# Oracle MaxRep for SAN

# User's Guide

ORACLE

FLASH STORAGE SYSTEMS

Part Number E51212-08
Oracle MaxRep for SAN release 3.0
2017 June

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at *http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc*.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit *http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info* or visit *http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs* if you are hearing impaired.

# Contents

# List of Tables

# List of Figures

# Preface

## Oracle Resources

**Important:** For the latest version of this document, visit the *SAN Storage – Oracle Flash Storage Systems* section at the Oracle Help Center (http://www.oracle.com/goto/fssystems/docs).

**Table 1: Oracle resources**

| For help with... | Contact... |
|---|---|
| Support | *http://www.oracle.com/support* (www.oracle.com/support) |
| Training | *https://education.oracle.com* (https://education.oracle.com) |
| Documentation | • *SAN Storage – Oracle Flash Storage Systems*: (http://www.oracle.com/goto/fssystems/docs)<br>• From Oracle FS System Manager (GUI): **Help** > **Documentation**<br>• From Oracle FS System HTTP access: (*system-name-ip*/documentation.php where *system-name-ip* is the name or the public IP address of your system) |
| Documentation feedback | *http://www.oracle.com/goto/docfeedback* (http://www.orarcle.com/goto/docfeedback) |
| Contact Oracle | *http://www.oracle.com/us/corporate/contact/index.html* (http://www.oracle.com/us/corporate/contact/index.html) |

# Typographical Conventions

**Table 2: Typography to mark certain content**

| Convention | Meaning |
|---|---|
| *italics* | Within normal text, words in italics indicate one of the following items:<br>• Hypertext, as in a URL<br>• A reference to a book title<br>• New terms and emphasized words<br>• Command variables |
| `monospace` | Indicates one of the following, depending on the context:<br>• The name of a file or the path to the file<br>• *Output* displayed by the system on the command line |
| **`monospace`** (bold) | *Input* provided by an administrator on the command line. |
| **>** | Indicates a menu item or a navigation path in Oracle FS System Manager (GUI). For example, "Click **SAN** > **Storage** > **LUNS** > **Action** > **Clone**" means to click the **Clone** link on the **SAN** page in the GUI. |
| **...** | Indicates that one or more steps have been omitted from the path or menu structure. The ellipsis is used within an expression of a navigation path or within a cascading menu structure. For example, in the **SAN** > **Storage** > **LUNS** > **...** > **Clone** menu structure, the **...** implies that one or more menu items have been omitted. |

# Related Documentation

Familiarize yourself with the following related documents:

- *Oracle FS1-2 Flash Storage System Installation Guide*
- *Oracle Flash Storage System Administrator's Guide*
- *Oracle MaxRep for SAN Hardware Guide*

CHAPTER 1

# Introduction to Oracle MaxRep for SAN

## Oracle MaxRep for SAN

Oracle MaxRep for SAN enables you to replicate and restore Oracle FS System data in a SAN environment.

In SAN replication, pairs of LUNs that are made up of source LUNs and target LUNs, are called replication pairs. The LUNs can reside on two Oracle FS Systems in a single location or on separate remotely distributed Oracle FS System, designated as primary and secondary.

One or more Oracle MaxRep Replication Engines manage and monitor the data replication process. The transfer of data takes place automatically as the data on the source LUN changes. Those changes are replicated to the target LUN. The replication pair updates continuously as long as the integrity of both LUNs persists and the communication link between the LUN locations is maintained.

Oracle MaxRep for SAN can replicate between Oracle FS Systems that reside in the same data center, or are geographically distributed between remote locations. The Oracle MaxRep Replication Engines use communication links between the two sites to replicate changes.

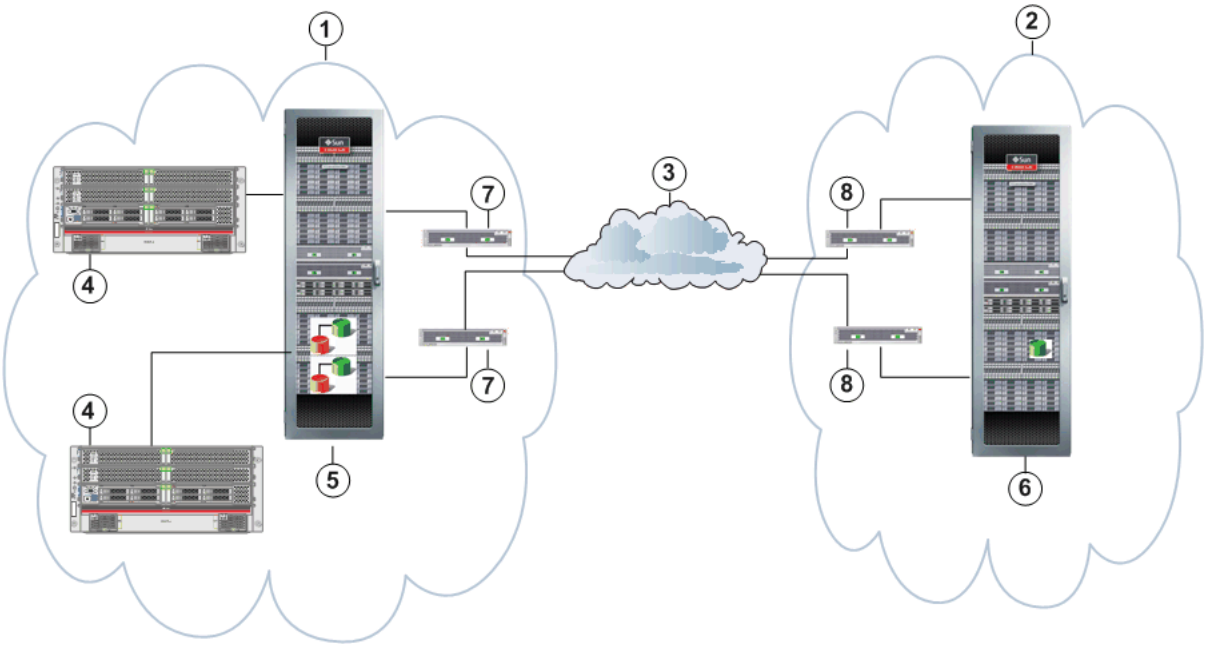
Oracle MaxRep for SAN supports synchronous and asynchronous LUN replication or application consistent volume sets.

- Synchronous replication requires at least one Replication Engine and is supported when the source LUN, the target LUN, and the Replication Engines are all attached to the same SAN fabric. Replication can also be synchronous when the source LUN and the target LUN are located in two data centers that are connected by an extended SAN fabric. The fabric might consist of fiber optic cables that uses dense wavelength division multiplexing (DWDM) between the primary and secondary locations.
- Asynchronous replication requires at least two Replication Engines. Asynchronous replication is supported generally when the primary and secondary locations are geographically distributed, and communication is over a wide area network (WAN) link, with separate Replication Engines at each location. The default connectivity for the WAN connection is through the Ethernet management ports (eth0 and eth2).

To ensure high availability (HA), Replication Engines can be deployed in HA pairs. One of the Replication Engines is in active mode. If the active Replication

Engine should fail, the second Replication Engine in each clustered pair is in passive mode, ready to take over.

**Figure 1: Asynchronous Oracle MaxRep for SAN configuration**




**Legend**

| | |
|---|---|
| 1 Primary site | 5 Primary Oracle FS System |
| 2 Secondary site | 6 Secondary Oracle FS System |
| 3 WAN connection | 7 Replication Engines on the primary site clustered for high availability |
| 4 Host | 8 Replication Engines on the secondary site clustered for high availability |

Data can be recovered from either the primary or the secondary site, and the direction of replication can be reversed. Several failover and failback scenarios can be planned and implemented using Oracle MaxRep for SAN.

### Related Links

*Oracle MaxRep for SAN Components*
*How Oracle MaxRep for SAN Works*
*Understanding Replication Concepts*
*Replication Configurations*

## Oracle MaxRep for SAN Components

The Oracle MaxRep for SAN relies on several key hardware and software components for reliable data protection and recovery.

The Oracle MaxRep for SAN includes the following components:

**Oracle FS System**

The Oracle FS System is an application-aware storage solution using policy-based Quality of Service (QoS) technology to serve application storage over iSCSI storage area networks. The replication process begins with the Oracle FS System that accepts a write operation to the protected LUNs and forwards the write operation to the Oracle MaxRep Replication Engine for replication.

