Pools** to launch the **Disk Pool Configuration Wizard**.

   The **Disk Pool Configuration Wizard** page is displayed, which is where you define media servers for use in a disk pool.
2. In the **Welcome to the Disk Pool Configuration Wizard** page, click **Next**.

   The **Disk Pool** page is displayed.
3. In **Type**, select **OpenStorage (DELL)**, and click **Next**.

   The **Select Storage Server** page is displayed, and contains a list of available storage servers.
4. In the **Storage server** list, select a server, and click **Next**.

   The **Disk Pool Properties** page is displayed.
5. Select the LSUs (volumes) to include from the list, and click **Next**.

   The **Disk Pool Properties** page is displayed.
6. Enter a **Disk pool name**, and click **Next**.

   The **Summary** page for the **Disk Pool Configuration Wizard** is displayed.
7. Verify the disk pool configuration in the **Summary** page, and click **Next** to configure the disk pool you created.

   The **Performing required task** page is displayed, with the status being: **Configuration completed successfully**. You have several options available at this point:

   - Clear the **Create a storage unit** for the disk pool.
   - Click **Finish** and close the **Disk Pool Configuration Wizard**.
   - Click **Next** to create the storage unit with this disk pool.

   NOTE: If you create the storage unit using the **Disk Pool Configuration Wizard**, you can skip the step where you create storage units using a disk pool.
8. Click **Next** to continue with creating a storage unit using this wizard.
9. Enter a **Storage unit name**, and click **Next**.

   The **Successfully Completed Disk Pool Configuration** page is displayed.
10. Click **Finish**.

To display the disk pool you created, click **Devices** → **Disk Pools** in the left navigation pane in the **NetBackup Administrator** console.

Creating Storage Units Using the Disk Pool

Use the NetBackup GUI to create storage units using the disk pools on the DR Series system.
Log in to NetBackup, and complete the following tasks:

1. In the main window of the **NetBackup Administrator** console, click **Storage** in the left navigation pane, and select **Storage Units**.
2. In the **NetBackup Administrator** console main window, right-click and select **New Storage Unit** from the drop-down list.
3. In the **New Storage Unit** page, enter a name in **Storage unit name**, and select the OST disk pool that you created in the **Disk pool** drop-down list.
4. Click **OK** to create the new storage unit.

Backing Up Data From a DR Series System (NetBackup)

This topic describes how to use NetBackup to back up data from a DR Series system.
Before backing up data, you first need to configure a policy that creates a backup on the OST logical storage unit (LSU). This type of policy is similar to what is done for network-attached storage (NAS) shares, except that when defining policy attributes, you need to select the LSU that contains the OST disk pool.
To back up data from a DR Series system using a policy, complete the following:

1. Log into the **NetBackup Administrator** console.
2. Click **NetBackup Management** in the left navigation pane, and select **Policies**.
3. In the **All Policies** main window, right-click **OST**, and select **Change Policy** from the drop-down list.

   The **Change Policy** page is displayed.
4. In the **Change Policy** page, click the **Attributes** tab, and select the settings for the policy you want to create.
5. Click **OK** to create the policy, which displays under OST in the main window.
6. Right-click the policy, and select **Manual Backup** from the drop-down list.

   The **Manual Backup** page is displayed.
7. In the **Manual Backup** page, enter the name of the media server in **Server**, and click **OK**.

To monitor the status of any backup operation, click **Activity Monitor** in the left navigation pane of the **NetBackup Administrator** console, and select the backup job you are interested in to view details about the operation.

Restoring Data From a DR Series System Using NetBackup

This topic describes how to use NetBackup to restore data from a DR Series system. The process for restoring data from OST logical storage units (LSUs) is similar to how restores are performed from any backup device.
To restore data from a DR Series system, complete the following:

1. Log into the **NetBackup Administrator** console.
2. Click **Backup, Archive**, and **Restore** in the left navigation pane.
3. In the **Restore** main window, click the **Restore Files** tab.
4. Select the data that you want to restore, and click **OK**.

To monitor the status of any restore operation, click **Activity Monitor** in the left navigation pane of the **NetBackup Administrator** console, and select the restore job you are interested in to view details about the operation.

Duplicating Backup Images Between DR Series Systems Using NetBackup

Using NetBackup with the DR Series system, you can duplicate backup images from a disk pool on one DR Series system to a target disk pool (or a storage unit derived from it) that could be on the same DR Series system or on a different DR Series system.
To duplicate backup images between DR Series systems using NetBackup, complete the following:

1. Log into **NetBackup Administrator** console.
2. Click **NetBackup Management** in the left navigation pane, and select **Catalog**.
3. In the **Catalog** main window, select **Duplicate** from the **Action** drop-down list, and click **Search Now**.

   The **Search Results** pane is displayed, which lists images from which you can choose to duplicate.
4. Right-click to select the image in the **Search Results** pane that you would like to duplicate, and select **Duplicate** in the drop-down list.

   The **Setup Duplication Variables** page is displayed.
5. In the **Setup Duplication Variables** page, select the LSU that is the target DR Series system in the **Storage unit** drop-down list, and click **OK**.
6. To monitor the status of any duplicate image operation, perform the following:
   a. Click **Activity Monitor** in the left navigation pane of the **NetBackup Administrator** console.
   b. Select the data duplication job in which you are interested.
   c. View the operation details.

Using Backup Exec With a DR Series System (Windows)

This topic introduces the RDA with OST plug-in and describes the installation prerequisites for Backup Exec within a Microsoft Windows environment. After it is installed, Backup Exec can perform DR Series system operations via the plug-in.

RDA with OST Plug-In and Supported Versions

For details on the supported Backup Exec versions and media server operating systems, see the *Dell DR Series System Interoperability Guide*, available at **support.dell.com/manuals**.

Installation Prerequisites for the RDA with OST Plug-In for Backup Exec

This topic introduces the installation prerequisites for installing the plug-in for Backup Exec on Windows media servers.
Ensure that you meet the following prerequisites prior to installing the plug-in:

1. The Backup Exec installation must be running on one of the supported Windows platforms.
2. Dell recommends that the DR Series system appliance have an OST container created and configured. For details, see Configuring an LSU.
3. The RDA with OST plug-in must be downloaded. If not, download the Windows installer (DellOSTPlugin-xxxxx.msi or DellOSTPlugin64-xxxxx.msi), which is available at **support.dell.com/support/drivers**, to a network directory location you can access.
4. The plug-in needs to installed in the following directory on the designated Windows-based media server running the supported Microsoft Windows operating system software ($INSTALL_PATH\VERITAS\NetBackup\bin\ost-plugins) for NetBackup installations.

Configuring the DR Series System Using the Backup Exec GUI

Backup Exec only supports the use of its own graphical user interface (GUI) for configuring the DR Series system. There is no supported Backup Exec command-line interface (CLI) for using Backup Exec 2010 version.
To configure the DR Series system using the Backup Exec GUI, complete the following:

1. Launch the **Backup Exec Administrator** console, select **Tools**, and **Backup Exec Services...**.
2. Select the server that you want to configure in the **Backup Exec Services Manager** page, and select **Start all services**.
3. Verify that all services have been started, and click **OK**.
4. In the **Connect to Media Server** page, log into the media server, and enter a **User name**, a **Password**, and click **OK**.
5. In the **Backup Exec Administrator** page, click **Network**, and click **Logon Accounts**.

   The **Logon Account Management** page is displayed.
6. Click **New** to create a new logon account.

   The **Add Logon Credentials** page is displayed.
7. In the **Account Credentials** pane, enter the **User name** and **Password** account credentials for the DR Series system, and click **OK** (for example, the default user name is **backup_user**).
8. In the **Backup Exec Administrator** page, click the **Devices** tab, and right-click on the local system name that is listed as the root node.

   A drop-down list of device-related options is displayed.
9. Select **Add OpenStorage** in the drop-down list.

   The **Add OpenStorage Device** page is displayed.
10. Configure the **Add OpenStorage Device** page with the following information, and click **OK**:

    - **Server**—enter the host name or IP address of the DR Series system.
    - **Logon account**—select the account from the drop-down list, which has credentials for accessing the DR Series system.
    - **Server type**—select the type of plug-in from the drop-down list (DELL OST plug-in).
    - **Logical storage unit**—enter the LSU (DR Series system container) name to use.
11. Click **Yes** in response to the prompt about making the new device the default destination for new jobs.
12. Close the **Add OpenStorage Device** page.

    The **Restart Services** confirmation dialog is displayed (this dialog recommends against restarting the services if any jobs are currently running).
13. Click **Restart Now** to restart the Backup Exec services.

Creating Backups on the DR Series System Using Backup Exec

This topic describes how to use Backup Exec to create backups on the DR Series system.
To create backups on the DR Series system using Backup Exec, complete the following:

NOTE: This procedure documents this process using Backup Exec 2010. The procedure for Backup Exec 2012 is different. For specific details and procedures, see the product-specific documentation from Symantec for the specific DMA product and version you are using.

1. Launch the **Backup Exec Administrator** console, and select the **Job Setup** tab.
2. Click **Backup Tasks** in the left navigation panel, and select **New job**.

   The **Backup Job Properties** page is displayed.
3. In the left navigation pane of the **Backup Job Properties** page, select **Source**, and select **Selections**.

   The **Selections** page is displayed.

4. Select the system or node name in the center pane of the **Selections** page, and click the check boxes that correspond to the files you want backed up.
5. In the left navigation pane of the **Backup Job Properties** page, select **Destination**, and select **Device and Media**.

   The **Device and Media** page is displayed.
6. In the **Device** pane in the **Device and Media** page, select the **DELL OST** device in the drop-down list, and click **Run Now** to start the backup job.
7. Click the **Job Monitor** tab to view the progress of the backup job you created.

Optimizing Duplication Between DR Series Systems Using Backup Exec

Backup Exec can replicate backups between two DR Series systems that are part of a defined source and target replication pair. This process uses the deduplication and replication features of the DR Series system via RDA with OST. Using RDA with OST, backed up data is catalogued which makes it available from the designated media server so that a seamless restore can be performed from either the target or source DR Series system. This is considered an integrated replication, where the appliance does the replication. It is considered to be "optimized" because the data flows from the local appliance directly to the remote appliance in a deduplicated format, and it does not travel through the media server.

When the data is in a deduplicated format (in an optimized form), only new or unique data is copied between the two DR Series systems. Because the duplication job is initiated by Backup Exec, there are two entries in its catalog: one entry is for the source file, while the other entry is for the target file. The backup administrator can restore backup data from either appliance in case of data loss or disaster.

To optimize duplication between DR Series systems, create an additional OST device that points to the target DR Series system, and complete the following steps:

1. Launch the **Backup Exec Administrator** console, select the **Devices** tab, and right-click the target DR Series system.
2. Select **Add OpenStorage** in the drop-down list.

   The **Add OpenStorage Device** page is displayed
3. Configure the **Add OpenStorage Device** page with the following information:

   - **Server**—enter the host name or IP address of the DR Series system.
   - **Logon account**—select the account from the drop-down list (or click **...** and browse to the account location), which has credentials for accessing the DR Series system.
   - **Server type**—select the type of server from the drop-down list (**DELL**).
   - **Logical storage unit**—enter the name of the logical storage unit (LSU), also known as a DR Series system container, to use.
4. Click **Yes** in response to the prompt if you want to make the new device the default destination for new jobs.
5. Close the **Add OpenStorage Device** page.
6. Click the **Job Setup** tab.
7. In the left navigation pane, select **Backup Tasks**, and click **New job** to duplicate backup sets.

   The **New Job to Duplicate Backup Sets** page is displayed.
8. Select **Duplicate existing backup sets**, and click **OK**.
9. Click the **View by Resource** tab in the **Selections** page, and select the dataset you want copied.
10. In the left navigation pane, select **Destination**, and select **Device and Media**.
11. In **Device**, select the destination device from the drop-down list (that was created in this procedure), and click **Run Now** to start the replication operation between the two DR Series systems.
12. Click the **Job Monitor** tab to view the progress of the replication operation you created.

Restoring Data from a DR Series System Using Backup Exec

This topic describes how to use Backup Exec to restore data from a DR Series system.
To restore data from a DR Series system using Backup Exec, complete the following:

1. Launch the **Backup Exec Administrator** console, and select the **Job Setup** tab.
2. In the left navigation pane, select **Restore Tasks**, and click **New job**.

   The **Restore Job Properties** page is displayed.
3. Click the **View by Resource** tab in the **Selections** pane, and select the dataset to be restored.
4. Click **Run Now** to start the restore job.
5. Click the **Job Monitor** tab to view the progress of the restore job operation you created.

Understanding the OST CLI Commands

The **--mode** component supported in the DR Series system command line interface (CLI) command supports three values, which represent optimized writes done via:

- deduplication (**--mode dedupe**) The client will process hashing on data, so deduplication processing occurs on the server side (client-side deduplication).
- passthrough (**--mode passthrough**) The client will pass all data to DR for deduplication processing (appliance-side deduplication).
- auto (**--mode auto**)
  DR will set the deduplication to Dedupe or Passthrough, based on the client's number of cores and whether it is 32– or 64–bit.

These OST commands are used in the following format: **ost --update_client --name --mode**.

NOTE: If a RDA with OST client has four or more CPU cores, it is considered to be dedupe-capable. However, the client operating mode depends upon how it is configured in the DR Series system (**Dedupe** is the default RDA with OST client mode). If the administrator did not configure a client to operate in a specific mode and it is dedupe-capable, it will run in the **Dedupe** mode. If a client is not dedupe-capable (meaning the client has less than four CPU cores), and the administrator sets it to run in the **Dedupe** mode, it will only run in the **Passthrough** mode. If a client is set to run in **Auto** mode, the client will run in the mode setting determined by the media server. The following table shows the relationship between the configured client mode types and the supported client mode based on client architecture type and corresponding number of CPU cores.

Table 3. Supported RDA with OST Client Modes and Settings

Client Mode Settings	32–Bit Client (4 or more CPU cores)	64–Bit Client (4 or more CPU cores)	32–Bit Client (Less than 4 CPU cores)	64–Bit Client (Less than 4 CPU cores)
Auto	Passthrough	Dedupe	Passthrough	Passthrough
Dedupe	Not Supported	Supported	Not Supported	Not Supported
Passthrough	Supported	Supported	Supported	Supported

Supported DR Series System CLI Commands for RDA with OST

The following are the supported DR Series system CLI commands for RDA with OST operations:

```
administrator@acme100 > ost
Usage:
   ost --show [--config]
```

```
              [--file_history] [--name <name>]
              [--clients]
              [--limits]

   ost --setpassword
   ost --delete_client --name <OST Client Hostname>

   ost --update_client --name <OST Client Hostname>
       --mode <auto|passthrough|dedupe>

   ost --limit --speed <<num><kbps|mbps|gbps> | default>
       --target <ip address | hostname>

   ost --help

ost <command> <command-arguments>
<command> can be one of:
   --show            Displays command specific information.
   --setpassword     Updates the OST user password.
   --delete_client   Deletes the OST client.
   --update_client   Updates attributes of the OST client.
   --limit           Limits bandwidth consumed by ost.

For command-specific help, please type ost --help <command>
For example:
     ost --help show
```

NOTE: The **--files** in the **ost --show --file_history** command represents replicated files that were processed via the DMA optimized duplication operation. This command displays only up to the last 10 such files. The **--name** in the **ost --show --name** command represents the OST container name.

NOTE: For more information about OST-related DR Series system CLI commands, see the *Dell DR Series System Command Line Reference Guide*.

Understanding RDA with OST Plug-In Diagnostic Logs

You can collect diagnostic logs for supported DMAs with the RDA with OST plug-in.

NOTE: The directory location, C:\ProgramData, is considered to be a hidden directory on Windows-based systems. However, you can copy and paste **C:\ProgramData\Dell\DR\log\** into your Internet Explorer **Address bar** or you can enter this into the Windows command prompt window (**Start→ All Programs→ Accessories→ Command Prompt**).

For more information about RDA with OST plug-ins and logs, see the topics that follow.

Rotating RDA with OST Plug-In Logs for Windows

By default, the Windows log rotation size is set at 10 megabytes (MB). Once a log file has been reached this size, the RDA with OST plug-in automatically renames the existing log file, libstspiDell.log to libstspiDell.log.old, and creates a new log.

Modifying Log Rotation Size

To modify the log rotation size, you can edit the following registry key value:

```
HKLM\Software\Dell\OST\LogRotationSize
```

Immediately after modifying this value, the new rotation size value takes effect (meaning that you do not have to restart the backup process).

Collecting Diagnostics Using a Linux Utility

You can use a Linux utility called **Dell_diags** to collect diagnostics from Linux-only clients. This Linux utility is installed by the OST plug-in installer in the /opt/Dell directory. The tool collects the following types of information:

- var/log/libstspiDell.log.*
- usr/openv/netbackup/logs
- usr/openv/logs/nbemm/
- usr/openv/logs/nbrmms/

The **Dell_diags** diagnostics file is written to the following location: /var/log/diags_client location.

The following example shows the process for collecting the RDA with OST diagnostic logs (the root user account shown represents one that resides on the media server, and is not to be confused with a root user account on the DR Series system):

```
root@oca3400-74 ~]# ./Dell_diags –collect
Collecting diagnostics...Done
Diagnostics location: /var/log/diags_client//oca3400-74_2012-02-27_23-02-13.tgz
```

The default log level is set to **Error** in the OST plug-in, is user-configurable, and can be modified via the DR Series system CLI or GUI.

Rotating RDA with OST Plug-In Logs for Linux

If you set the RDA with OST plug-in log level to **Debug**, this can cause the plug-in log to quickly grow in size. The best practice for preventing any issues with log sizes is to rotate the plug-in logs using the **logrotate** utility that is commonly available on Linux-based systems.
To configure log rotation, complete the following:

1. Create a file in /etc/logrotate.d/, name it “ost”, and add the following entries:

   ```
   /var/log/libstspiDell.log {
       rotate 10
       size 10M
       copytruncate
   }
   ```

2. Create a file in /etc/cron.hourly/, name it “ost_logrotate.cron”, and add the following entries:

   ```
   #!/bin/bash
   /usr/sbin/logrotate /etc/logrotate.d/ost
   ```

The **logrotate** utility runs every hour, and rotates the logs whenever the log file size exceeds 10 megabytes (MB). This procedure is automated as part of the plug-in installation.

Guidelines for Gathering Media Server Information

In addition to the DR Series system diagnostics log file bundles and core files that you can collect for history and troubleshooting purposes, if you have run any RDA with OST operations, Dell recommends that you also gather some important media server-related files. This topic introduces some of these key media server files that reside on Linux and Windows platforms .

NetBackup on Linux Media Servers

For NetBackup running on a Linux media server, Dell recommends gathering the following files:

- RDA with OST plug-in configuration files and log files from the media server
  - Location: /var/log/libstspiDell.log.*
- NetBackup backup job logs and command logs from the media server:
  - Location: NetBackup log files reside in /usr/openv/netbackup/logs/. For each process in NetBackup, there is a subdirectory in the logs directory. Dell is interested in the following process-related logs: bptm, bpdm, bprd, bpcd, bpbrm.
  - Be aware that these five directories may not exist by default, so only collect these logs if they exist on your media server. If they were created, the locations where these log files reside are as follows: /usr/openv/netbackup/logs/bptm, /usr/openv/netbackup/logs/bpdm, /usr/openv/netbackup/logs/bpcd, /usr/openv/netbackup/logs/bprd, and /usr/openv/netbackup/logs/bpbrm.
  - Dell recommends that you collect logs from the following directories: /usr/openv/logs/nbemm and /usr/openv/logs/nbrmms/.
- Check for any core files that were generated on the NetBackup media server or on the DR Series system that can include:
  - Core files on a Linux NetBackup media server reside in the /usr/openv/netbackup/bin directory. Most of the NetBackup binaries that link with the RDA with OST plug-in are in this directory.
  - The location of the core files on the client is not a fixed location. Verify if the core files reside in following directories: /, /root/, or the directory mentioned in the /proc/sys/kernel/core_pattern. For example, if the following is a core_pattern from a DR Series system (/var/cores/core.%e.%p.%t), then all the core files would reside in /var/cores.

Dell recommends that if core_pattern on the client is set by NAT to a specific directory, then the diagnostics script has to look into that directory for any related cores.

NetBackup on Windows Media Servers

For NetBackup running on a Windows media server, Dell recommends gathering the following files:

- RDA with OST plug-in configuration files and log files from the media server:
  - Location: %ALLUSERSPROFILE%\Dell\OST\log\libstspiDell.log*
- NetBackup job logs and command logs from the media server, with log files from following directories:
  - C:\Program Files\Veritas\NetBackup\logs\bptm (if it exists)
  - C:\Program Files\Veritas\NetBackup\logs\bpdm (if it exists)
  - C:\Program Files\Veritas\NetBackup\logs\bpbrm (if it exists)
  - C:\Program Files\Veritas\NetBackup\logs\bprd (if it exists)
  - C:\Program Files\Veritas\NetBackup\logs\bpcd (if it exists)
  - C:\Program Files\Veritas\NetBackup\logs\nbemm
  - C:\Program Files\Veritas\NetBackup\logs\nbrmms
- Any core files generated on the NetBackup media server or on the DR Series system.
- If a server failure is involved (which could be an inapparent or silent failure), the Windows media server event log for the application could be collected by using **Administrative Tools → Event Viewer**. Next, check the **Windows Logs → Application**. Typically, the last entry marked with **Error** is the one for which you are searching.
  - Copy and paste this text in the window, as shown in the following example:

    ```
    Faulting application bptm.exe, version 7.0.2010.104, time stamp
    0x4b42a78e, faulting module libstspiDellMT.dll, version 1.0.1.0, time
    stamp 0x4f0b5ee5, exception code 0xc0000005, fault offset
    0x000000000002655d, process id 0x12cc, application start time
    0x01cccf1845397a42.
    ```

- If the system is unresponsive, force the crash of bptm.exe and complete the following:

  1. Click to open **Task Manager**.
  2. Locate the process.
  3. Right-click, and select **Create Dump File**.
  4. Retrieve the dump file from the location specified in the dialog that displays after the dump file is created.

Backup Exec on Windows Media Servers

For Backup Exec running on a Windows media server, Dell recommends gathering the following files:

- RDA with OST plug-in configuration files and log files from the media server:
  - Location: %ALLUSERSPROFILE%\Dell\OST\log\libstspiDell.log*
- Backup Exec job logs and command logs from the media server.
- Any core files generated on the Backup Exec media server or on the DR Series system.
- If a crash is involved, collect any mini-dump file(s) that reside in %ProgramFiles%\Symantec\Backup Exec\BEDBG.
- If the system is unresponsive, force the crash of pvlsvr.exe and bengine.exe, and complete the following:

  a. Open Task Manager.

  b. Locate the process.

  c. Right-click, and select **Create Dump File**.

  d. Retrieve the dump file from the location specified in the dialog that displays after the dump file is created.

12

Configuring and Using VTL

This topic introduces Virtual Tape Libraries (VTLs) and related concepts and tasks. Refer to the following topics and procedures:

Understanding VTL

A Virtual Tape Library (VTL) is an emulation of a physical tape library on a disk-based deduplication and compression system such as the DR Series system. The tape library is exposed to a Data Management Application (DMA) as if it is a physical library with tape drives and cartridges, which the application uses for backup. Because a VTL completely emulates a standard library, the introduction of virtual tape is seamless and transparent to existing tape backup/ recovery applications. The management of the library, including the drives and tapes, is done by the DMA using SCSI commands. For details on the applications supported, see the *Dell DR Series System Interoperability Guide*.

Terminology

This topic introduces and briefly defines some basic VTL terminology used throughout the DR Series system documentation.

Term	Description
Library	A library is an emulation of a physical tape library and shares the same characteristics such as media changer, tape drives, and slots (cartridge slots).
Tape Drive	A Tape drive is a logical unit which is part of the emulated library. The media or cartridge is loaded in the Tape drives to be accessed by the Data Management application.
Tapes/Media/Cartridges	Tapes are represented as files and are units within the VTL where data is actually written. Tapes are loaded into a Tape Drive before being accessed.
Slots	Tapes are parked in Slots before they are retrieved by the data management application for access.

Supported Virtual Tape Library Access Protocols

The DR Series system supports the following virtual tape library (VTL) tape access protocols.

- Network Data Management Protocol (NDMP)
- Internet Small Computer System Interface (iSCSI)

NDMP

The Network Data Management protocol (NDMP) is used to control data backup and recovery between primary and secondary storage in a network environment. For example, a NAS server (Filer) can talk to a tape drive for the purposes of a backup.

You can use the protocol with a centralized data management application (DMA) to back up data on file servers running on different platforms to tape drives or tape libraries located elsewhere within the network. The protocol separates the data path from the control path and minimizes demands on network resources. With NDMP, a network file server can communicate directly to a network-attached tape drive or virtual tape library (VTL) for backup or recovery.

The DR Series system VTL container type is designed to work seamlessly with the NDMP protocol.

iSCSI

iSCSI or **Internet Small Computer System Interface** is an Internet Protocol (IP)-based storage networking standard for storage subsystems. It is a carrier protocol for SCSI. SCSI commands are sent over IP networks by using iSCSI. It also facilitates data transfers over intranets and to manage storage over long distances. iSCSI can be used to transmit data over LANs or WANs.

In iSCSI, clients are called *initiators* and SCSI storage devices are *targets*. The protocol allows an *initiator* to send SCSI commands (*CDBs*) to the *targets* on remote servers. It is a storage area network (SAN) protocol, allowing organizations to consolidate storage into data center storage arrays while providing hosts (such as database and web servers) with the illusion of locally attached disks. Unlike traditional Fibre Channel, which requires different cabling, iSCSI can be run over long distances using existing network infrastructure.

iSCSI is a low-cost alternative to Fibre Channel, which requires dedicated infrastructure except in FCoE (Fibre Channel over Ethernet). Note that the performance of an iSCSI SAN deployment can be degraded if not operated on a dedicated network or subnet

The VTL container type is designed to work seamlessly with the iSCSI protocol. For details, see the topic, Creating Storage Containers.

VTL and DR Series Specifications

This topic describes key specifications of VTL support in the DR Series system.

- **Supported VTL Types** — The DR4X00 and DR6000 Series systems support two types of virtual tape libraries.
  - Standard emulation of StorageTek L700 library
  - Dell OEM version of the StorageTek L700 library

    NOTE: The Dell OEM type VTL is supported only with Symantec Backup Exec and Netbackup data management applications (DMAs).

    NOTE: Refer to the documentation for your specific DR Series system, which includes DMA best practices whitepapers and the latest *Dell DR Series Interoperability Guide*, for a complete list of the supported DMAs. Visit the following site and select your specific DR Series system to download documentation: http://www.dell.com/powervaultmanuals.
- **Use of VTL with Virtual DR Series system (DR2000v)** — The use of VTL is not supported on the DR2000v.
- **Number of Tape Drives** — Each tape library contains 10 tape drives of the type IBM-LTO-4 ('ULT3580-TD4')
- **Tapes or Media Sizes**— Each library initially is created with 10 slots housing 10 tape media of the default size of 800GiB, which is the equivalent of an LTO4 tape.

  You can add additional tapes to the library as needed by editing the container in the GUI or by using the following CLI command:

  ```
  vtl --update_carts --name <name> --add --no_of_tapes <number>
  ```

NOTE: For more information about using the CLI, see the *Dell DR Series CLI Reference Guide*.

A library can only contain tapes of the same size. For example, if the library is originally created with 10 tapes of size 10GiB, additional tapes of size 10GiB can only be added.

Tapes of the following capacity are supported:

Tape	Size	Max number of slots supported
LTO-4	800GiB	2000
LTO-4	400GiB	4000
LTO-4	200GiB	8000
LTO-4	100GiB	10000
LTO-4	50GiB	10000
LTO-4	10GiB	10000

- **Maximum Number of DMAs or Initiators Supported** — A tape library can be accessed by one DMA or iSCSI initiator at a time.
- **Replication** — Replication of VTL containers is currently not supported; however, it is planned for a future release of the DR Series system.

Guidelines for Configuring VTL

The overall steps and recommended guidelines for using and configuring a virtual tape library (VLT) with the DR Series system are described below.

Plan your Environment

Determine the following before creating a container of type VTL.