**Oracle MaxRep Replication Engine**

The Replication Engine is an out-of-band offload engine that manages and monitors the replication and recovery process. You create protection plans to guide the replication operations. Using the web-based Oracle MaxRep for SAN GUI or command line reference (CLI), you can create, monitor, and recover protection plans. Utilization and trending reports and alerts are managed by the Replication Engine.

**Oracle MaxRep Agents**

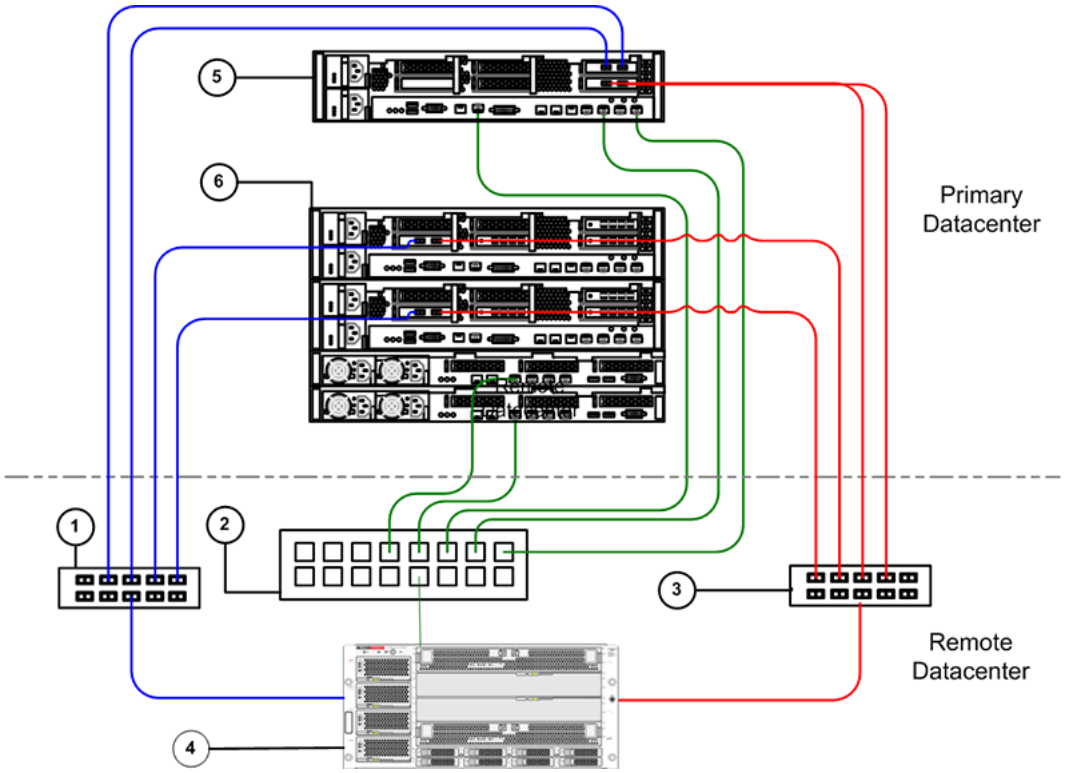
(Optional Oracle MaxRep agents are installed on application hosts and can issue application consistency bookmarks on a scheduled basis.

**Replication Engine Cluster**

Replication Engine Cluster is an optional component of the Oracle MaxRep solution. This component is a high availability feature that includes a passive Replication Engine, which is ready to take over if a failure of the active Replication Engine occurs.

The following figure shows the relationship of each Oracle MaxRep for SAN component in a remotely distributed Oracle FS System.

### Figure 2: Oracle FS MaxRep components




**Legend**

| | |
|---|---|
| 1 SAN Fabric (FC) switch "A" | 2 Ethernet switch |
| 3 SAN Fabric (FC) switch "B" | 4 Host server |
| 5 Replication Engine | 6 Oracle FS System |

### Related Links

*Oracle MaxRep for SAN*
*Understanding Replication Concepts*

## How Oracle MaxRep for SAN Works

Oracle MaxRep for SAN uses continuous data protection (CDP) technology. Oracle MaxRep can be configured to support long-distance disaster recovery requirements and operational recovery and backup requirements.

Oracle MaxRep for SAN replicates your mission-critical LUNs to one or more secondary LUNs that can be either local or remote.

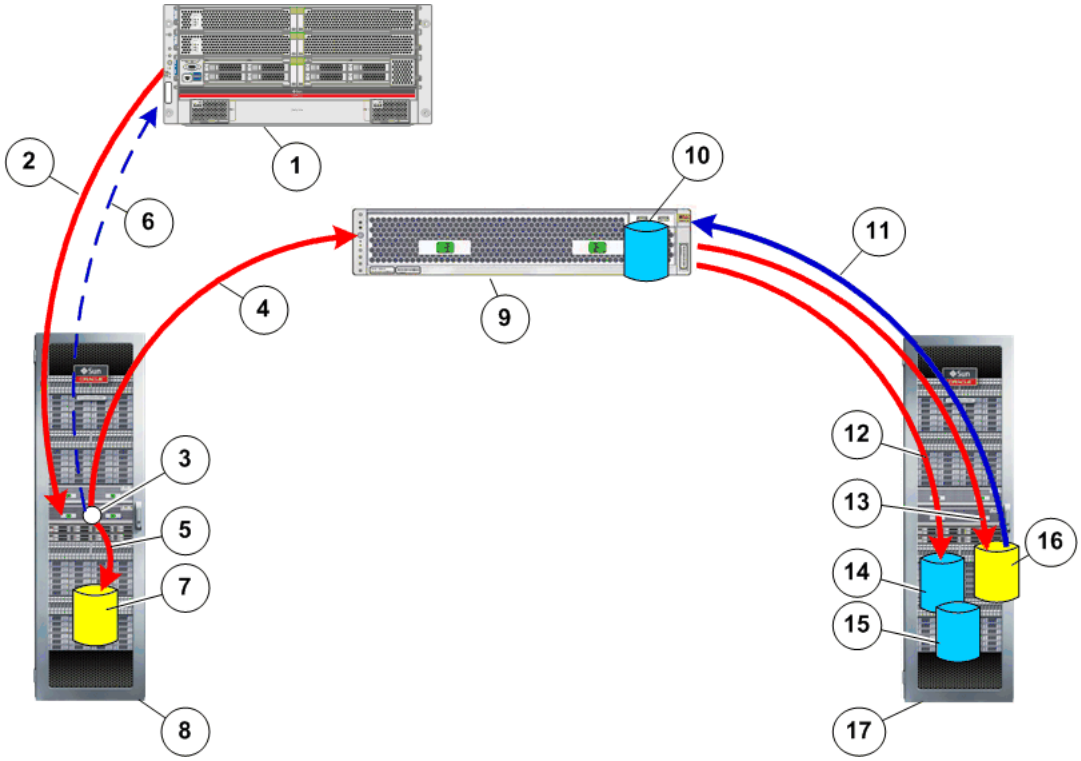
In the following illustration, which represents a local site, continuous data protection starts with new data written by the application server or host to the source Oracle FS System. The Controller copies (splits) the data by transmitting one copy to the LUN on the primary Oracle FS System, and the other copy to the Replication Engine. When the system writes the data to the primary LUN, the

system sends an acknowledgment to the application server that the data is successfully written to the LUN.

The Replication Engine reads the corresponding location of the target LUN and compares the new source and the existing target data. If the target LUN requires updating, the Replication Engine updates the target LUN and the retention LUN, or journal, of the protection plan LUNs.

Retention LUNs are LUNs on the Oracle FS System that hold the retention journal for the Replication Engine. The retention journal contains a list of time indexed replication events that allow rollback to any point in time.

**Figure 3: Continuous data protection process flow**



**Legend**

| | |
|---|---|
| 1 Application Server | 10 Home LUN |
| 2 New data write to primary Oracle FS System | 11 Read of target LUN data |
| 3 Write split at Controller | 12 Metadata write to replication journal |
| 4 Data write split to Replication Engine | 13 New data write to target LUN |
| 5 Data write split to source LUN | 14 Retention LUN |
| 6 Target LUN write acknowledgment to host | 15 Backup LUN |
| 7 Source LUN | 16 Target LUN |
| 8 Primary Oracle FS System | 17 Secondary Oracle FS System |
| 9 Replication Engine | |

The Replication Engine is never in the data path of the source application. This configuration prevents any impact on the operation of the production server that is hosting an application if a failure or replacement of the Replication Engine occurs. The benefit of such a configuration is that Oracle MaxRep for SAN can be deployed into your existing environments without disrupting your business operations.

The initial replication of the data from the source LUN to the target is performed in steps. The initial synchronization is performed in two steps and a final step checks for differences in the replicated data. These steps are explained in detail below.

**Note:** The Oracle MaxRep for SAN GUI uses the terms *sync* and *resync* to refer to synchronization and resynchronization, respectively.

**Resync Step 1**

The initial step of the replication process in which a baseline copy of the source LUN is replicated to the target LUN. For protection plans configured with the fast-copy option, this initial step transfers only unmatched blocks of data between the source and target LUNs between two Oracle FS Systems.

This comparison can significantly reduce the time and network resources that are required for the initial synchronization, compared to performing a complete copy.

**Resync Step 2**

Any additional data that is written to the source LUN during the Resync Step 1 process is journaled for processing in Resync Step 2. The Replication Engine replicates the captured changes to the target LUN.

**Differential Sync**

In the Differential Sync step Oracle MaxRep for SAN captures changes to the source LUN and sends them to the target LUN.

If resynchronization is required after the initial synchronization, the system captures ongoing changes, similar to the synchronization process. Oracle MaxRep for SAN supports Fast Resync, which replicates only unmatched blocks to the target LUN during the initial synchronization step. Asynchronous replication uses the Fast Resync feature. Synchronous replication uses Direct Resync, which reads data from the source LUN and writes the data directly to the target LUN.

During maintenance activities or an actual failure on a source LUN, Oracle MaxRep for SAN can switch direction to restore the source LUN from the target LUN. Because Oracle MaxRep for SAN uses CDP technology to replicate the data, the source can be restored to any point in time during the retention window. If optional Oracle MaxRep agents are in use, the target LUN can also be rolled back to an application consistency bookmark to ensure consistency of data.

Oracle MaxRep also supports the storing of snapshots (exact replica of the data of a source LUN as it existed in a single point-in-time copy) on physical or virtual drives.

### Related Links

*Understanding Replication Concepts*
*Oracle MaxRep for SAN Requirements*

## Understanding Replication Concepts

Replicating data using Oracle MaxRep for SAN involves a number of key concepts and technologies.

**Continuous Data Protection**

Continuous Data Protection (CDP) refers to a technology that continuously captures or tracks data modifications by saving a copy of every change made to your data, capturing every version of the data that you save. It allows you to restore data to any point in time. It captures the changes to data and sends them to a separate journal.

CDP-based solutions can provide fine granularities of restorable objects ranging from crash-consistent images to logical objects such as files, mail boxes, messages, and database files and logs.

Traditional backups require a schedule and can only restore data to the point at which it was backed up. CDP does not need a schedule because all the data changes on the source LUN are tracked continuously and sent to a target LUN.

Oracle MaxRep for SAN replicates block-level differences rather than file-level differences. This means that if you change one byte of a 100 GB file, only the changed block is replicated.

CDP technology has the following attributes:

- Data changes to a protected primary site are continuously captured or tracked.
- All data changes are stored in a secondary Oracle FS System.
- Data recovery takes much less time than tape backup or archives.

**Disaster Recovery**

Disaster Recovery (DR) is the ability to continue work after a catastrophic problem in a critical technology of the company infrastructure. A DR solution using CDP technology replicates your data to a secondary site. In case of disaster, you can get immediate access to the data that was on the primary site up to the moment of the disaster.

**Replication Stages**

Oracle MaxRep for SAN replicates drive level data in three stages:

**Resyncing (Step 1)**

The original data at your source LUN is replicated to the target LUN.

**Resyncing (Step 2)**

All data changes during Resyncing (Step I) are replicated to the target LUN.

**Differential Sync**

Differential Sync is a real-time process where any change in the source LUN is copied to the target LUN simultaneously.

**Consistent Data**

In case of DR or backup, the restored data must be consistent with the original data. To ensure the consistency of backup data, consistent bookmarks are issued at the source LUN at periodic intervals of time or on demand.

There are three types of consistency:

**Consistent**

Also called *crash consistent*. Specifies that all point-in-time LUN information is available. Non-bookmark point-in-time recoveries are Consistent.

**File System Consistent**

Specifies that the file system has flushed its caches to disk at the time that the bookmark was issued. File system consistency uses host-based Oracle MaxRep agents.

**Application Consistent**

Specifies that all application data, possibly across multiple volumes and including cached data, is flushed to storage at that point in time and is available. Oracle MaxRep for SAN also provides application consistency through host-based Oracle MaxRep agents.

Only Oracle MaxRep agents that work with an application or file system create bookmarks.

**Retention or CDP logs**

The Retention logs, sometimes called the CDP logs, store information about data changes on a source LUN within a specified time period. This time frame is referred to as the *retention window*. Consistent points are stored as bookmarks in the retention window. The LUN can be rolled back to any of the application-consistent bookmarks in this retention window.

If application consistency is not needed, the LUN can be rolled back to any point in time of this retention window. Applications that are rolled back without using any bookmarks in this retention window are only *crash consistent*.

There are four types of retention policies associated with this retention window:

**Time-Based**

The data in the retention window will be overwritten after the specified time period.

**Space-Based**

The data in the retention window is overwritten after the space limit is reached within the retention drives.

**Time and Space-Based**

The data in the retention window will be overwritten either after the specified time or after the specified space is used, depending on what occurs first.

**Sparse Retention**

For long-term data retention purposes, the sparse policy is used. The sparse policy helps to save space on retention drives and increases the retention window.

Depending on the type of policy enforced, the retention window is maintained by preserving periodic bookmarks while discarding older data changes within the retention log files. Discarding older data makes room for new data changes.

**Snapshot**

A snapshot is an accessible replica of data from the primary Oracle FS System as it existed at a single point in time in the retention window. There are two types of snapshots: physical snapshots and virtual snapshots.

- A physical snapshot is a full copy of the physical LUN. The size of the intended copy must be equal to or larger than the target LUN (in the replication pair).

  **Note:** Mount the physical snapshot from the Oracle FS System where the physical LUN is located.

- A virtual snapshot is a virtual LUN. A virtual snapshot is also known as a *vsnap*. Vsnaps require minimal system resources and load and unload quickly.

  **Note:** Mount a virtual snapshot to the recovery host from the Replication Engine that is hosting the virtual snapshot.

Physical snapshots and virtual snapshots are accessed in one of the following modes:

**Read-Only**

Read-only snapshots are for informational purposes and cannot accept or retain writes. The read-only option is available for virtual snapshots only. Physical snapshots are always read-write.

**Read-Write**

Read-write virtual snapshots accepts and retains writes. This is done by maintaining an archive log on some part of the local drive as specified.

**Read-Write-Journaled**

For virtual snapshots, read-write-journaled mode allows you to roll back the virtual snapshot to a different point in time after you recover your data. The read-write-journaled option is available for virtual snapshots only. Physical snapshots are always read-write.

## Related Links

*How Oracle MaxRep for SAN Works*
*Application Consistency Protection Plans*
*Oracle MaxRep for SAN Requirements*

# Oracle MaxRep for SAN Requirements

Oracle MaxRep for SAN has several requirements that must be met for replication to work properly.