- Identify the Data Management Application (DMA) that you will be using to back up data. Refer to the *Dell DR Series System Interoperability Guide* for a complete list of the supported DMAs.
- For the NDMP protocol, determine the filer that will be backed up using NDMP Refer to the *Dell DR Series System Interoperability Guide* for a list of the supported Filers and Operating systems.
- For the iSCSI protocol, determine the iSCSI initiator's properties – This is the DMA IP, hostname or IQN of the software initiator on the operating system.
- Assess the estimated size of full and incremental backups and retention periods.

  NOTE: The size of the full and incremental backups will determine the tape capacity size that you set. You should use a larger tape size for full backups and a smaller size for incremental backups that have smaller retention periods. Note that faster expiration periods of incremental backups residing on smaller tapes results in the release of space back to the system for future backups.

Create Containers of Type VTL.

- Determine the VTL library type (NDMP or iSCSI) that you should be using as per the suggested type in the best practices guide of your preferred DMA.

  Refer to the DR Series system documentation, which includes best practices whitepapers for the supported DMAs, for your specific DR Series system at:

  http://www.dell.com/powervaultmanuals
- When creating the container in the GUI or by using the CLI, you will need to set the connection type of either NDMP or iSCSI. You need to provide either the DMA IP/hostname for NDMP or the IP/hostname or IQN for an iSCSI connection type.

Refer to the topics, Creating Storage Containers and Creating a VTL Type Container, for detailed instructions about creating containers. Refer to the *Dell DR Series System Command Line Interface Guide* for details about the CLI commands for creating containers.

Authentication/User Management Considerations

- You can use the following commands to view user information and manage passwords for the iSCSI user: iscsi_user, and NDMP user: ndmp_user.

  - `iscsi --show`
  - `ndmp --show`
  - `iscsi --setpassword`
  - `ndmp --setpassword`

  Refer to the *Dell DR Series System Command Line Reference Guide* for more details about using these commands.
- For iSCSI, you need to configure the system-wide CHAP account for the DR Series system. After creating an iSCSI VTL container, you need to set the CHAP password for the system-wide CHAP account by using the CLI. Or, you can set the password on the Clients Page > iSCSI tab. See the topic, Clients Page (Using the iSCSI Tab), for more information about setting the CHAP password in the GUI.
- For NDMP, you can set the password for ndmp_user by using the CLI or from the clients Page (Using NDMP Tab). These credentials are needed for configuring the NDMP-VTL in the DMA.

Verify the Tape Library Creation

You can easily check that the library has been created and is available for use by using the following commands.

- Check the container properties by executing the following command:
  `container --show –verbose`

  - Upon initial addition of the connection, the NDMP/iSCSI connection status shows as 'Added". At this time, the library is not officially created.
  - After a few minutes, the NDMP/iSCSI connection status changes to "Available" . This status indicates that the library is online, and the tape drives and media is available for usage.
- To check the status of the virtual tape library and all the tapes in the library, you can execute one of the following commands:

  - `vtl –show`
  - `vtl --show --name <container_name> --verbose`

Configure the Library in the DMA

See the DR Series system documentation, which includes DMA best practices whitepapers for your specific DR Series system at:

http://www.dell.com/powervaultmanuals

13

Configuring and Using Encryption at Rest

This chapter introduces the concept of Encryption at Rest as used by the DR Series system as well as related concepts and tasks.

Refer to the subsequent topics for more information.

Understanding Encryption at Rest

Data that resides in the DR Series system can be encrypted. When encryption is enabled, the DR Series system uses the Industry standard FIPS 140-2 compliant 256-bit Advanced Encryption Standard (AES) encryption algorithm for encrypting and decrypting user data. The content encryption key is managed by the key manager, which operates in either a Static mode or an Internal mode. In Static mode, a global, fixed key is used to encrypt all data. In internal mode, key lifecycle management is performed in which the keys are periodically rotated. The minimum key rotation period before the content encryption key can be rotated and a new key is generated is 7 days. This rotation period is user-configurable and can be specified in days. A user-defined passphrase is used to generate a pass phrase key, which is used to encrypt the content encryption keys. It is mandatory to define a passphrase to enable encryption. The system supports up to a limit of 1023 different content encryption keys. All streams of a data-store are encrypted or re-encrypted with the same content encryption key. DR Series system statistics report the amount of data encrypted and decrypted bytes consistently.

Encryption at Rest Terminology

This topic introduces and briefly defines some basic encryption at rest terminology used in the DR Series system documentation.

Term	Description
Passphrase	A passphrase is a sequence of words or other text used to control access to data, similar to a password in usage, but is generally longer for added security. In the DR Series system, the passphrase is user-defined and is used to generate a passphrase key that encrypts the file in which the content encryption keys are kept. The passphrase is a human readable key, which can be up to 256 bytes in length. It is mandatory to define a passphrase to enable encryption.
Content encryption key	The key used to encrypt the data. The content encryption key is managed by the key manager, which operates in either a static mode or an internal mode. The system supports up to a limit of 1023 different content encryption keys.
Key management mode	The mode of key lifecycle management as either static or internal.
Static mode	A global mode of key management in which a fixed key is used to encrypt all data.
Internal mode	A mode of key lifecycle management in which the keys are periodically generated and rotated. The minimum key rotation period before the content encryption key can be rotated and a new key is generated is 7

Term	Description
	days. This rotation period is user-configurable and can be specified in days.

Encryption at Rest and DR Series Considerations

This topic describes key features and considerations of using Encryption at Rest in the DR Series system.

- Key Management — In internal mode there is a maximum limit of 1023 keys. By default when encryption is enabled on the system, the key rotation period is set to 30 days. Users can later change the key rotation period from 7 days to 70 years, while configuring internal mode of encryption.
- Performance Impacts — Encryption should have minimal to zero impact on both backup and restore workflows. It should also have no impact on the replication workflows.
- Replication — Encryption must be enabled on both the source and target DR Series systems to store encrypted data on the systems. This means that encrypted data on the source does not automatically imply that when it is replicated to the target it will be encrypted unless encryption is explicitly turned 'ON' on the target DR Series system.
- Seeding — Encryption must be enabled on both the source and target DR Series systems to store encrypted data on the systems. If seeding is configured for encryption, then the data will be re-encrypted and stored. When the data stream is imported onto the target from the seed device, the stream will be encrypted as per the target policy and stored.
- Security Considerations for Passphrase and Key Management —
  - A passphrase is very important part of the encryption process on the DR Series system as the passphrase is used to encrypt the content encryption key or keys. If the passphrase is compromised or lost, the administrator should change it immediately so that the content encryption keys do not become vulnerable.
  - The administrator should closely consider security requirements to drive the decision for selecting the mode of key management for the DR Series system.
  - The Internal mode is more secure than the Static mode since the keys are periodically changed. Key rotation can be set to 7 days minimum.
  - Key modes can be changed at any time during the lifetime of the DR Series system; however, changing the key mode is a significant operation to undertake as all encrypted data must be re-encrypted.
  - Content encryption keys are stored in their encrypted form in a primary keystore, which is maintained on the same enclosure as the data-stores. For redundancy purposes, a backup copy of the primary keystore is stored on the system in the root partition, separate from the data-store partitions.

Understanding the Encryption Process

The overall steps for how Encryption at Rest is enabled and used in the DR Series system are described below.

1. Setting a passphrase.

   Encryption is disabled by default on a factory installed DR Series system (running version 3.2 software or later) or a DR Series system that has been upgraded to version 3.2 from a previously released version.

   The administrator must set a passphrase as the first step in configuring encryption. This passphrase is used to encrypt the content encryption keys, which adds a second layer of security to the key management.
2. Enabling encryption and setting the mode.

   The administrator should enable encryption by using the GUI or CLI. At this time, the mode is also set. The default key management mode is “internal” mode, in which key rotation happens periodically as specified by the set key rotation period.

3. **Encryption process.**

   After encryption is enabled, the data on the DR Series system that gets backed up is encrypted and is kept encrypted until it is expired and cleaned by the system cleaner. Note that the encryption process is irreversible.

4. **Encryption of pre-existing data**. Any pre-existing data on a DR Series system will also be encrypted using the currently set mode of key management. This encryption occurs as part of the system cleaner process. Encryption is scheduled as the last action item in the cleaner workflow. You must launch the cleaner manually using the maintenance command to reclaim space. It then encrypts all pre-existing unencrypted data. The cleaner can also be scheduled as per the existing pre-defined cleaner schedule.

   NOTE: The cleaner can take some time to start the encryption process if the system is nearing full system capacity. Encryption starts only after the cleaner processes data slated for cleaning and the related logs. This ensures that space reclamation is prioritized when free space is low and also ensures that data stores are not redundantly encrypted.

Refer to the *Dell DR Series System Command Line Reference Guide* for information about the CLI commands used for encryption.

14

Troubleshooting and Maintenance

This topic provides an overview of the basic troubleshooting and maintenance information that is available to help you better understand the current state of your DR Series system. The following list of information sources can aid you in understanding the current state of and maintaining your system:

- System alert and system event messages, for more information, see DR Series System Alert and Event Messages, which provides a tables that list the system alerts and system events.
- Diagnostics service, for more information, see About the Diagnostics Service.
- Maintenance mode, for more information, see About the DR Series Maintenance Mode.
- Scheduling system operations, for more information, see Scheduling DR Series System Operations.
- Scheduling Replication operations, for more information, see Creating a Replication Schedule.
- Scheduling Cleaner operations, for more information, see Creating a Cleaner Schedule.

Troubleshooting Error Conditions

To troubleshoot error conditions that disrupt your normal DR Series system operations, complete the following:

1. Generate a DR Series system diagnostics log file bundle if one has not already been automatically created.

   For more information, see Generating a Diagnostics Log File.
2. Check the system alert and system event messages to determine the current status of your DR Series system.

   For more information, see DR Series System Alert and Event Messages, Monitoring System Alerts, and Monitoring System Events.
3. Verify if the DR Series system has recovered or whether it has entered into Maintenance mode.

   For more information, see About the DR Series System Maintenance Mode.
4. If you cannot resolve the issue using the information in this DR Series system documentation, then read Before Contacting Dell Support, and seek assistance from Dell Support.

DR Series System Alert and Event Messages

The DR Series system provides a variety of system alert and system event message types that describe the current state of the system. You can review these messages, and see if there are any actions you can perform to resolve any reported issue.

Dell recommends that you refer to the material in this and other related topics:

- Before any attempt is made to troubleshoot your DR Series system.
- Before contacting Dell Support for technical assistance.

You may be able to resolve any basic issues using the information presented in the DR Series system documentation.

Some alert and event messages are purely informational, and provide general system status. Other alert and event messages display specific status or component information or suggest a specific task you can perform to resolve an issue or to verify that a condition exists.

There are still other alert and event messages that direct you to contact Dell Support for assistance, where Dell Support intervention may be required.

- Table 1 lists the DR Series System Alert Messages by system alert type: general system, system chassis, NVRAM, and PERC-specific alert messages that could be displayed during the course of backup and deduplication-related operations.
- Table 2 lists the DR Series System Event Messages by system event type (type 1 through 7): event messages that could be displayed during the course of backup, replication, deduplication, diagnostics, cleaner, DataCheck, maintenance, and OpenStorage Technology (OST) operations.

Table 4. DR Series System Alert Messages

Alert Message	Description/Meaning or Action
General System Alerts	
Filesystem scan requested.	System is switching to Maintenance mode. Filesystem has read-only access.
NVRAM not detected.	Ensure that the NVRAM card is seated properly.
NVRAM capacitor is disconnected.	Contact Dell Support for possible support assistance or intervention.
NVRAM capacitor has degraded.	Contact Dell Support for possible support assistance or intervention.
NVRAM solid-state drives (SSD) are disconnected.	Contact Dell Support for possible support assistance or intervention.
NVRAM has failed to backup or restore data during the last boot.	Contact Dell Support for possible support assistance or intervention.
NVRAM hardware failure.	Contact Dell Support for possible support assistance or intervention.
Data volume is not present. Check that all drives are installed and powered up.	Contact Dell Support for possible support assistance or intervention.
File server failed to start after multiple attempts.	Contact Dell Support for possible support assistance or intervention.
File server failed multiple times. Entering Maintenance mode.	Contact Dell Support for possible support assistance or intervention.
Insufficient disk space exists.	The filesystem is now read-only.
Unable to detect filesystem type on the Data volume.	Contact Dell Support for possible support assistance or intervention.
Unable to detect filesystem type on the Namespace volume.	Contact Dell Support for possible support assistance or intervention.
Filesystem scan discovered inconsistencies.	Please check the filesystem report, and perform the suggested action. Contact Dell Support for possible assistance or intervention.
Replication peer network disconnected.	Check access to remote site.

Alert Message	Description/Meaning or Action
NVRAM does not match the data volume.	If this is a newly replaced NVRAM, use the **maintenance --hardware --reinit_nvram** command to reinitialize the NVRAM. For more information, see the *Dell DR Series System Command Line Reference Guide*.
Storage usage is approaching the system capacity.	Clean up the filesystem. If issue persists, contact Dell Support for possible assistance or intervention.
Replication re-sync cannot proceed.	Namespace limit has reached its maximum.
Out of space on replication target.	Clean up the filesystem. If issue persists, contact Dell Support for possible assistance or intervention.
The filesystem has reached the maximum allowable limit for files and directories. Creating new files and directories will be denied.	Clean up the filesystem. If issue persists, contact Dell Support for possible assistance or intervention.
System Chassis Alerts	
Power Supply <*number*> detected a failure.	• Reconnect the power cable to the designated power supply unit if it is disconnected. • Ensure that there is input AC power at the power cable. • Use a different power cord. If this does not resolve the issue, replace the designated power supply.
Power Supply <*number*> is missing or has been removed.	• The power supply might not be making a proper connection. • Try reseating the power supply in the power supply slot. • Reconnect the power cable to the designated power supply unit if it is disconnected. • Ensure that there is input AC at the power cable. • Use a different power cord. If this does not resolve the issue, replace the designated power supply.
Power Supply <*number*> is unplugged.	• Reconnect the power cable to the designated power supply unit if it is disconnected. • Ensure that there is input AC power at the power cable. • Use a different power cord.
Fan <*number*> failed.	• Verify that the designated cooling fan is present and is installed correctly. • Verify that the designated cooling fan spins up and runs. If this does not resolve the issue, replace the designated cooling fan.

Alert Message	Description/Meaning or Action
Fan <*number*> is missing.	Attach or replace the designated missing cooling fan.
Abnormal network errors detected on Network Interface Controller <*number*>.	The Network Interface Controller errors could be caused by network congestion or by packet errors. • Check your network. If that does not resolve the problem, then replace the NIC. • If the NIC is embedded, the DR Series system appliance requires service.
Network Interface Controller is missing.	• Remove and reinsert the NIC. • If this does not resolve the problem, replace the NIC.
Network Interface Controller <*name*> is disconnected.	Connect it to a network and/or check your network switches or routers for any network connectivity issues.
Network Interface Controller <*name*> is disabled.	Enable the port on the designated NIC.
Network Interface Controller <*name*> driver is bad.	Upgrade the DR Series system appliance (in the **Software Upgrade** page, and click **Start Upgrade**).
CPU <*name*> failed.	Replace the designated failed processor.
CPU <*name*> is missing.	Reinsert or replace the designated missing processor.
DIMM <*name*> failed.	Replace the designated failed DIMM (Dual In-line Memory Module) device.
DIMM <*name*> is missing.	• Reinsert or replace the designated DIMM device. • The memory capacity of the storage appliance is below the minimum required for correct operation. • The storage appliance requires service.
Temperature probe <*name*> failed.	The storage appliance requires service.
Voltage probe <*name*> failed.	The storage appliance requires service.
Temperature probes have recorded temperatures in the failed range.	• Check the **Events** page in the DR Series system for specific temperature events and the location of the temperature probes. • Check the data center air conditioning, ventilation, and internal system cooling fans for any problems. • Ensure there is proper air flow through the storage appliance, and as needed, clean the cooling vents.
Voltage probes have recorded readings in the failed range.	• Check the **Events** page in the DR Series system for specific voltage events and the location of the voltage probes. • Check the power supplies. If there are no issues with the power supplies, have a service technician check the DR Series system appliance to see if it requires any servicing.
Storage Controller <*number*> failed.	Replace the RAID controller in the DR Series system.

Alert Message	Description/Meaning or Action
Storage Controller <*number*> is missing.	Reinsert or replace the RAID controller in the DR Series system.
Storage Controller <*number*> has an illegal configuration.	The expected number of virtual drives is <*number*>, and the actual number of virtual drives found was <*number*>. Run the Dell Restore Manager (RM) utility to repair the drive configuration mismatch. The expected number of enclosures is <*number*>, and the actual number of enclosures found was <*number*>. • Check the SAS cable connections between the storage controller and all its enclosures. • Check the power cable connections to the enclosure power supplies.
Physical disk <*number*> failed.	Replace the physical disk that failed.
Physical disk <*number*> is missing, removed, or it cannot be detected.	Reinsert or replace the physical disk.
Physical disk <*number*> predictive failure reported.	Replace the physical disk. **NOTE:** Even though the disk may not have failed yet, the recommended best practice is to replace the disk.
Physical disk <*number*> is an unsupported type.	This disk type is unsupported and cannot be used in this configuration. Replace the unsupported physical disk with a Dell-supported SAS physical disk.
Physical disk <*number*> has been manually set to offline with a configuration command.	Remove the physical disk and reinsert it (the drive is non-operational in this state).
Physical disk <*number*> is foreign.	This can occur when a storage controller has been replaced or all drives have been migrated from another system. In such cases, the foreign configuration should be imported. If this is seen on a single physical disk, the foreign configuration should be cleared. **NOTE:** This condition can also be seen when a drive is removed and reinserted while a rebuild is still in progress.
Virtual Disk <*number*> failed.	Replace any failed or missing physical disk(s) and run the Dell Restore Manager (RM) utility.
Virtual Disk <*number*> has an invalid layout.	Run the Dell Restore Manager (RM) utility to repair this installation.
<*device*> failed.	• Verify that the device is present, and then check that the cables are properly connected. For more information, see the *Dell DR Series System Owner's Manual* to verify the system cabling is correct. • Check the connection to the controller battery and the status of battery health.

Alert Message	Description/Meaning or Action
	- If none of these steps resolve the problem, replace the storage controller battery.
<*device*> is missing.	- Verify that the device is present, and then check that the cables are properly connected. For more information, see the *Dell DR Series System Owner's Manual* to verify the system cabling is correct. - Check the connection to the controller battery and the status of battery health. **NOTE:** A battery with a weak or depleted charge can cause this warning.
Storage <*device*> has failed.	Check cable connections between the storage controller and the enclosure or backplane.
Storage <*device*> is missing.	Perform the following: - Check SAS and power cable connections between the storage controller and the enclosure or backplane. - Check the external enclosure management modules (EMM) and PERC status LEDs.
NVRAM Alerts	
NVRAM PCI Controller failed.	Replace the NVRAM PCI Controller.
NVRAM PCI Controller is missing.	Reinsert or replace the NVRAM PCI Controller.
Super Capacitor on the NVRAM PCI Controller failed.	Replace the NVRAM PCI Controller.
Super Capacitor on the NVRAM PCI Controller is missing.	Replace the NVRAM PCI Controller.
Failed to check software compatibility.	Upgrade the DR Series system appliance (in the **Software Upgrade** page, click **Start Upgrade**).
The system software package is incompatible with the current software stack.	Upgrade the DR Series system appliance (in the **Software Upgrade** page, click **Start Upgrade**).
PERC Alerts	
The storage appliance failed to gather the system diagnostics.	- Resolve all issues in the DR Series system diagnostics log bundle. - Re-attempt to collect the diagnostics log bundle. - Contact Dell Support for assistance.
Storage Appliance Critical Error: BIOS System ID is incorrect for correct operation of this storage appliance.	- The DR Series system appliance requires service. - Contact Dell Support for assistance.
Seeding Alerts	
Seeding device became full.	Add a new seeding device to continue.
Seeding cannot contact the target device.	Check to make sure that the target device is available and write-enabled. Then, remove and re-add the target device.

Alert Message	Description/Meaning or Action
Seeding process complete.	Informational message. No user intervention is required.
System has reached space full condition, seeding will be stopped.	
Seeding failed to create Zero log entries.	Switch to maintenance mode to correct the issue.
Found corrupted stream on seeding device. This error will be rectified during replication re-sync done on this seed data.	Informational message. No user intervention is required.
Seeding device metadata info file missing, unable to import.	
Seeding device mount not accessible.	
Seeding export paused as the device contains data from another seeding job.	Cleanup the device and re-add to continue seeding.
Seeding encountered error.	
Unable to decrypt the Seeding data.	Check that the "password" and "encryption type" matches the Seeding export job.
System diagnostics partition is running low on space.	Copy out the old diagnostics bundles and delete for future auto diagnostics collection.
Appliance available storage level is below the set threshold.	Schedule filesystem cleaner or expire older backups.
Primary Keystore corruption detected.	Run filesystem scan with data verification check.

Table 5. DR Series System Event Messages

System Event Message	Description/Meaning or Action
System Event = Type 1	
System requires a Restore Manager (RM) recovery.	
System failed basic initialization.	
HTTP Service failed. Web services will be unavailable.	
HTTP Service started.	Informational message. No user intervention is required.
HTTP Service is available now.	Informational message. No user intervention is required.
Diagnostics collection service failed.	
Diagnostic collection service started.	Informational message. No user intervention is required.
Diagnostics collection service re-started.	Informational message. No user intervention is required.
Configuration Service started.	Informational message. No user intervention is required.
Configuration Service is not healthy.	
Configuration Service is healthy.	Informational message. No user intervention is required.
Configuration Service failed to start.	

System Event Message	Description/Meaning or Action
Unsupported RAID Configuration detected.	
No Fault Tolerant RAID configuration found.	
Data volume not present.	Check all drives are inserted and powered up.
Unable to detect filesystem type on data volume.	
Non certified disk drive detected. Disk needs to be pulled out for the system to become operational.	Disk needs to be pulled out for the system to become operational.
NVRAM devices not found.	Check card is seated properly.
Invalid/Unsupported Network Configuration detected.	Use CLI "network --restart" to re-configure network cards.
Some of the network cards are not part of the bond configuration.	
No IP address has been assigned to the system.	
No valid hostname has been assigned to the system.	Use "system --setname" to set hostname.
No valid system name found in configuration Database.	Use "maintenance --configuration --restore" to recover from backup configuration.
No valid system configuration file(s) found in configuration database.	Use "maintenance --configuration --restore" to restore from backup configuration.
Data volume filesystem is not yet initialized.	
Backup configuration file is missing.	Contact Dell Support.
Working configuration file is missing.	Use "maintenance --configuration --restore" to restore configuration from backup.
Working configuration file is corrupted.	Use "maintenance --configuration --restore" to restore configuration from backup.
NVRAM signature is missing.	If NVRAM device was replaced use "maintenance --hardware --reinit_nvram" to initialize NVRAM.
Windows Active Directory client module failed to start. Active Directory support will not be available.	
Windows Active Directory client module started.	Informational message. No user intervention is required.
Windows Server module started.	Informational message. No user intervention is required.
Windows Server module re-started.	Informational message. No user intervention is required.
Windows Server module is down. Windows client access will be disrupted.	
Windows Server module has been disabled because of multiple crashes.	
System initialization is required.	Informational message. No user intervention is required.
Filesystem server maintenance requested.	
Filesystem server re-started.	Informational message. No user intervention is required.

System Event Message	Description/Meaning or Action
Filesystem server started.	Informational message. No user intervention is required.
Filesystem server re-started, in Read-Only mode.	Informational message. No user intervention is required.
Filesystem server started, in Read-Only mode.	Informational message. No user intervention is required.
Filesystem server is not healthy. Client access will be interrupted.	
Filesystem scan triggered.	
Filesystem check re-started.	Informational message. No user intervention is required.
Filesystem check continued from previous boot.	Informational message. No user intervention is required.
Filesystem checker is not healthy, will be re-started.	
Filesystem checker terminated with unexpected error.	
Filesystem checker crashing multiple times, entering support mode.	Please contact Dell Support.
Diagnostics collection module failed to start.	Reboot the system to recover. If problem persists contact Dell Support.
Hardware Health Monitor module failed to start.	Reboot the system to recover. If problem persists contact Dell Support.
System is exiting Support Mode.	Informational message. No user intervention is required.
De-dupe engine dictionary is corrupted.	Use "maintenance --configuration --reinit_dictionary" to re-init.
Not enough memory to validate NVRAM contents.	System reboot is required.
Failed to complete basic system initialization.	
Unable to detect filesystem type on the Name Space Volume.	
Name Space Volume is not mounted.	
iSCSI server started.	Informational message. No user intervention is required.
iSCSI server re-started.	Informational message. No user intervention is required.
iSCSI server is not healthy.	
iSCSI server is crashing repeatedly.	Contact Dell Support.
NDMP tape server started.	Informational message. No user intervention is required.
NDMP tape server re-started.	Informational message. No user intervention is required.
NDMP tape server is not healthy.	
NDMP tape server has crashed repeatedly.	Contact Dell Support.
Virtual Tape Library daemons started successfully.	Informational message. No user intervention is required.
Virtual Tape Library daemons re-started successfully.	Informational message. No user intervention is required.
Virtual Tape Library daemons are not healthy.	

System Event Message	Description/Meaning or Action
Virtual Tape Library daemons have crashed repeatedly. All Virtual Tape functionality will not be available.	
Failed to process deleted files and containers.	Contact Dell Support.
Internal failure processing ingest log.	Contact Dell Support for assistance or intervention.
Hardware Health Monitor Database is corrupted.	Use "maintenance --hardware --restore_hw_db".
Unable to communicate with Hardware Health Monitor.	Informational message. No user intervention is required.
Unable to communicate with NVRAM device. Check hardware.	Verify that the NVRAM card is seated properly in the DR Series system appliance. Contact Dell Support for assistance or intervention.
Capacitor is disconnected from NVRAM. If problem persist after reboot, replace NVRAM card.	Contact Dell Support for assistance or intervention.
SSD is disconnected from NVRAM device. If problem persist after reboot, replace NVRAM card.	Contact Dell Support for assistance or intervention.
NVRAM capacitor is not charging. If problem persist after 5 minutes of power shutdown, replace NVRAM card.	Contact Dell Support for assistance or intervention.
NVRAM has failed to backup or restore data during the last boot.	Contact Dell Support for assistance or intervention.
NVRAM is not yet ready to accept write commands.	Wait for NVRAM to become ready.
NVRAM hardware has failed.	Contact Dell Support for assistance or intervention.
Filesystem server is crashing repeatedly. Entering Maintenance mode to run filesystem scan utility.	
System is not initialized.	Use "system --init" to initialize the system.
NVRAM does not match the data volume.	If this is a newly replaced NVRAM, use "maintenance --hardware --reinit_nvram" to initialize.
Software upgrade is in progress.	Informational message. No user intervention is required.
Upgrade did not complete.	Retry upgrade after rebooting the appliance.
Upgrade completed successfully. Reboot required.	Reboot the system.
Upgrade completed successfully. System coming online.	Informational message. No user intervention is required.
Unable to set Filesystem Scan Markers.	Reboot the system. If problem persist contact Dell Support.
Not enough space to run Filesystem Scan.	Please clean-up older diagnostics file(s) and reboot the system. On reboot, execute "maintenance --filesystem --start_scan" to start filesystem scan. If the file system scan fails with not enough space, please contact Dell Support.