**Table 3: Oracle FS MaxRep requirements**

| Item | Requirement |
|---|---|
| Oracle FS System | All source and target Oracle FS Systems must be running Oracle FS System Manager release 6.0.0, or higher.<br>• For FC only: The system must have FC SAN fabric connectivity.<br>• For iSCSI only: The system must have Ethernet LAN connectivity.<br>Drive Enclosure capacity must be sized properly to account for the additional capacity required for the replication solution. The Drive Enclosure spindle count must be sized properly to account for the performance requirements for the replication solution. |
| Pillar Axiom 600 | All source and target Pillar Axiom systems must be running Pillar Axiom Storage Services Manager, release 5.4.8, or higher.<br>• For FC only: The system must have FC SAN fabric connectivity.<br>• For iSCSI only: The system must have Ethernet LAN connectivity.<br>**Note:** For all Pillar Axiom systems, refer to the release notes for a list of supported firmware running on the Oracle MaxRep Replication Engines. |
| Oracle MaxRep Replication Engines | The number of Replication Engines that are required varies based on the specific replication solution. Synchronous replication between two Oracle FS Systems connected to the same SAN fabric might only require a single Replication Engine.<br>Complex implementations that include 1-to-many or many-to-1 synchronous and asynchronous replication with Replication Engine high availability (HA) clustering can include up to eight Replication Engines.<br>Refer to your account representative to ensure the number of Replication Engines in your environment is sufficient for your replication needs. |

Table 3: Oracle FS MaxRep requirements (continued)

| Item | Requirement |
|---|---|
| Ethernet ports | Each Replication Engine requires two RJ-45 Ethernet connections: one 10 Gigabit Ethernet (10 GbE) R-J45 connection for management, and one 100BT R-J45 connection for console access by Oracle Customer Support.<br><br>Two 10 Gb/s Ethernet ports are used for management, heartbeat, and wide area network (WAN) connectivity for asynchronous replication. An additional Integrated Lights-Out Manager (ILOM) port is used for remote console accessibility for remote support.<br><br>To support IP bonding for the management interface, one additional 10 GbE RJ-45 Ethernet port is required.<br><br>Twisted pair (TP) ports also support 1 Gb speeds. |
| Power | **Item**<br>iSCSI ports<br>**Requirement**<br>Each Replication Engine that uses iSCSI connectivity to a primary or secondary Oracle FS System requires six additional Ethernet connections. These Ethernet connections are separate requirements from the Ethernet ports. These connections will be either using 10 GbE RJ-45 ports or 10 GbE optical Ethernet ports that use optional Fortville PCIe NIC cards.<br><br>**Note:** Refer to the *Oracle MaxRep for SAN Hardware Guide* for additional information on Ethernet connectivity and for wiring diagrams for your specific Replication Engine hardware.<br><br>iSCSI configuration is limited to 255 replication pairs.<br><br>Each Replication Engine is powered by two Intel Xeon processor E5-2600 v4 CPUs with 24 memory slots. Each engine is redundant, hot-swappable with cooling fans, and power supply units..<br><br>Refer to the *Oracle MaxRep for SAN Hardware Guide* for specific power requirements. |
| Rack space | Each Replication Engine has a standard 1U form factor. |

**Table 3: Oracle FS MaxRep requirements (continued)**

| Item | Requirement |
|---|---|
| Browser | Access to the management interface of the Replication Engine is provided through a standard Internet browser. Browser requirements include:<br>• Microsoft Internet Explorer 5.5 or later<br>• Mozilla Firefox 1.5 or later<br>• Adobe Flash Player 10 or later<br>Screen resolution of 1024 x 768 pixels |
| Environment | Connectivity between sites for remote synchronous replication must include an extension of the local SAN fabric. This network system consists of fibre optic cables between the primary and secondary locations to the remote site using Dense Wavelength Division Multiplexing (DWDM) technology.<br>Sufficient bandwidth must be available to accommodate the change rate of the source data and the target Oracle FS System writes and journaling.<br>Connectivity between sites for remote asynchronous replication must include sufficient WAN bandwidth to accommodate the change rate of the source data. |

# Replication Configurations

Oracle MaxRep for SAN release 3.1 supports two basic types of replication configurations: synchronous and asynchronous.

Separate licenses are available for synchronous and asynchronous replication. Synchronous and asynchronous replication solutions can also be combined to provide one-to-many replication as well as many-to-one replication.

### Related Links

*Asynchronous Replication*
*Synchronous Replication*
*Capacity-Based Licenses and Features*

## Synchronous Replication

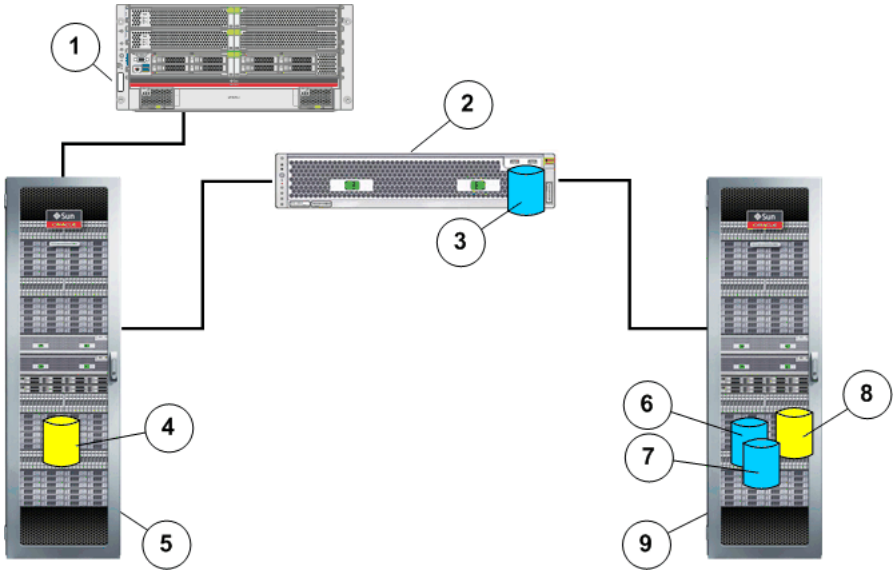
Synchronous replication involves saving data simultaneously in primary storage and in secondary storage, within a 100-kilometer radius, usually in the same campus or metropolitan area. Synchronous replication can be configured for standard or high availability requirements.

Synchronous replication requires at least one Replication Engine and is supported when the source LUN, the target LUN, and the Replication Engines

are all attached to the same SAN fabric. Replication can also be synchronous when the source LUN and the target LUN are located in two data centers that are connected by an extended SAN fabric. Whenever data is written to primary storage, the data is simultaneously replicated to secondary storage.

For example, a typical synchronous replication configuration in a local site consists of a single Oracle MaxRep Replication Engine and two Oracle FS Systems located in the same SAN fabric.

**Figure 4: Configuration for synchronous replication**



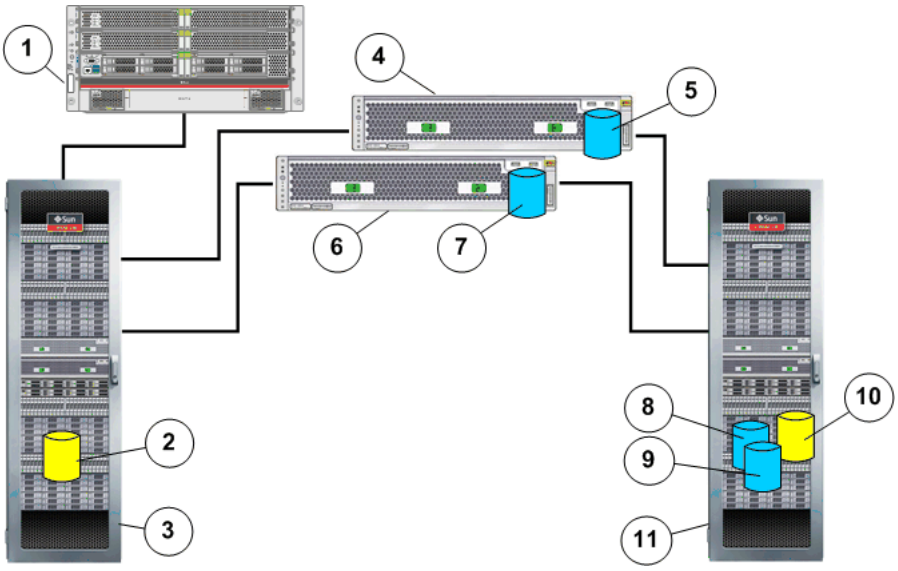

**Legend**

| | |
|---|---|
| 1 Host | 6 Retention LUN |
| 2 Replication Engine | 7 Backup LUN for configuration file |
| 3 Home LUN | 8 Target LUN |
| 4 Source LUN | 9 Secondary Oracle FS System |
| 5 Primary Oracle FS System | |

**Note:** If a service disruption on the primary site occurs, reverse replication is implemented. In this scenario, the target LUN becomes the source LUN, and the original source LUN becomes the target LUN. Reverse replication is activated when the original source site comes back online. In order for reverse replication to be effective, a retention LUN must be added to the original source location to facilitate the replication process.

Another example of synchronous replication includes adding a Replication Engine to each existing Replication Engine to provide high availability configuration. The two Replication Engines form an active-passive cluster. One of the Replication Engines is in active mode. The other Replication Engine is in passive mode, ready to take over if the active Replication Engine should fail.