System Event Message	Description/Meaning or Action
Filesystem server is crashing repeatedly in Maintenance Mode.	Please contact Dell Support.
One or more software package is incompatible, please upgrade the appliance to rectify the issue.	Please upgrade the system appliance to rectify the issue. Upgrade the DR Series system appliance (in the **Software Upgrade** page, click **Start Upgrade**).
NVRAM Controller detected a memory failure	
NVRAM Health check in progress, please wait for it to complete before using the system.	Informational message. No user intervention is required.
NVRAM Health check is required, system will perform a quick health check	Informational message. No user intervention is required.
Failed to start NVRAM Health check, please reboot the appliance to recover from this state	Reboot the system.
Appliance encountered O/S issues. Please reboot the appliance to recover from this condition.	Reboot the system.
High system memory usage detected, system performance will be sluggish.	
System memory usage has returned to an optimal level.	Informational message. No user intervention is required.
A high level of system process usage has been detected, if it persists, please collect system diagnostics.	Informational message. No user intervention is required.
System process usage has returned to an optimal level.	Informational message. No user intervention is required.
A high-temperature reading has been detected on the NVRAM PCI controller. System will operate only in a read-only mode. Please check system airflow.	Informational message. No user intervention is required.
A high-temperature reading has been detected on the NVRAM PCI controller. System will not become operational until the temperature reduces to an ambient value of 55 degrees Celsius (131 degrees Fahrenheit).	Informational message. No user intervention is required. If issue persists, contact Dell Support for assistance or intervention.
The next NVRAM capacitor health check is scheduled for <*variable*>.	Informational message. No user intervention is required.
Windows Active Directory client is unable to contact the Active Directory domain server.	Informational message. No user intervention is required.
Active Directory domain server connectivity is restored.	Informational message. No user intervention is required.
Storage enclosure <*variable*> is authorized.	Informational message. No user intervention is required.
Storage enclosure <*variable*> is de-commissioned.	Informational message. No user intervention is required.

System Event Message	Description/Meaning or Action
The system IP address has changed from <*variable*> to <*variable*>.	Informational message. No user intervention is required.
Refresh NHM Inventory	
One or more storage enclosure(s) are missing/offline.	Please check whether all required storage enclosure(s) are powered-up and connected to the appliance.
Data Volume has become in-accessible.	Contact Dell Support.
Data Volume has become read-only.	Contact Dell Support.
Namespace Volume has become in-accessible, please call Dell support.	Contact Dell Support.
Namespace Volume has become read-only.	Contact Dell Support.
Core Volume has become in-accessible.	Contact Dell Support.
Invalid storage appliance memory configuration.	
Storage Enclosure with Service Tag <*variable*> added successfully.	Informational message. No user intervention is required.
One of the storage enclosure has become offline.	Power-off the appliance, fix the connectivity issues and power-on the appliance.
Data Volume has become read-only.	Contact Dell Support.
Upgrade did not complete. Retry upgrade.	Retry to upgrade. If the problem persists, contact Dell Support.
Filesystem scan completed, restarting filesystem for normal operation.	Informational message. No user intervention is required.
Storage enclosure license(s) are missing.	If Restore Manager (RM) recovery was performed recently, please re-apply the license(s) and reboot.
BIOS System ID is incorrect for correct operation of this storage appliance. The storage appliance requires service.	
System clock has drifted more than 24 hours, from the last filesystem start.	Please check your clock settings and reboot.
This DR4x00 Virtual Machine usage time limit has expired.	Please contact your DR4x00 Sales representative to get the Hardware Version.
This DR4x00 Virtual Machine is for evaluation purpose only. Evaluation period ends on <*variable*>.	Informational message. No user intervention is required.
This DR4x00 Virtual Machine requires an evaluation license.	Please contact your DR4x00 Sales representative.
This DR4x00 Virtual Machine is designed to work only with 4 CPU(s) and 8GB of memory.	Informational message. No user intervention is required.
This DR2000v requires a license to operate.	Please install an evaluation license or register the DR2000v with a DR4000/DR4100/DR6000 series hardware appliance.

System Event Message	Description/Meaning or Action
This DR2000v is unable to contact the license server to validate the license usage.	Please rectify the connectivity issues and reboot the system.
This DR2000v Virtual appliance usage time limit has expired.	Contact your Dell DR Series Sales representative to get a permanent license.
This DR2000v Virtual appliance usage time limit will expire on <*variable*>.	Informational message. No user intervention is required.
System Asset Tag information has non-printable characters.	Please use the iDRAC interface console and fix the issue.
This DR2000v has been deleted at license server.	Register using the CLI command "virtual_machine --register" again.
Filesystem scan requested. Switching to Maintenance Mode. Filesystem has read-only access.	Informational message. No user intervention is required.
NVRAM not detected.	Ensure card is seated properly.
NVRAM capacitor is disconnected.	Contact Dell Support.
NVRAM capacitor has degraded.	Contact Dell Support.
NVRAM SSD is disconnected.	Contact Dell Support.
NVRAM has failed to backup/restore data during last boot.	Contact Dell Support.
NVRAM hardware failure.	Contact Dell Support.
Data volume is not present. Check that all drives are inserted and powered up.	Contact Dell Support for assistance or intervention.
Filesystem server failed to start after multiple attempts.	Contact Dell Support for assistance or intervention.
Filesystem server crashed multiple times. System is now entering Maintenance mode.	Contact Dell Support for assistance or intervention.
Insufficient disk space. Filesystem switched to read-only mode.	Informational message. No user intervention is required. If issue persists, contact Dell Support for assistance or intervention.
Unable to detect filesystem type on the Data Volume.	Contact Dell Support for assistance or intervention.
Unable to detect filesystem type on the Namespace Volume.	Contact Dell Support for assistance or intervention.
Filesystem scan discovered inconsistencies.	Please check report and take the recommended action. Contact Dell Support for assistance or intervention.
NVRAM does not match data volume.	If this is a newly replaced NVRAM device, use the CLI **maintenance --hardware --reinit_nvram** command. For more information, see the *Dell DR Series System Command Line Reference Guide*.
Storage usage is approaching the DR Series system capacity.	Informational message. No user intervention is required. If issue persists, contact Dell Support for assistance or intervention.

System Event Message	Description/Meaning or Action
Replication re-sync cannot proceed because the Namespace depth has reached its maximum.	Informational message. No user intervention is required. If issue persists, contact Dell Support for assistance or intervention.
Filesystem has reached the maximum allowable file(s) and directories limit. New file and directory creation will be denied until sufficient space exists.	Please clean up the filesystem. If issue persists, contact Dell Support for assistance or intervention.
Filesystem is reaching the maximum allowable file(s) and directories limit. New file and directory creation will be denied after the limit has been reached.	Please clean up the filesystem. If issue persists, contact Dell Support for assistance or intervention.
Replication has encountered an unexpected error.	Contact Dell Support for assistance or intervention.
DataCheck has detected a potential corruption.	Run data consistency checks at the first available opportunity. If this issue persists, contact Dell Support for assistance or intervention.
Datacheck detected potential namespace inconsistency.	Run filesystem scan as soon as possible. ("maintenance --filesystem --start_scan")
Datacheck detected inconsistency in lsu image.	Run filesystem scan as soon as possible. ("maintenance --filesystem --start_scan verify_rda_metadata")
Datacheck detected potential corrupt lsu info.	Run filesystem scan as soon as possible. ("maintenance --filesystem --start_scan verify_rda_metadata")
Temperature warning detected on NVRAM PCI controller.	Please check the data center air conditioning, rack ventilation, and internal cooling fans for any issues. Ensure that there is proper air flow through the system appliance, and clean the system cooling vents as needed. If issue persists, contact Dell Support for assistance or intervention.
Filesystem Name Space partition has reached its maximum allowable limit.	Please delete any old, unused file(s) or disable replication(s). If issue persists, contact Dell Support for assistance or intervention.
Filesystem Name Space partition is reaching its maximum allowable limit.	New replication resynch(s) will be stopped. If issue persists, contact Dell Support for assistance or intervention.
One or more software package is incompatible.	Please upgrade the appliance to rectify the issue.
Filesystem volume has become in-active.	Please contact Dell Support for assistance or intervention.
Filesystem server response time exceeded max threshold.	Informational message. No user intervention is required.
The memory capacity of the storage appliance is below the minimum required for correct operation. The storage appliance requires service.	
An OST container quota is exceeded.	Check the event for container details.
One of the storage enclosure has become offline.	Please power-down the appliance and rectify the issue.
One or more storage enclosure(s) are missing/offline.	Please check whether the storage enclosure(s) are powered-up and connected to the appliance.

System Event Message	Description/Meaning or Action
Storage enclosure license(s) are missing.	If Restore Manager (RM) recovery was performed recently, please re-apply the license(s) and reboot.
System has a huge backlog of book keeping work. Filesystem cleaner will be enabled outside of schedule setting and performance impact will be observed.	Informational message. No user intervention is required.
System clock has drifted more than 24 hours, from the last filesystem start.	Please check your clock settings and reboot.
Replication is disconnected on one or more containers.	Please check event log or replication stats for details.
One or more replication target systems are running low in space.	Please check event log or replication stats for details.
Filesystem scan completed with no inconsistencies. Switching back to operational mode.	Informational message. No user intervention is required.
Replication detected potential inconsistency.	Run filesystem scan with data verification check as soon as possible. ("maintenance --filesystem --start_scan verify_data")
Seeding device became full.	Add new seeding device to continue.
Seeding cannot contact the target device.	Check to make sure that the target device is available and write-enabled. Then remove and re-add the target device.
Seeding process complete.	Informational message. No user intervention is required.
System has reached space full condition, seeding will be stopped.	Informational message. No user intervention is required.
Seeding failed to create Zero log entries.	Switch to maintenance mode to correct the issue.
Found corrupted stream on seeding device. This error will be rectified during replication re-sync done on this seed data.	Informational message. No user intervention is required.
Seeding device metadata info file missing, unable to import.	
Seeding device mount not accessible.	
Seeding export paused as the device contains data from another seeding job.	Cleanup the device and re-add to continue seeding.
Seeding encountered error.	
Unable to decrypt the Seeding data.	Please check that the "password" and "encryption type" matches the Seeding export job.
System diagnostics partition is running low on space.	Please copy out the old diagnostics bundles and delete for future auto diagnostics collection.
Appliance available storage level is below the set threshold.	Please schedule filesystem cleaner or expire older backups.
Primary Keystore corruption detected.	Run filesystem scan with data verification check.

System Event Message	Description/Meaning or Action
System Event = Type 2	
Data check configuration successful.	Informational message. No user intervention is required.
Successfully <*variable*> system marker.	Informational message. No user intervention is required.
<*variable*> OPDUP encryption updated to <*variable*>	Informational message. No user intervention is required.
System storage usage alert has been set at <*level*>.	Informational message. No user intervention is required.
Successfully <*variable*> container <*variable*> with the following marker(s) "<*markers*>".	Informational message. No user intervention is required.
Container <*name*> created successfully.	Informational message. No user intervention is required.
Container <*name*> marked for deletion.	For more information, see Deleting Containers. Use the DR Series system CLI **maintenance --filesystem --reclaim_space** command to recover this storage space.
Container <*name*> has been deleted.	Informational message. No user intervention is required.
Successfully renamed container <*name*> as <*name*>.	Informational message. No user intervention is required.
Container <*name*> is configured to access over <*variable*> by the following clients: <*clients*> ('*' means access for everyone).	Informational message. No user intervention is required.
Container <*name*> is updated to access over <*variable*> by the following clients: <*clients*> ('*' means access for everyone).	Informational message. No user intervention is required.
Disabled access for Container <*name*> over <*variable*> for the following clients: <*clients*> ('*' means disabled access for everyone).	Informational message. No user intervention is required.
Successfully added connection entry for container <*name*>: type <*variable*> clients <*variable*>.	Informational message. No user intervention is required.
Successfully updated connection entry for container <*name*>: type <*variable*> clients <*variable*>.	Informational message. No user intervention is required.
Successfully deleted connection entry for container <*name*>: type <*variable*> clients <*variable*>.	Informational message. No user intervention is required.
Replication entry created successfully for container <*name*>: role <*variable*> peer <*variable*> peer container <*variable*>.	Informational message. No user intervention is required.
Replication configuration updated successfully for container <*name*>: role <*variable*> peer <*variable*>.	Informational message. No user intervention is required.
Replication marked for deletion for Container <*name*>: peer <*variable*> peer container <*name*>.	Informational message. No user intervention is required.
Replication deleted for container <*name*>.	Informational message. No user intervention is required.
Successfully initiated replication re-sync on Container <*name*>.	Informational message. No user intervention is required.

System Event Message	Description/Meaning or Action
Replication <*variable*> defaults successfully updated: role <*variable*> peer <*variable*>.	Informational message. No user intervention is required.
Successfully updated replication bandwidth limit for <*variable*> to <*variable*>.	Informational message. No user intervention is required.
Successfully removed replication bandwidth limit for <*variable*>.	Informational message. No user intervention is required.
Successfully set <*variable*> replication bandwidth limit.	Informational message. No user intervention is required.
Replication enabled for container <*name*> with role <*role*>.	Informational message. No user intervention is required.
Replication disabled for container <*name*> with role <*role*>.	Informational message. No user intervention is required.
Snapshot <*variable*> → <*variable*> created successfully.	Informational message. No user intervention is required.
Snapshot <*variable*> → <*variable*> successfully updated.	Informational message. No user intervention is required.
Snapshot <*variable*> → <*variable*> successfully deleted.	Informational message. No user intervention is required.
Client <*client*> authorized to access NDMP Tape Server.	Informational message. No user intervention is required.
Successfully updated NDMP to use port <*number*>.	Informational message. No user intervention is required.
De-authorized NDMP client - <*client*>.	Informational message. No user intervention is required.
NDMP password successfully updated.	Informational message. No user intervention is required.
OST password updated successfully.	Informational message. No user intervention is required.
OST state updated successfully.	Informational message. No user intervention is required.
OST client <*variable*> with mode <*variable*> added successfully	Informational message. No user intervention is required.
OST client <*variable*> deleted successfully.	Informational message. No user intervention is required.
OST client <*variable*> with mode <*variable*> updated successfully.	Informational message. No user intervention is required.
OST client <*variable*> deleted successfully.	Informational message. No user intervention is required.
OST client <*variable*> with mode <*variable*> updated successfully.	Informational message. No user intervention is required.
Successfully updated <*variable*> schedule.	Informational message. No user intervention is required.
System compression level set to <*variable*>.	Informational message. No user intervention is required.
System configuration backup failed.	