### Figure 5: High availability configuration for synchronous replication




**Legend**

| | |
|---|---|
| 1 Application Server | 7 Secondary Home LUN |
| 2 Source LUN | 8 Retention LUN |
| 3 Primary Oracle FS System | 9 Backup LUN for configuration file |
| 4 Active Replication Engine | 10 Target LUN |
| 5 Home LUN | 11 Secondary Oracle FS System |
| 6 Passive Replication Engine | |

**Note:** If a service disruption on the primary site occurs, reverse replication is implemented. In this scenario, the target LUN becomes the source LUN, and the original source LUN becomes the target LUN. Reverse replication is activated when the original source site comes back online. In order for reverse replication to be effective, a retention LUN must be added to the original source location to facilitate the replication process.

A full high availability configuration for synchronous replication consists of a cluster of two Replication Engines and two Oracle FS Systems, both on the same SAN fabric.

### Related Links

*Replication Configurations*
*Oracle MaxRep for SAN Components*

## Asynchronous Replication

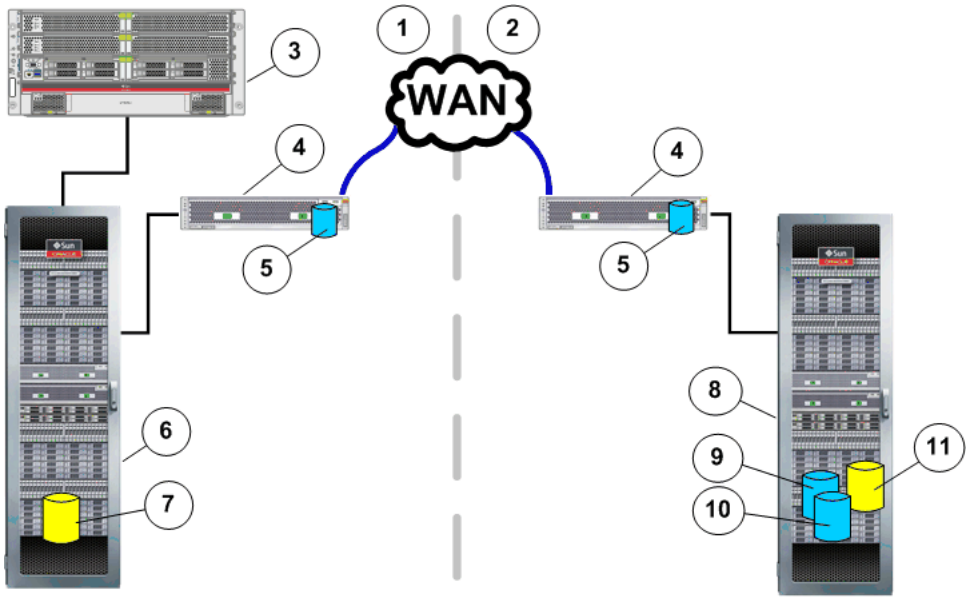
Asynchronous replication provides a time-lagged copy of data that is written to a secondary storage site, usually located remotely from the primary storage site.

Asynchronous replication requires at least two Replication Engines. Asynchronous replication is supported generally when the primary and secondary locations are geographically distributed, and communication is over a wide area network (WAN) link, with separate Replication Engines at each location. The default connectivity for the WAN connection is through the Ethernet management ports (eth0 and eth2). Whenever data is written to primary storage, a copy of that data is prepared for later transfer over a WAN connection to the secondary storage site.

For example, a typical asynchronous replication configuration consists of primary and secondary sites connected by an Internet protocol (IP) WAN. Each primary and secondary site consists of an Oracle MaxRep Replication Engine and an Oracle FS System.

When data from the application host is written to the primary Oracle FS System, a copy of the data, along with any necessary journal information, is prepared for transfer to the primary Replication Engine. The primary Replication Engine then transfers that data to the secondary Replication Engine, which writes the data to the secondary Oracle FS System.

**Figure 6: Basic configuration for asynchronous replication**



**Legend**

| | |
|---|---|
| 1 Primary site | 7 Source LUN |
| 2 Secondary site | 8 Secondary Oracle FS System |
| 3 Host | 9 Retention LUN |
| 4 Replication Engine | 10 Backup LUN |
| 5 Home LUN | 11 Target LUN |
| 6 Primary Oracle FS System | |

**Note:** If a service disruption on the primary site occurs, reverse replication is implemented. In this scenario, the target LUN becomes the source LUN, and the original source LUN becomes the target LUN. Reverse replication is activated when the original source site comes back online. In order for reverse replication to be effective, a retention LUN must be added to the original source location to facilitate the replication process.

Another example of asynchronous replication includes adding a secondary, or passive, Replication Engine to support the existing Replication Engine and to provide a high availability configuration. The primary Replication Engine and the secondary Replication Engine form an active-passive cluster. The first Replication Engine in each clustered pair is in active mode. The second Replication Engine in each clustered pair is in passive mode, ready to take over if the active Replication Engine should fail.

A full high availability configuration consists of a cluster of two Replication Engines and the primary Oracle FS System on the primary site. The secondary site contains a cluster of two Replication Engines and the secondary Oracle FS System. High availability is not required at both sites. You can configure any Replication Engine as high availability by adding another Replication Engine.

### Related Links

*Replication Configurations*
*Oracle MaxRep for SAN Components*

## Multi-Hop Replication

Multi-hop replication provides synchronous replication of a source LUN to a target LUN, and a second asynchronous replication of that target LUN to an additional target LUN.

Multi-hop replication requires both a synchronous and an asynchronous capacity-based license. The first synchronous hop of replication occurs between two Oracle FS Systems that are connected to the same SAN fabrics either at the same physical location, or between sites where the SAN fabrics are extended using dense wavelength division multiplexing (DWDM). The second hop of replication is asynchronous from the target Oracle FS System of the first synchronous hop to a remote location connected using the WAN.

Multi-hop replication is different from one-to-many replication in the following ways:

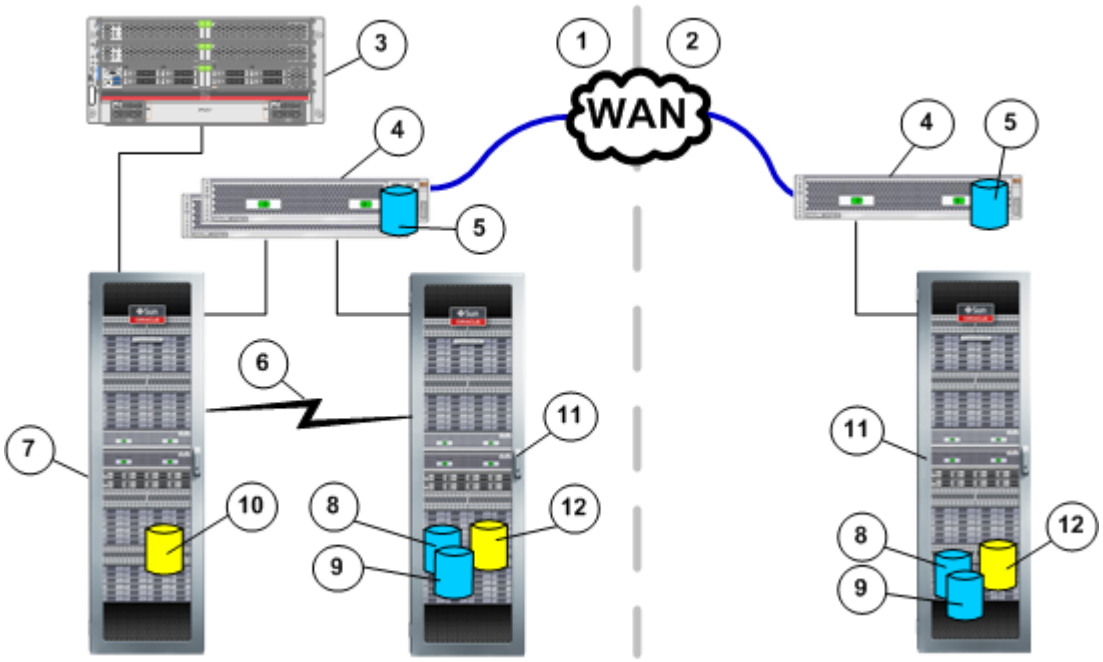
- Multi-hop replicates data from the source LUN to one target LUN. Then, this secondary target LUN is replicated to a third LUN.
- One-to-many replicates data from the source LUN at the primary site to multiple targets at multiple locations.