System Event Message	Description/Meaning or Action
Rapid Data Access (RDA) password updated successfully.	Informational message. No user intervention is required.
Rapid Data Access (RDA) state updated successfully.	Informational message. No user intervention is required.
Rapid Data Access (RDA) client <*variable*> with mode <*variable*> added successfully.	Informational message. No user intervention is required.
Rapid Data Access (RDA) client <*variable*> deleted successfully.	Informational message. No user intervention is required.
Rapid Data Access (RDA) client <*variable*> with mode <*variable*> updated successfully.	Informational message. No user intervention is required.
DR2000v with UUID <*variable*> IP Address <*variable*> Hostname <*variable*> registered successfully.	Informational message. No user intervention is required.
DR2000v with UUID <*variable*> IP Address <*variable*> Hostname <*variable*> unregistered successfully.	Informational message. No user intervention is required.
System Event = Type 3	
System is entering Maintenance mode.	Informational message. No user intervention is required. Contact Dell Support for assistance or intervention.
System entering Support Mode.	Contact Dell Support for assistance or intervention.
Internal failure—OFS client initialization failure.	Contact Dell Support for assistance or intervention.
Internal failure—mtab initialization failure for container if <*variable*>.	Contact Dell Support for assistance or intervention.
Internal failure—cannot initialize node mtab.	Contact Dell Support for assistance or intervention.
Internal failure retrieving configuration for container ID <*variable*>.	Contact Dell Support for assistance or intervention.
Internal failure deleting container ID <*variable*>.	Contact Dell Support for assistance or intervention.
Internal failure stopping container ID <*variable*>.	Contact Dell Support for assistance or intervention.
Internal failure adding connection <*variable*> for container ID <*variable*>.	Contact Dell Support for assistance or intervention.
Internal failure deleting connection <*variable*> for container ID <*variable*>.	Contact Dell Support for assistance or intervention.
Name space volume nearing low space condition. To prevent faster exhaustion of space, snapshot required for replication seeding for container <*variable*> will be paused until Name space volume recovers from low space conditions.	
Replication started as per schedule, will be active until <*variable*>.	Informational message. No user intervention is required.
Replication stopped as per schedule, will restart at <*variable*>.	Informational message. No user intervention is required.

System Event Message	Description/Meaning or Action
Container replay failed for container <*variable*>.	Informational message. No user intervention is required. Contact Dell Support for assistance or intervention.
Internal failure—Name Space subsystem initialization failed.	Informational message. No user intervention is required. Contact Dell Support for assistance or intervention.
Inconsistencies were found in the Name Space.	Please schedule a filesystem consistency check using the DR Series system CLI **maintenance --filesystem --start_scan** command.
System entering Maintenance mode—Name Space log replay failed.	Contact Dell Support for assistance or intervention.
System entering Maintenance Mode—Name Space transaction failure.	Contact Dell Support for assistance or intervention.
Internal failure—failed to commit Name Space transaction.	Contact Dell Support for assistance or intervention.
Filesystem has reached the maximum supported number of Name Space entries.	Please clean up the filesystem to allow new file and directory create operations. If this condition persists, contact Dell Support for assistance or intervention.
Filesystem has recovered from a lack of available Name Space entries.	Filesystem create operations will now be allowed. Contact Dell Support for assistance or intervention.
Internal attributes of some files were found to be corrupt. The DR Series system will not allow the setting or removing of Attributes or ACLs on files that have corrupt attributes.	To find all files with corrupt attributes and to clear the state, please perform a maintenance scan using the DR Series system CLI **maintenance --filesystem --start_scan** command. Contact Dell Support for assistance or intervention.
System entering maintenance mode - Name Space Log Rotation failed	
File/Directory Statistics table out of sync. Switching to maintenance mode.	
Root inode of container, id <*variable*>, was found to be inconsistent. Fixed the attribute, ACL on root inode needs to be manually verified and fixed.	
Replication re-sync started for container <*variable*>.	Informational message. No user intervention is required.
Replication internal re-sync started for container <*variable*>.	Informational message. No user intervention is required.
Replication re-sync completed for container <*variable*>.	Informational message. No user intervention is required.
Replication internal re-sync completed for container <*variable*>.	Informational message. No user intervention is required.
Internal failure creating replication snapshot for container <*variable*>.	If condition persists, reduce number of inodes, or contact Dell Support for assistance or intervention.
Internal failure deleting replication snapshot for container <*variable*>.	If condition persists, reduce number of inodes, or contact Dell Support for assistance or intervention.

System Event Message	Description/Meaning or Action
Replication client connected for container <*variable*>.	Informational message. No user intervention is required.
Replication client disconnected for container <*variable*>.	Verify that the ports for replication (9904, 9911, 9915, and 9916) and OST (10011 and 11000) operations have been enabled. If issue persists, contact Dell Support for assistance or intervention.
Replication server connected for container <*variable*>.	Verify that the ports for replication (9904, 9911, 9915, and 9916) and OST (10011 and 11000) operations have been enabled. If issue persists, contact Dell Support for assistance or intervention.
Replication server disconnected for container <*variable*>.	Informational message. No user intervention is required.
Replication Name Space oplog full for container <*variable*>.	Verify that the ports for replication (9904, 9911, 9915, and 9916) and OST (10011 and 11000) operations have been enabled. If issue persists, contact Dell Support for assistance or intervention.
Replication switching to re-sync due to corrupt replication Name Space oplog for container <*variable*>.	
Replication data operations log (oplog) full for container <*variable*>.	The DR Series system should self-correct itself. If condition persists, reduce number of inodes, or contact Dell Support for assistance or intervention.
Replication switching to re-sync due to corrupt replication data oplog for container <*variable*>.	
Replication transmit log (txlog) full for container <*variable*>.	The DR Series system should self-correct itself. If condition persists, reduce number of inodes, or contact Dell Support for assistance or intervention.
System entering Maintenance mode due to corrupt replication txlog for container <*variable*>.	Collect a diagnostics log file, and open a Support record with Dell Support for assistance.
System entering Maintenance mode due to replication txlog commit error <*variable*> for container <*variable*>.	Collect a diagnostics log file, and open a Support record with Dell Support for assistance.
Unable to make progress on filesystem replication for container <*variable*>.	Collect a diagnostics log file, and open a Support record with Dell Support for assistance.
Replication syncmgr exited for container <*variable*> error <*variable*>.	Collect a diagnostics log file bundle, and open a Support record with Dell Support for assistance.
Replication syncmgr event for container <*variable*> error <*variable*>.	Collect a diagnostics log file bundle, and open a Support record with Dell Support for assistance.
Name Space replicator exited for container <*variable*> error <*variable*>.	Collect a diagnostics log file bundle, and open a Support record with Dell Support for assistance.
Replication data replicator exited for container <*variable*> error <*variable*>.	Collect a diagnostics log file bundle, and open a Support record with Dell Support for assistance.

System Event Message	Description/Meaning or Action
Replication protocol version mismatch for container <*variable*> error <*variable*>.	Collect a diagnostics log file bundle, and open a Support record with Dell Support for assistance.
Replication protocol version mismatch detected for container <*variable*>. Replication will continue with downgraded source protocol version.	
Replication delete cleanup failed for container <*variable*> error <*variable*>.	Collect a diagnostics log file bundle, and open a Support record with Dell Support for assistance.
Replication target system <*variable*> is running low on space. Replication cannot proceed further on container <*variable*>.	Informational message. Contact Dell Support for assistance or intervention.
Replication misconfiguration detected for container <*variable*>. Replication relationship might have been deleted forcibly on target system <*variable*>.	Informational message. Contact Dell Support for assistance or intervention.
Replication failed for container <*variable*> error <*variable*>.	Collect a diagnostics log file bundle, and open a Support record with Dell Support for assistance.
Replication server failed to commit blockmap for container <*variable*>. System is entering Maintenance mode.	The DR Series system should self-correct itself. If condition persists, reduce number of inodes, or contact Dell Support for assistance or intervention.
Container <*variable*> replication is paused, cleaner on replica is reclaiming space.	Run the Cleaner on the replica container. If condition persists, contact Dell Support for intervention or assistance.
Found mismatch in system software version with peer <*variable*>. Replication on source container <*variable*> would be stalled.	
Replication stalled on source container <*variable*> due to a mismatch in system software version or network issue with peer <*variable*>.	
Found mismatch in system software version with peer <*variable*>. Backup or replication on some or all target containers would be stalled.	
Received a garbled message from peer <*variable*>. Connection would be dropped.	
Container <*variable*> replication encountered encryption setup error.	
NFS client successfully mounted <*variable*>.	Informational message. No user intervention is required.
Maximum NFS connection limit <*variable*> reached, active NFS connections <*variable*>.	You have reached the threshold limit. Reduce the number of connections.
NFS client <*variable*> successfully unmounted <*variable*>.	Informational message. No user intervention is required.
NFS client <*variable*> successfully unmounted all containers.	Informational message. No user intervention is required.

System Event Message	Description/Meaning or Action
CIFS client successfully connected to container <*variable*>.	Informational message. No user intervention is required.
CIFS client <*variable*> session successfully disconnected from container <*variable*> .	Informational message. No user intervention is required.
Maximum CIFS connection limit <*variable*> reached.	You have reached the threshold limit. Reduce the number of connections.
CIFS server failed to start <*variable*>.	Reboot the DR Series system. If issue persists, contact Dell Support for assistance or intervention.
CIFS client connected <*variable*> times to container <*variable*>.	Reboot the DR Series system. If issue persists, contact Dell Support for assistance or intervention.
CIFS server started successfully.	Informational message. No user intervention is required.
NFS server started successfully.	Informational message. No user intervention is required.
Storage usage approaching system capacity.	Informational message. No user intervention is required.
Online data verification (DataCheck) started.	Informational message. If issue persists, contact Dell Support for assistance or intervention.
Online data verification (DataCheck) suspended.	Informational message. If issue persists, contact Dell Support for assistance or intervention.
Online data verification (DataCheck) stopped.	Informational message. If issue persists, contact Dell Support for assistance or intervention.
Online data verification (DataCheck) resumed.	Informational message. If issue persists, contact Dell Support for assistance or intervention.
Online data verification (DataCheck) detected <*variable*> corruption.	Informational message. If issue persists, contact Dell Support for assistance or intervention.
Online data verification (DataCheck) detected <*variable*> corruptions.	Informational message. If issue persists, contact Dell Support for assistance or intervention.
Online data verification (DataCheck) failed to start.	Informational message. If issue persists, contact Dell Support for assistance or intervention.
Seeding device became full.	Add new seeding device to continue.
Seeding cannot contact the target device.	Check to make sure that the target device is available and write-enabled. Then remove and re-add the target device.
Seeding process complete.	Informational message. No user intervention is required.
System has reached space full condition, seeding will be stopped.	
Seeding failed to create Zero log entries.	Switch to maintenance mode to correct the issue.
Found corrupted stream on seeding device. This error will be rectified during replication re-sync done on this seed data.	Informational message. No user intervention is required.

System Event Message	Description/Meaning or Action
Seeding device metadata info file missing, unable to import.	
Seeding device mount not accessible.	
Seeding export paused as the device contains data from another seeding job.	Clean up the device and re-add to continue seeding.
Seeding encountered error.	
Unable to decrypt the Seeding data.	Please check that the "password" and "encryption type" matches the Seeding export job.
Seeding device deleted.	Informational message. No user intervention is required.
Seeding device added.	Informational message. No user intervention is required.
Seeding started.	Informational message. No user intervention is required.
Seeding stopped.	Informational message. No user intervention is required.
Container <*variable*> added to seeding.	Informational message. No user intervention is required.
Container <*variable*> is removed while seeding is in progress.	Informational message. No user intervention is required.
Container <*variable*> removed from seeding.	Informational message. No user intervention is required.
Seeding job created.	Informational message. No user intervention is required.
Seeding job deleted.	Informational message. No user intervention is required.
Seed space reclamation triggered.	Informational message. No user intervention is required.
Unable to use old seed dict. Creating a new dict.	Informational message. No user intervention is required.
Unable to read bmap scid. Retry seeding after running filesystem scan.	Retry seeding after running filesystem scan.
Unable to read DS scid. Retry seeding after running filesystem scan.	Retry seeding after running filesystem scan.
Seeding device mount not accessible. Check the CIFS mount and re-add the device to continue.	Check the CIFS mount and re-add the device to continue.
System Event = Type 4	
Internal Error. Unable to load deduplication dictionary <*variable*>.	Use the DR Series system CLI **maintenance --configuration --reinit_dictionary** command. If this issue persists, contact Dell Support for assistance or intervention.
Internal Error. Unable to locate deduplication dictionary <*variable*>.	Use the DR Series system CLI **maintenance --configuration --reinit_dictionary** command. If issue persists, contact Dell Support for assistance or intervention.
Filesystem cleaner run <*variable*> started.	Informational message. No user intervention is required.
Filesystem cleaner run <*variable*> completed in <*variable*> milliseconds (ms).	Informational message. No user intervention is required.

System Event Message	Description/Meaning or Action
Filesystem cleaner process encountered input/output (I/O) errors.	Maintenance-based issue with the DR Series system. Check status using Maintenance mode or DR Series system CLI commands. Contact Dell Support as needed.
Failure to sync NVRAM <*variable*>.	NVRAM hardware issue with the DR Series system. Check status using Maintenance mode or DR Series system CLI commands.
Failure reading from NVRAM <*variable*>.	NVRAM hardware issue with the DR Series system. Check status using Maintenance mode or DR Series system CLI commands.
Failure writing to NVRAM <*variable*>.	NVRAM hardware issue with the DR Series system. Check status using Maintenance mode or DR Series system CLI commands.
Failure to write sync NVRAM <*variable*>.	NVRAM hardware issue with the DR Series system. Check status using Maintenance mode or DR Series system CLI commands.
Internal Error. Datastore <*variable*> length mismatch <*variable*>.	Maintenance-based issue with the DR Series system. Check status using Maintenance mode or DR Series system CLI commands. Contact Dell Support as needed.
Data volume capacity threshold reached.	Informational message. No user intervention is required.
Out of space. Rollback of updates on object <*variable*> failed. Restarting file server.	Maintenance-based issue with the DR Series system. Check status using Maintenance mode or DR Series system CLI commands. Contact Dell Support as needed.
Failure reading from data volume.	Maintenance-based issue with the DR Series system. Check status using Maintenance mode or DR Series system CLI commands. Contact Dell Support as needed.
Failure writing to data volume.	Maintenance-based issue with the DR Series system. Check status using Maintenance mode or DR Series system CLI commands. Contact Dell Support as needed.
Checksum verification on metadata failed.	Contact Dell Support for assistance or repair the filesystem. For repairs, see About The DR Series Maintenance Mode.
Internal Error. Optimization engine log replay failed.	Contact Dell Support for assistance or repair the filesystem. For repairs, see About The DR Series Maintenance Mode.
Decompression of datastore failed <*variable*>.	Contact Dell Support for assistance or intervention.
Internal Error. Failed to clean active datastore <*variable*>.	Contact Dell Support for assistance or intervention.
Internal Error. Negative reference on datastore <*variable*>. Record type: <*variable*>. Count: <*variable*>.	Contact Dell Support for assistance or repair the filesystem. For repairs, see About the DR Series Maintenance Mode.
Internal Error. Data store <*variable*> contains negative stream reference count. Record type: <*variable*>. Count: <*variable*>.	Informational message. No user intervention is required.