For example, a multi-hop replication configuration consists of an Oracle MaxRep Replication Engine and two Oracle FS Systems that are set up in a synchronous replication relationship at the primary site. In addition, another Replication Engine and Oracle FS System at the secondary site are set up in an asynchronous replication relationship with the secondary Oracle FS System at the primary site.

When data from the application host is written to the source LUN at the primary site, the Replication Engine replicates any data changes to the secondary LUN on another Oracle FS System at the primary site. This is the synchronous hop of the multi-hop replication.

The target LUN from the synchronous replication acts as a source LUN to the asynchronous hop of the multi-hop solution. As writes are received to the target LUN of the synchronous replication, a copy of its data and metadata is sent to the Oracle FS System located at the secondary site.

**Figure 7: Multi-hop replication configuration**



**Legend**

| | |
|---|---|
| 1 Primary site | 7 Primary Oracle FS System |
| 2 Secondary site | 8 Retention LUN |
| 3 Host | 9 Backup LUN for configuration file |
| 4 Replication Engine | 10 Source LUN |
| 5 Home LUN | 11 Secondary Oracle FS System |
| 6 DWDM connectivity | 12 Target LUN |

Release 3.0 of Oracle MaxRep for SAN requires two separate MaxRep Replication Engine configurations for multi-hop replication. A minimum of three MaxRep Replication Engines are required for a multi-hop configuration.

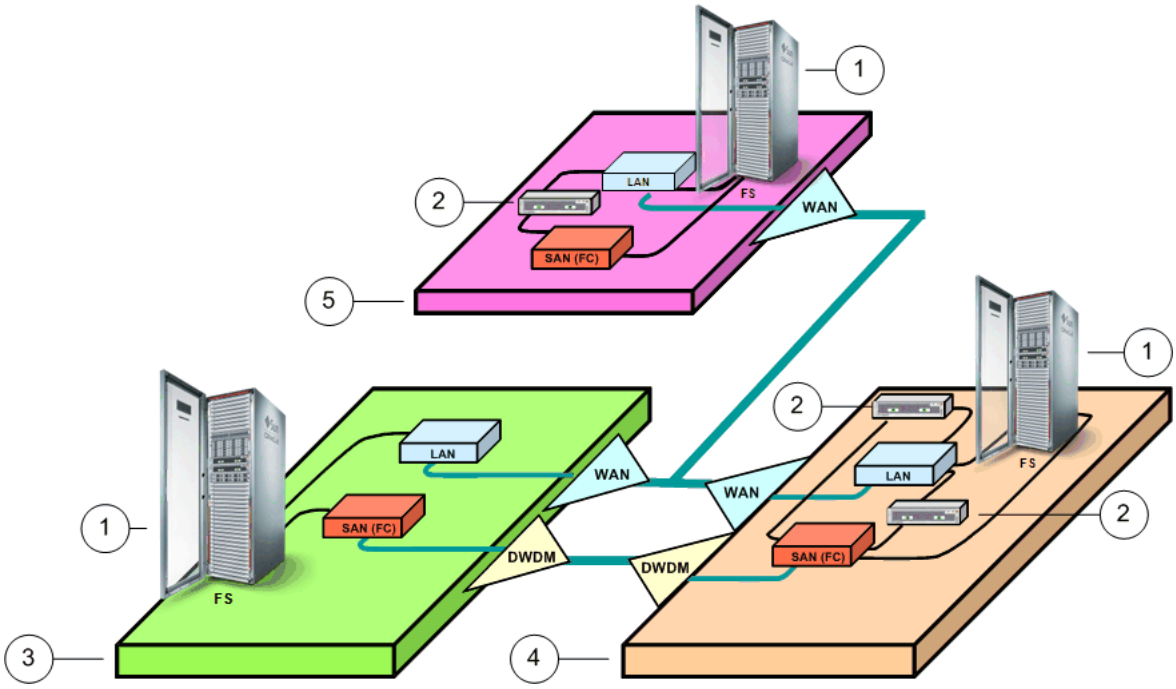
For example, a multi-hop solution can contain three Oracle Flash Storage Systems or three Pillar Axiom 600 systems dispersed over the three physical sites. This multi-hop replication topology would require the minimum amount of MaxRep R3 Replication Engines.

The first MaxRep R3 Replication Engine would replicate data synchronously between a source and target Oracle FS1 Flash Storage System or Pillar Axiom 600 system that are located at separate physical sites, if connected over dark fiber or DWDM.

The second and third MaxRep R3 Replication Engines would then replicate data asynchronously from the target Oracle FS1 Flash Storage System or Pillar Axiom 600 system in the first configuration to a third Oracle FS1 Flash Storage System or Pillar Axiom 600 system located at a third site.

This is accomplished by configuring the second MaxRep R3 Replication Engine in the second configuration to use the target Oracle FS1 Flash Storage System or Pillar Axiom 600 system from the first configuration as a source. The data would then be replicated asynchronously to a third site containing a target Oracle FS1 Flash Storage System or a target Pillar Axiom 600 system.

Figure 8: MaxRep R3 multi-hop replication configuration




**Legend**

| | |
|---|---|
| 1 Oracle FS System | 4 Secondary site |
| 2 Replication Engine | 5 Tertiary site |
| 3 Primary site | |

### Related Links

*Replication Configurations*
*Oracle MaxRep for SAN Components*

## One-to-Many Replication

One-to-many replication provides the capability to replicate data from a single source Oracle FS System to multiple target Oracle FS Systems. The one-to-many configuration protects your data in more than one remote facility.

One-to-many configuration is different from multi-hop replication in the following ways:

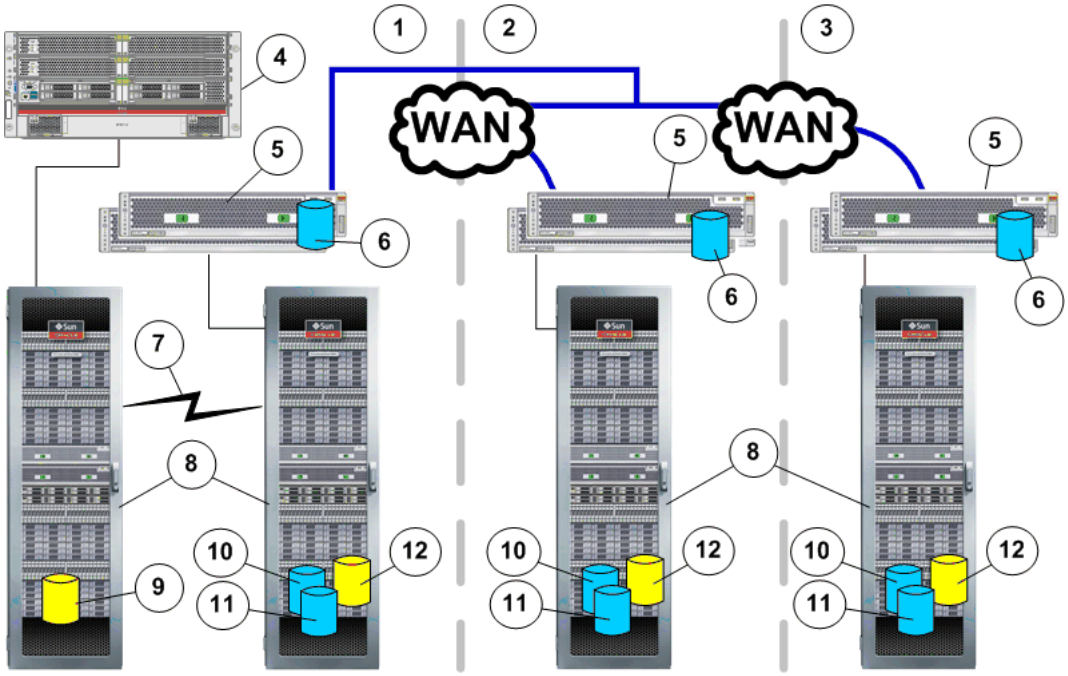
- One-to-many replicates data from the source LUN at the primary site to multiple targets at multiple locations.
- Multi-hop replicates data from the source LUN to one target LUN. Then, this secondary target LUN is replicated to a third LUN.

For example, a one-to-many replication configuration may consist of primary and secondary sites connected by the same extended SAN fabric that uses dense

wavelength division multiplexing (DWDM), and another remote site connected to the primary through a WAN.

The SAN fabric connection permits remote synchronous replication while the WAN connection permits remote asynchronous replication to the target Oracle FS Systems. Refer to the Oracle MaxRep for SAN release notes for the recommended limits for remote asynchronous configurations.