System Event Message	Description/Meaning or Action
Internal Error. Data store <*variable*> total reference count reached threshold. Record type: <*variable*>. Count: <*variable*>.	Informational message. No user intervention is required.
Internal Error. Entering Maintenance mode due to failure in processing logs.	Contact Dell Support for assistance or intervention.
Internal Error. Failed to acquire optimizer pipeline. Error: <*variable*>.	Contact Dell Support for intervention or assistance.
Internal Error. Failed to create optimizer event. Type: <*variable*>, Error: <*variable*>.	Contact Dell Support for intervention or assistance.
Internal Error. Task execution in fiber <*variable*> timed out after <*variable*> milliseconds (ms). Restarting file server.	Filesystem restarted. Collect diagnostics log file bundle, and upload diagnostics log file bundle to Dell Support.
Internal Error. Memory allocation failure.	Collect diagnostics log file bundle.
Background compression started.	Informational message. No user intervention is required.
Background compression completed.	Informational message. No user intervention is required.
Optimization initialized on container <*variable*>.	Informational message. No user intervention is required.
Optimization terminated on container <*variable*>.	Informational message. No user intervention is required.
Cleaner aborted at <*variable*>.	The DR Series system should enter Maintenance mode, and Cleaner process will restart.
Internal Error. Moving data from NVRAM to disk failed. System is entering its Maintenance mode.	Informational message. No user intervention is required.
System entering Maintenance Mode due to corrupt encryption keystore. Triggering key import.	Run filesystem scan with verify data enabled
Key rotation successful in internal mode	Informational message. No user intervention is required.
Key limit reached, reusing the last key	Informational message. No user intervention is required.
Filesystem encryption setting changed	Informational message. No user intervention is required.
Filesystem Cleaner process started as per schedule (will be active until <*variable*>).	Informational message. No user intervention is required.
Filesystem Cleaner process stopped as per schedule (will restart at <*variable*>).	Informational message. No user intervention is required.
Filesystem cleaner is paused, to speed up disk maintenance (e.g. Rebuild / Background Init) activities.	Informational message. No user intervention is required.
System entering Support Mode due to keystore repair failure, both primary and backup keystore are corrupt	
System entering Support Mode due to keystore empty failure, both primary and backup keystore are empty or removed	

System Event = Type 5

System Event Message	Description/Meaning or Action
System shutdown initiated by administrator.	Informational message. No user intervention is required.
System reboot initiated by administrator.	Informational message. No user intervention is required.
Start system upgrade to version <*variable*>.	Informational message. No user intervention is required.
System name changed to <*variable*>.	Informational message. No user intervention is required.
System date changed to <*variable*>.	Informational message. No user intervention is required.
System time zone changed to <*variable*>.	Informational message. No user intervention is required.
Password changed for user: administrator.	Informational message. No user intervention is required.
NTP server <*variable*> added.	Informational message. No user intervention is required.
NTP server <*variable*> deleted.	Informational message. No user intervention is required.
NTP service enabled.	Informational message. No user intervention is required.
NTP service disabled.	Informational message. No user intervention is required.
User data destroyed using CLI command.	Informational message. No user intervention is required.
User <*variable*> enabled.	Informational message. No user intervention is required.
User <*variable*> disabled.	Informational message. No user intervention is required.
Networking interfaces restarted.	Informational message. No user intervention is required.
DHCP enabled: IP address assigned by DHCP.	Informational message. No user intervention is required.
Static IP address <*variable*> assigned.	Informational message. No user intervention is required.
Network interface bonding mode set to <*variable*>.	Informational message. No user intervention is required.
Network MTU size set to <*variable*>.	Informational message. No user intervention is required.
System name set to <*variable*>.	Informational message. No user intervention is required.
Email relay host set to <*variable*> for email alerts.	Informational message. No user intervention is required.
Recipients for email alerts set to <*variable*>.	Informational message. No user intervention is required.
Recipient <*variable*> added to receive email alerts.	Informational message. No user intervention is required.
Recipient <*variable*> is no longer receiving email alerts.	Check whether email recipient still exists, or if mailbox is full.
Administrator information set to <*variable*> for email alerts.	Informational message. No user intervention is required.
Test email sent.	Informational message. No user intervention is required.
Joined the Windows Active Directory domain <*variable*>.	Informational message. No user intervention is required.
Left the Windows Active Directory domain <*variable*>.	Informational message. No user intervention is required.
System diagnostics package <*variable*> deleted.	Informational message. No user intervention is required.
All diagnostic packages deleted.	Informational message. No user intervention is required.

System Event Message	Description/Meaning or Action
System diagnostic package <*variable*> is copied off the system.	Informational message. No user intervention is required.
System statistics reset by administrator.	Informational message. No user intervention is required.
System diagnostic package <*variable*> is collected.	Informational message. No user intervention is required.
System diagnostics space usage exceeded threshold. Auto cleaning oldest package: <*variable*>.	Informational message. No user intervention is required.
Internal Error. CIFS server cannot access file service.	Contact Dell Support for intervention or assistance. Collect diagnostics log file bundle, and upload to Dell Support.
Host <*variable*> added to SNMP alert recipient list.	Informational message. No user intervention is required.
Host <*variable*> deleted from SNMP alert recipient list.	Informational message. No user intervention is required.
Host <*variable*> enabled for SNMP alerts.	Informational message. No user intervention is required.
Host <*variable*> disabled for SNMP alerts.	Informational message. No user intervention is required.
User <*variable*> logged into the system.	Informational message. No user intervention is required.
CIFS user <*variable*> added.	Informational message. No user intervention is required.
CIFS user <*variable*> deleted.	Informational message. No user intervention is required.
Password changed for CIFS user <*variable*>.	Informational message. No user intervention is required.
System upgrade completed <*variable*>.	Informational message. No user intervention is required.
Cleared foreign configuration on disk <*variable*>.	Informational message. No user intervention is required.
User <*variable*> logged into the system.	Informational message. No user intervention is required.
Disk <*variable*> configured as hot spare.	Informational message. No user intervention is required.
Telnet service enabled.	Informational message. No user intervention is required.
Telnet service disabled.	Informational message. No user intervention is required.
DNS settings updated with primary <*variable*>, secondary <*variable*>, and suffix <*variable*>.	Informational message. No user intervention is required.
System initialized successfully.	Informational message. No user intervention is required.
<*variable*> added with entitlement id <*variable*>.	Informational message. No user intervention is required.
Security privilege(s) changed for <*variable*>.	Informational message. No user intervention is required.
User <*variable*> logged into the administrative web interface.	Informational message. No user intervention is required.
Network interface(s) <*variable*> enabled.	Informational message. No user intervention is required.
Network interface(s) <*variable*> disabled.	Informational message. No user intervention is required.
SMBD backup traffic interface(s) <*variable*> do not have an IP.	
DR2000v registered successfully.	Informational message. No user intervention is required.
DR2000v unregistered successfully.	Informational message. No user intervention is required.

System Event Message	Description/Meaning or Action
DR2000v data storage expanded by 1 TiB.	Informational message. No user intervention is required.
Miscellaneous Invalid/Last Event.	Informational message. No user intervention is required.
System Event = Type 6	
File system check started.	Informational message. No user intervention is required.
File system check completed successfully. No inconsistencies were found.	Informational message. No user intervention is required.
File system check found some inconsistencies.	The DR Series system Maintenance mode repair process should resolve this. If the problem persists, contact Dell Support for assistance or intervention.
File system repair started.	Informational message. No user intervention is required.
File system repair completed.	Informational message. No user intervention is required.
File system check stop requested.	Informational message. No user intervention is required.
One (or more) file(s) were deleted as part of the repair process.	Informational message. No user intervention is required. To verify, please use the DR Series system CLI **maintenance --filesystem --repair_history verbose** command.
One or more file(s) were deleted as part of the repair process for container <*variable*>. Replication will be stopped for this container.	Informational message. No user intervention is required.
One or more file(s) were deleted as part of the repair process for container <*variable*>. Re-sync has been initiated for this container.	Informational message. No user intervention is required.
System Event = Type 7	
RDA server started successfully.	Informational message. No user intervention is required.
RDA server failed to start.	Restart the RDA server. If issue persists, contact Dell Support for assistance or intervention.
RDA server stopped successfully.	Informational message. No user intervention is required.
<*Variable*> client authentication failed.	Retry the OST client authentication. If issue persists, contact Dell Support for assistance or intervention.
<*Variable*> Logical Storage Unit (LSU) quota exceeded <*variable*>.	Informational message. Reduce the number of LSUs. If issue persists, contact Dell Support for assistance or intervention.
<*Variable*> backup failed <*variable*>.	Retry the OST backup operation. If issue persists, contact Dell Support for assistance or intervention.
<*Variable*> Opdup failed <*variable*>.	The OST optimized duplication process failed. If issue persists, contact Dell Support for assistance or intervention.
<*Variable*> Restore failed <*variable*>.	The OST restore process failed. If issue persists, contact Dell Support for assistance or intervention.

System Event Message	Description/Meaning or Action
RDA connections exceeded the maximum limit; count: <*variable*>, maximum limit: <*variable*>.	Informational message. Reduce the number of OST connections. If issue persists, contact Dell Support for assistance or intervention.
Connection from the <*variable*> client <*variable*> aborted.	Informational message. No user intervention is required.
RDA client protocol version is not supported.	Informational message. No user intervention is required. Check for the supported OST client versions in the *Dell DR Series System Interoperability Guide*.
System is entering the Maintenance mode: <*variable*> LSU information file is corrupted.	Informational message. No user intervention is required. If issue persists, contact Dell Support for assistance or intervention.
System is entering the Maintenance mode: <*variable*> image information is corrupted.	Informational message. No user intervention is required. If issue persists, contact Dell Support for assistance or intervention
<*variable*> client connection was reset.	Informational message. No user intervention is required.
System is entering the Maintenance mode: RDA meta directory is corrupted.	Informational message. No user intervention is required.
RDA server initialization failed.	Informational message. No user intervention is required.
RDA server initialization was successful.	Informational message. No user intervention is required.
System entering Maintenance Mode - RDA txlog full, LSU <*variable*>.	Informational message. No user intervention is required.
System entering Maintenance Mode - RDA txlog operation error <*variable*>, LSU <*variable*>.	Informational message. No user intervention is required.
System entering Maintenance Mode - RDA txlog roll-forward error <*variable*>, LSU <*variable*>.	Informational message. No user intervention is required.

About the Diagnostics Service

The **Diagnostics** service in the DR Series system lets you display, collect, and manage your system's diagnostic log file bundles. Each diagnostic log file bundle provides:

- A current snapshot of system operations
- System-related information that assists in understanding system operations
- A record of system operations in case Dell Support needs to provide technical assistance

To access this functionality, use the following DR Series system navigation panel GUI option:

- **Support → Diagnostics**

The **Diagnostics** service works by collecting all the system-related information that could help when diagnosing a problem or error condition in the system.

For more information about diagnostics log file bundles, see Diagnostics Page and Options.

Diagnostics runs as a service during system startup, and this process listens for incoming requests. There are two modes in which the diagnostics collection process is started:

- **Admin-Generated mode**: when a DR Series system CLI or DR Series system GUI request is made by the administrator (and the default reason that is listed is admin-generated).
- **Auto-Generated mode**: when a process or service failure is reported, the DR Series system starts collecting system-related information. After it completes the auto-generated collection, it generates a system event.

When the diagnostics log directory exceeds the maximum storage capacity, any log older than one hour is automatically deleted. The DR Series system GUI lets you download and save diagnostics log files to other systems on your network. The DR Series system also maintains a separate archive logs directory that collects other system-related information, and these archive logs are also automatically deleted when they exceed a maximum capacity.

For more information, see Diagnostics Page and Options, Generating a Diagnostics Log File, Downloading Diagnostics Log Files. and Deleting a Diagnostics Log File.

NOTE: When you generate a diagnostics log file bundle, it contains all of the DR Series system information that you need when contacting Dell Support for technical assistance. When a diagnostics log file bundle is generated, this process also collects all the previous auto-generated diagnostics and deletes them from the system.

The diagnostics log file bundle collects the same type of hardware, storage, and operating system information that is collected when using the Dell System E-Support Tool (DSET) and the DR Series system CLI commands (**diagnostics --collect --dset**). For more information about DR Series system command line interface commands, see the *Dell DR Series Command Line Reference Guide*.

The DSET-based information that gets collected for the system helps Dell Support to troubleshoot or evaluate the status of your DR Series system.

Understanding Diagnostics Collection

The Diagnostics service collection tool process observes the following guidelines:

- DR Series system triggers an automatic diagnostic log collection of the DR Series system status for any system process or service failures.
- All automatic diagnostic collection requests are queued and executed sequentially.
- The DR Series system GUI provides options to display existing diagnostics logs, generate new diagnostics logs, download and save copies of existing diagnostics logs, or delete existing diagnostics logs. For more information, see Diagnostics Page and Options and About the Diagnostics Service.
- The DR Series system CLI also provides the means for managing, generating, or downloading the diagnostics log files. For more information, see the *Dell DR Series System Command Line Reference Guide*.

About the DR Series System Maintenance Mode

In general, the DR Series system enters the **Maintenance** mode whenever the file system has encountered an issue that prevents it from operating normally.

NOTE: You can use the **Reason code** information available in the **Maintenance** mode to call Dell Support. All maintenance must be conducted using the DR Series systems Command Line Interface.

When in its **Maintenance** mode, the filesystem is in a read-only state, and the system runs the following maintenance-based operations:

NOTE: Whenever the DR Series systems enters or exits from the **Maintenance** mode state, all communication via protocols is lost.

- Runs an internal filesystem check.

- Generates a filesystem status report (if the filesystem check finds no issues, the DR Series system switches back to **Operational** mode without user intervention).

If the filesystem check finds issues, you can choose to make repairs (using **Confirm Repair Filesystem**) or ignore the detected issue (using **Skip Repair Filesystem**), at which point the system switches back to **Operational** mode.

The **Maintenance** mode process displays a number of stages, indicated on the Maintenance Mode progress bar, which include:

- Preparing for Filesystem Check
- Scan in Progress
- Completed Generating Report

  NOTE: If the Filesystem Check detects any repairable files, it generates a Repair Report that identifies these reported files. The Maintenance Mode progress bar halts at the Completed Generating Repair stage, and remains in **Maintenance** mode until you click **Confirm Repair Filesystem**. The DR Series system does not advance to the Switching to Operation Mode stage until the filesystem repair is completed.

- Switching to Operational Mode
- Operational Mode (Normal State)

The **Maintenance Mode** page provides the following information:

- Maintenance Mode Progress bar:
  - Displays the five stages of **Maintenance** mode
  - Updates the progress bar as each stage completes

    NOTE: If an alert displays above the Maintenance Mode progress bar, this indicates that the filesystem check has completed, and it has generated a report on the repairable files (which are displayed in the Repair Report pane under the Maintenance Mode progress bar). To repair all of the reported files listed in the Repair Report, you must click **Confirm Repair Filesystem**.
- Repair Report:
  - Displays a list of repairable filesystem files that were detected in the Filesystem Check.
  - Identifies the repairable files by Container ID, File/Inode/Directory location, and a brief reason for failure.
  - Provides a search capability that allows you to click **prev** or **next** to display the previous or next page in the Repair Report, or lets you display a specific page number of the Repair Report by entering this number in the **Goto** page and click **go**.
- System Information pane:
  - **System Name**
  - **Software Version**
  - **Current Date/Time**
  - **iDRAC IP Address**
- Support Information
  - **Service Tag**
  - **Last Diagnostic Run**
  - **BIOS Version**

NOTE: When in Maintenance mode, the DR Series system navigation panel displays the following options that are links to display the correspond page in the DR Series system GUI:

- **Alerts**
- **Events**
- **Health**
- **Usage**
- **Diagnostics**
- **Software Upgrade**

After the DR Series system enters **Maintenance** mode, there can only be two possible outcome states:

- **Operational** mode (Normal State): where the filesystem check was successful, and no system files need to be repaired (Filesystem Check: successful).
- **Maintenance** mode has halted: where the filesystem check detected one or more repairable files (Filesystem Check: unsuccessful).

Filesystem Check — Successful: when the **Maintenance** mode successfully completes all of its stages, the DR Series system displays its status as having entered **Operational** mode (Normal State). Only after the **Maintenance** mode has successfully completed its internal check can it return to an **Operational** mode.

To return to the **Operational** mode, click **Go to Dashboard** on the **Maintenance Mode** page options bar. **Go to Dashboard** is only active when all of the internal system checks have completed and the progress bar indicates that all stages have been completed.

NOTE: You may encounter issues when using data management agents (DMAs) such as NetBackup with expired backup images when the DR Series system is in its **Maintenance** mode.

NOTE: When in **Maintenance** mode, image expiration fails because the DR Series system is in a read-only state. If this occurs, the DMA assumes that the backup images have expired. However, the DR Series system administrator may be unaware that the backup data images still reside on the DR Series system.

Filesystem Check — Unsuccessful: when the **Maintenance** mode halts at the Completed Generating Report stage, this indicates that the filesystem check detected some repairable files, and listed them in the Repair Report pane on the **Maintenance Mode** page.

To return to the **Operational** mode, click **Confirm Repair Filesystem** on the **Maintenance Mode** page options bar to repair the files listed in the Repair Report. **Confirm Repair Filesystem** is the only active option you can select when the progress bar indicates that some filesystem files are in need of repair.

Scheduling DR Series System Operations

The most important thing to remember when scheduling critical DR Series system operations is that you want to ensure that you perform each of these operations at a time when it will not overlap or interfere with the running of any of the other key system operations.

By better scheduling when you run system operations, you can optimize your system resources and make it possible to achieve the best possible DR Series system performance. To do this, plan and schedule time periods in which to perform the following critical system operations:

- Data ingests (which are dependent upon the DMAs)
- Replication process
- Cleaner process (space reclamation)

The main goal in planning and scheduling operations is running the Cleaner and Replication operations at times when they do not overlap or interfere with other important system operations. You want to make sure that by properly scheduling and planning, your system can perform each of these key operations independent of the other.

The best practice is to run these two operations during non-standard business hours, so that they do not conflict with any of your other backup or ingest operations. In short, efficient scheduling maximizes the best use of your system resources.

Dell recommends scheduling resource-intensive operations during specific time periods when no other system operations are being performed. This approach is called *windowing*, which requires scheduling a specific block of time (or "window"), each with a set starting and stopping point so that you can perform data ingests, replication, or space reclamation operations without interfering with the running of any other operation.

Creating a Cleaner Schedule

Performing scheduled disk space reclamation operations are recommended as a method for recovering disk space from system containers in which files were deleted as a result of deduplication. The best method is to schedule a time when you can run the Cleaner on your DR Series system with no other planned processes running. Alternately, another method lets the Cleaner process on the DR Series system run whenever it determines that there are no active data ingests.

NOTE: Even if no Cleaner schedule is set, but the system detects that there is disk space that can be reclaimed, the Cleaner process runs. However, the Cleaner will not start until the following conditions are met: it detects that there are no active data ingests, that two minutes of system idle time have elapsed since the last data file ingest was completed, and that the Replication process is not running (the Cleaner process runs as a lower system priority operation than the Replication process).

NOTE: Running the Cleaner while ingesting data, reduces system performance. Ensure that you schedule the Cleaner to run when backup or replication is not in progress.

NOTE: The **Cleaner Schedule** page displays the current DR Series system time zone and current timestamp (using this format: US/Pacific, Fri Nov 2 15:15:10 2012).

To schedule Cleaner operations on your system, complete the following:

1. Select **Schedules** → **Cleaner Schedule**.

   The **Cleaner Schedule** page is displayed.
2. Click **Schedule** to create a new schedule (or click **Edit Schedule** to modify an existing schedule).

   The **Set Cleaner Schedule** page is displayed.
3. Select (or modify) the **Start Time** and **Stop Time** setpoint values using the **Hour** and **Minutes** pull-down lists to create a Cleaner schedule.

   NOTE: You must set a corresponding **Stop Time** for every **Start Time** set in each Cleaner schedule you create. The DR Series system will not support any Cleaner schedule that does not contain a **Start Time/Stop Time** pair of setpoints (daily or weekly).
4. Click **Set Schedule** for the system to accept your Cleaner schedule (or click **Cancel** to display the **Cleaner Schedule** page).

   NOTE: To reset all of the values in the current Cleaner schedule, click **Reset** in the **Set Cleaner Schedule** dialog. To selectively modify values in the current schedule, make your changes to the corresponding hours and minutes pull-down lists to represent the **Start Time** and **Stop Time** you wish to set, and click **Set Schedule**.

The current Cleaner Status is represented in the **Dashboard** page in the System Information pane as one of the three following states:

- **Pending**—displayed when there is any scheduled window set and the current time is outside the scheduled window for the Cleaner operation.

- **Running**—displayed when the Cleaner operation is running during a scheduled window.
- **Idle**—displayed only if there is no Cleaner operation running during a scheduled window.

Dell recommends that you do not schedule the running of any Cleaner operations during the same time period when replication or ingest operations will be running. Failure to follow this practice will affect the time required to complete the system operations and/or impact your DR Series system performance.

Displaying Cleaner Statistics

To display additional Cleaner statistics, you can use the DR Series system CLI **stats --cleaner** command to show the following categories of Cleaner statistics:

- Last Run Files Processed (number of files processed by Cleaner)
- Last Run Bytes Processed (number of bytes processed by Cleaner)
- Last Run Bytes Reclaimed (number of bytes reclaimed by the Cleaner)
- Last Run Start Time (indicates date and time last Cleaner process started)
- Last Run End Time (indicates date and time last Cleaner process ended)
- Last Run Time To Completion(s) (indicates the number of times that Cleaner process has successfully completed)
- Current Run Start Time (indicates date and time current Cleaner process started)
- Current Run Files Processed (number of files processed by current Cleaner process)
- Current Run Bytes Processed (number of bytes processed by current Cleaner process)
- Current Run Bytes Reclaimed (number of bytes reclaimed by the current Cleaner processed)
- Current Run Phase 1 Start Time (indicates date and time for start of current Cleaner process phase 1)
- Current Run Phase 1 Records Processed (lists the number of data records processed in current Cleaner process phase 1)
- Current Run Phase 1 End Time (indicates date and time for end of current Cleaner process phase 1)
- Current Run Phase 2 Start Time (indicates date and time for start of current Cleaner process phase 2)
- Current Run Phase 2 Records Processed (lists the number of data records processed in current Cleaner process phase 2)
- Current Run Phase 2 End Time (indicates date and time for end of current Cleaner process phase 2)
- Current Run Phase 3 Start Time (indicates date and time for start of current Cleaner process phase 3)
- Current Run Phase 3 Records Processed (lists the number of data records processed in current Cleaner process phase 3)
- Current Run Phase 3 End Time (indicates date and time for end of current Cleaner process phase 3)
- Current Run Phase 4 Start Time (indicates date and time for start of current Cleaner process phase 4)
- Current Run Phase 4 Records Processed (lists the number of data records processed in current Cleaner process phase 4)
- Current Run Phase 4 End Time (indicates date and time for end of current Cleaner process phase 4)

For more information about DR Series system CLI commands, see the *Dell DR Series System Command Line Reference Guide*.

15

Supported Ports in a DR Series System

The following table lists the application and service ports found on a normally operating DR Series system. There may be other ports that are not listed here, that an administrator may need to open and enable to support specific operations across the network. Be aware that the ports listed in the following table may not reflect your specific network environment, or any planned deployment. While some of these DR Series system ports may not need to be accessible through the firewall, this information is made available when deploying the DR Series system in your own network because it indicates supported ports that may need to be exposed.

Table 6. Supported DR Series System Ports

Port Type	Number	Port Usage or Description
DR Series System Application Ports		
TCP	20	File Transfer Protocol (FTP)—for transferring files.
TCP	23	Telnet—remote terminal access protocol for unencrypted text communications.
TCP	80	Hypertext Transfer Protocol (HTTP)—unencrypted protocol communications.
TCP	443	HTTPS—combination of the HTTP with Secure Socket Layer (SSL)/Transport Layer Security (TLS).
TCP	1311	Hardware Health Monitor (Note: this is not used on the DR2000v)
TCP	9901	Watcher
TCP	9904	Configuration Server (needed for replication operations)
TCP	9911	Filesystem Server (needed for replication operations)
TCP	9915	MetaData Replication (needed for replication operations)
TCP	9916	Data Filesystem Server (needed for replication operations)
TCP	9918	Diagnostics Collector
TCP	9920	Data path used for OST replications
TCP	10011	Control channel (needed for OST operations)
TCP	11000	Data channel (needed for OST operations)
DR Series System Service Ports		
TCP	22	Secure Shell (SSH)—used for secure logins, file transfers like SCP (Secure Copy) and SFTP (Secure File Transfer Protocol)
TCP	25	Simple Mail Transfer Protocol (SMTP)—used for routing and sending email
TCP	139	SMB daemon—used for SMB protocol-related processes

Port Type	Number	Port Usage or Description
TCP	199	SNMP daemon—used by Simple Network Management Protocol (SNMP) requests
TCP	801	NFS status daemon

16

Getting Help

For more information about what you can attempt to resolve yourself or to get technical assistance from Dell for the DR Series system, see the topics below, "Before Contacting Dell Support," and "Contacting Dell."

Before Contacting Dell Support

If you encounter an error condition or operational issue, Dell recommends that you first attempt to see if you can resolve it using the supporting Dell DR Series system documentation before you make an attempt to contact Dell Support for technical assistance.

To help isolate or diagnose any basic issues that you may encounter with the Dell DR Series system, Dell recommends that you perform the following tasks:

- Refer to the *Dell DR Series System Administrator Guide* to verify if it contains information that can explain or resolve your issue. See Chapter 9, "Troubleshooting and Maintenance".
- Refer to the *Dell DR Series System Command Line Reference Guide* to verify if it contains information that can explain or resolve your issue.
- Read the latest set of *Dell DR Series System Release Notes* to verify if they contain any information that can explain or resolve your issue.
- Locate your Dell support account number and password, locate the Service Tag for your DR Series system, understand your type of support account, and be ready to provide specific details about the system operations you were performing.
- Record the content of any status or error dialog messages that you received, and the sequence in which they were displayed.
- Generate a current version diagnostics file (or if this is not possible, locate your latest existing diagnostics file).
  - Using the DR Series system GUI, click **Diagnostics** → **Generate** to generate a diagnostics file.
  - Using the DR Series system CLI, at the system prompt, enter the command **diagnostics --collect** to generate a diagnostics file. For more information, see the *Dell DR Series System Command Line Reference Guide*.

NOTE: For best results in addressing replication issues, you should generate diagnostics files on both DR Series source and target systems as close in time as possible.

NOTE: Each generated diagnostics file bundle contains information to assist Dell Support with the most current data about:

- System alerts and events
- System configuration status
- System log files
- System statistics for storage and replication containers
- System hardware component status

Contacting Dell

The topic explains the process for customers who need to contact Dell Support for technical assistance. For customers in the United States, please call 800-WWW-DELL (800-999-3355).

NOTE: If you do not have an active Internet connection, you can still find the proper contact information that you need on your purchase invoice, packing slip, bill, or Dell product catalog.

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area.
To contact Dell for sales support, technical support, or customer service issues:

1. Visit **support.dell.com**.
2. Click to select your country/region at the bottom of the **support.dell.com** page. For the full listing of countries and regions, click **All**.

   The **Choose a Country/Region** page is displayed.
3. Click the country/region from the **Americas**, **Europe, Middle East, & Africa**, or **Asia Pacific** choices.
4. Select the appropriate service or support link based on your need.
5. Select the method of contacting Dell that is most convenient for you.