**Figure 9: Basic configuration for one-to-many replication**




**Legend**

| | |
|---|---|
| 1 Primary site | 7 DWDM connectivity |
| 2 Secondary site | 8 Oracle FS System |
| 3 Site “N” | 9 Source LUN |
| 4 Host | 10 Retention LUN |
| 5 Replication Engine | 11 Backup LUN for configuration file |
| 6 Home LUN | 12 Target LUNs |

**Note:** If a service disruption on the primary site occurs, reverse replication is implemented. In this scenario, the target LUN becomes the source LUN, and the original source LUN becomes the target LUN. Reverse replication is activated when the original source site comes back online. In order for reverse replication to be effective, a retention LUN must be added to the original source loation to facilitate the replication process.

Another example of an one-to-many replication includes adding a secondary, or passive, Replication Engine to support the existing Replication Engine and to provide a high availability configuration. The primary Replication Engine and

the secondary Replication Engine form an active-passive cluster. The first Replication Engine in each clustered pair is in active mode. The second Replication Engine in each clustered pair is in passive mode, ready to take over if the active Replication Engine should fail.

A full high availability configuration consists of a cluster of two Replication Engines and the primary Oracle FS System on the primary site. The secondary site contains a cluster of two Replication Engines and the secondary Oracle FS System. High availability is not required at both sites. You can configure any Replication Engine as high availability by adding another Replication Engine.

### Related Links

*Replication Configurations*
*Oracle MaxRep for SAN Components*

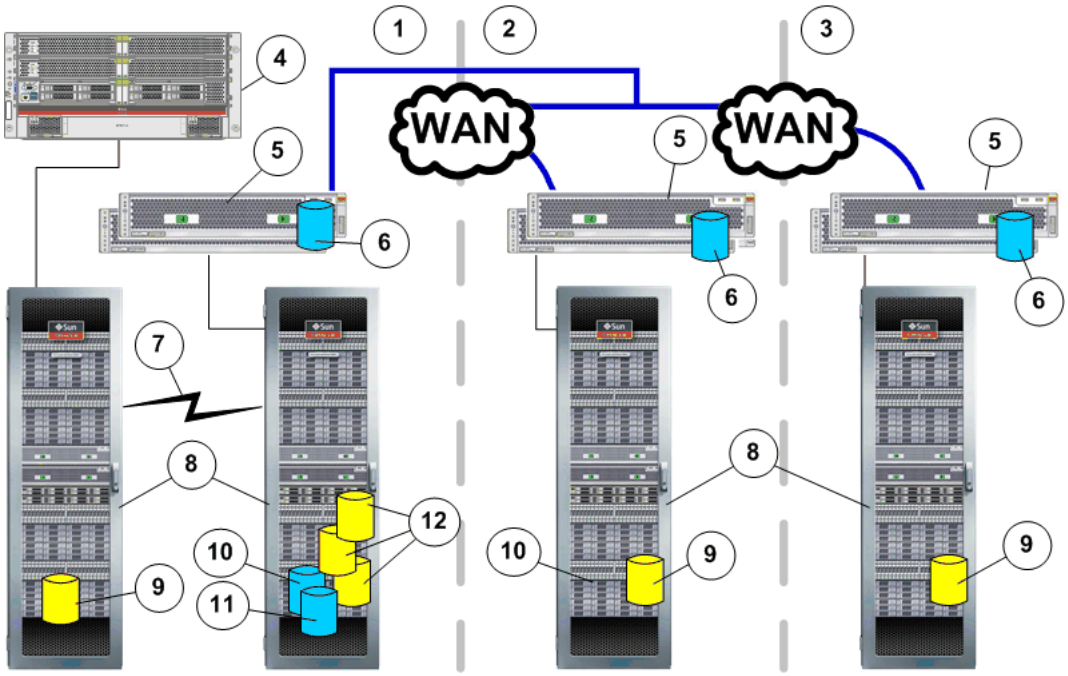
## Many-to-One Replication

Many-to-One replication provides the capability to replicate data from multiple source Oracle FS Systems to a single target Oracle FS System. The many-to-one configuration is useful for a consolidated disaster recovery facility across the enterprise, or for the consolidating data for backup purposes.

For example, a many-to-one replication configuration may consist of primary and secondary sites connected by the same extended SAN fabric that uses dense wavelength division multiplexing (DWDM), and another remote site connected to the primary through a WAN.

The SAN fabric connection permits remote synchronous replication while the WAN connection permits remote asynchronous replication to the target Oracle FS Systems. Refer to the Oracle MaxRep for SAN release notes for the recommended limits for remote asynchronous configurations.

**Figure 10: Basic configuration for many-to-one replication**




**Legend**

| | |
|---|---|
| 1 Primary site | 7 DWDM connectivity |
| 2 Secondary site | 8 Oracle FS System |
| 3 Site “N” | 9 Source LUN |
| 4 Host | 10 Retention LUN |
| 5 Replication Engine | 11 Backup LUN for configuration file |
| 6 Home LUN | 12 Target LUNs |

Another example of many-to-one replication includes adding a secondary, or passive, Replication Engine to support the existing Replication Engine and to provide a high availability configuration. The primary Replication Engine and the secondary Replication Engine form an active-passive cluster. The first Replication Engine in each clustered pair is in active mode. The second Replication Engine in each clustered pair is in passive mode, ready to take over if the active Replication Engine should fail.

### Related Links

*Replication Configurations*
*Oracle MaxRep for SAN Components*

CHAPTER 2

# Configure Oracle FS Systems and Servers

## Oracle FS System and Server Configuration

Before you configure Oracle MaxRep for SAN, you will need to set up your Oracle FS Systems for replication and install the necessary Oracle MaxRep agent on the application server that will be accessing or managing the Oracle MaxRep Replication Engine.

Initially, you need to configure the source and target LUNs for your replication pairs on your Oracle FS Systems, and, if you are using application consistency, install the Oracle MaxRep agent on your application servers. Use the Oracle MaxRep agent if you have application servers that need application consistency checks. If you do not have application servers to protect, then Oracle MaxRep for SAN provides crash consistent recovery.

### Related Links

*Oracle MaxRep Agents*
*Create an Administrator Account*

### Create an Administrator Account

Create additional accounts to allow other administrator to perform various tasks on the Oracle FS System.

1. From Oracle FS System Manager (GUI), navigate to **System** > **Global Settings** > **Administrator Accounts**.
2. Select **Actions** > **Create**.
3. Enter the name of the account in the **Login Name** field.
4. Select a role from the **Role** list.

   **Note:** Refer to the **Administrator Account Description** that is provided on the dialog for a full description of each role.
5. Enter the remaining information about the account owner.

   Additional information:

| | |
|---|---|
| **Required** | **Password**<br>**Confirm Password** |
| **Optional** | **Full Name** |

**Email Address** *(highly recommended)*
**Phone Number**

**Important:** Setting the email address is crucial should a password expire. If you do not enter an email address for an administrator account, administrators cannot reset their own passwords using the **Reset password** feature. Furthermore, if the password for the primary administrator account or for the Oracle Support account is changed from the factory setting, the changed password has been forgotten, and the email address is not configured, you will need to contact Oracle Customer Support for assistance.

6 (Optional) To disable the account, select the **Disable Account** option.

Use the **Disable Account** option when you want to create accounts that you want to enable later.

7 Click **OK**.

### Related Links

*Source and Target LUNs*
*Oracle MaxRep Administrator Accounts*
*Create an Oracle MaxRep User Account*

## Oracle MaxRep Agents

The Oracle MaxRep agents provide file system and application consistency protection for data that is hosted by Windows, Solaris, or Linux servers. The agents enable Oracle MaxRep for SAN to replicate consistent application data by tagging the data with consistency bookmarks.

Oracle MaxRep for SAN ships with the agent from the original equipment manufacturer (OEM). If you require additional information or an agent software package for a specific operating system, please contact your account representative.

Oracle MaxRep for SAN supports application consistency agents for standalone and clustered applications.

Table 4: Supported agents for standalone applications

| Application consistency | Application | Operating system |
|---|---|---|
| Oracle | Oracle 11g R2 | Solaris 10 U9<br>RHEL5-U5 |
| Microsoft Exchange | Exchange 2007<br>Exchange 2007 SP1<br>Exchange 2007 SP2<br>Exchange 2007 SP3<br>Exchange 2010<br>Exchange 2010 SP1 | Windows 2003<br>Windows 2003 SP2<br>Windows 2008<br>Windows 2008 R2<br>Windows 2008 R2 SP1 |
| Microsoft SQL server | SQL 2005<br>SQL 2005 SP1<br>SQL 2005 SP2<br>SQL 2005 SP3<br>SQL 2005 SP4<br>SQL 2008<br>SQL 2008 SP1<br>SQL 2008 SP2<br>SQL 2008 SP3<br>SQL 2008 R2<br>SQL 2008 R2 SP1<br>SQL 2008 R2 SQ2 | Windows 2003<br>Windows 2003 SP2<br>Windows 2008<br>Windows 2008 R2<br>Windows 2008 R2 SP1 |
| Fileserver | Not applicable | Windows 2003<br>Windows 2003 SP2<br>Windows 2008<br>Windows 2008 R2<br>Windows 2008 R2 SP1 |

Table 5: Supported agents for clustered applications

| Application consistency | Application | Operating system |
|---|---|---|
| Oracle | Oracle 11g R2 + VCS 5.1 | Solaris 10 U9<br>RHEL5-U5 |
| Microsoft Exchange | Exchange 2007<br>Exchange 2007 SP1<br>Exchange 2007 SP2<br>Exchange 2007 SP3<br>Exchange 2010<br>Exchange 2010 SP1 | Windows 2008 Cluster<br>Windows 2008 R2 Cluster<br>Windows 2008 R2 Cluster SP1 |

Table 5: Supported agents for clustered applications (continued)

| Application consistency | Application | Operating system |
|---|---|---|
| SQL | SQL 2005<br>SQL 2005 SP1<br>SQL 2005 SP2<br>SQL 2005 SP3<br>SQL 2005 SP4<br>SQL 2008<br>SQL 2008 SP1<br>SQL 2008 SP2<br>SQL 2008 SP3<br>SQL 2008 R2<br>SQL 2008 R2 SP1<br>SQL 2008 R2 SQ2 | Windows 2008 Cluster<br>Windows 2008 R2 Cluster<br>Windows 2008 R2 Cluster SP1 |
| Fileserver | Not applicable | Windows 2008 Cluster<br>Windows 2008 R2 Cluster<br>Windows 2008 R2 Cluster SP1 |

### Related Links

*Oracle MaxRep Agent Settings*
*Monitor Replication Engine Communication*
*Verify Oracle MaxRep Agent Installation*
*Display Host Logs*

## Oracle MaxRep Agent Settings

Allows you to configure the Oracle MaxRep Replication Engine agents.

To view the agent settings from the Oracle MaxRep for SAN GUI, navigate to **Settings** > **Settings** > **Agent Settings**.

### Agent Settings

**Server**

Indicates the primary and secondary Oracle FS System.

**Agent Type**

Indicates the type of agent installed on the Oracle FS System.

**Agent Timeout**

Indicates the number of seconds the agent waits before sending notification alerts to the users.

**Replication Engine IP for File Agent**

Identifies the IP address of the Replication Engine.

**Replication Engine NAT IP**

Identifies the IP address of the Replication Engine Net Address Translation (NAT) table.

**Alias**

Allows you to provide an easily understood, alternate name for the Replication Engine.

**Save**

Allows you to keep the changes made to the screen.

### Process Service

**IP Address**

Identifies the name and IP address of the process service.

**NAT IP Address**

Identifies the IP address of the process service Net Address Translation (NAT) table.

**Save**

Allows you to keep the changes made to the screen.

### Retention Reserve Space Setting

**Unused space**

Allows you to specify the amount of storage to allocate for LUN retention.

### Related Links

*Verify Oracle MaxRep Agent Installation*
*Display Host Logs*

## Install Oracle MaxRep Agents

### Install an Oracle MaxRep Agent on Windows

Enable the creation of bookmarks by installing the Oracle MaxRep agent on a Windows Server.

**Prerequisites**

- The Windows Server 2008 Application Server Role has been added to the **Role Services** dialog box on the Windows Server.
- The **Incoming Remote Transactions** (IRT) check box has been selected. The IRT is used by the Microsoft Distributor Transaction Coordinator (MSDTC) to install the MS.Net Frameworks required for MSDTC.
- A Cluster has been created.
- MSDTC has been configured.

1. Save the Oracle MaxRep agent `*.exe` file to your desktop.
2. Double-click the file, then select **Run**.
3. To allow the program to make changes on your computer, click **Yes**.
   The Oracle Agent Setup Wizard window appears.
4. Click **Next**.
5. To install the Oracle MaxRep agent in the current folder, click **Next**. To select an alternative folder, click **Browse** and navigate to the appropriate folder.
6. Click **Install**.
   The Oracle Agent Config window appears.
7. In the **IP Address** box, enter the IP address for the control service Replication Engine.
8. Click **OK**.
   The Oracle Agent Setup Wizard completes the installation.
9. When the Completing the Oracle Agent Setup Wizard window appears, click **Finish**.
   The Oracle MaxRep agent installation is complete.

### Install an Oracle MaxRep Agent on Solaris

**Prerequisites**

You have root privileges to install the Replication Engine.

1. Save the Oracle MaxRep agent binary file to your desktop.
2. Navigate to the command-line interface on your operating system.
3. At the command line, uncompress the binary file using the `gunzip` and `tar` commands. For example, `gunzip <tarname>; tar -xvf <file name>`.
4. Run the command `./install`.
   Result: You receive a prompt to agree to the license terms and conditions.
5. Type `Y`.
   Result: You receive a prompt to select an installation location for the agent.
6. Press **Enter**.
   Result: The host agent configuration interface displays.
7. Enter the IP address of the Replication Engine, then press **Enter**.
8. Enter the HTTP port number of the Replication Engine, then press **Enter**.
   Result: You are asked if you would like to start the File Agent.
9. Type `Y`.
   Result: The Oracle MaxRep agent has been installed successfully.

### Install an Oracle MaxRep Agent on Linux

**Prerequisites**

You have root privileges to install the Replication Engine.

1. Save the Oracle MaxRep agent binary file to your desktop.
2. Navigate to the command-line interface on your operating system.
3. At the command line, uncompress the binary file using the `gunzip` and `tar` commands. For example, `gunzip <tarname>; tar -xvf <file name>`.
4. Run the command `./install`.
   Result: You receive a prompt to agree to the license terms and conditions.
5. Type `Y`.
   You receive a prompt to select an installation location for the agent.
6. Press **Enter**.
   The host agent configuration interface displays.
7. Enter the IP address of the Replication Engine, then press **Enter**.
8. Enter the HTTP port number of the Replication Engine, then press **Enter**.
   You are asked if you would like to start the File Agent.
9. Type `Y`.
   The Oracle MaxRep agent has been installed successfully.

## Uninstall Oracle MaxRep Agents

### Uninstall an Oracle MaxRep Agent on Windows

When application consistency is no longer required for data that is hosted on Windows, uninstall the Oracle MaxRep agent from your Windows operating system.

1. Navigate to **Start > Control Panel > Programs and Features**.
2. From the list that is presented, locate and highlight the Oracle MaxRep agent file you want to uninstall.
3. Right-click the file, then select **Uninstall**.
   Result: An Oracle Agent Uninstall window appears to confirm the action.
4. Click **Yes**.
   Result: A message informs you that uninstallation may take a while.
5. Click **OK**.
   Result: When the uninstallation process is complete, a message is presented confirming that the Oracle MaxRep Agent was successfully removed from your system.

### Uninstall an Oracle MaxRep Agent on Solaris

When application consistency is no longer required for data that is hosted on Solaris, uninstall the Oracle MaxRep agent from your Solaris operating system.

1. From the Solaris command-line interface, enter the change directory command to locate the Oracle MaxRep agent you want to uninstall, then press **Enter**. For example, `cd /usr/local/InMage/Fx/`.
2. Type `./uninstall`, then press **Enter**.
   A message displays asking you to confirm the uninstallation.
3. Type `Y`, and press **Enter**.
   The command-line interface will display a message that states FileAgent uninstallation successful.

### Uninstall an Oracle MaxRep Agent on Linux

When application consistency is no longer required for data that is hosted on Linux, uninstall the Oracle MaxRep agent from your Linux operating system.

1. From the Linux command-line interface, enter the change directory command to locate the Oracle MaxRep agent you want to uninstall, then press **Enter**. For example, `cd /usr/local/InMage/Fx/`.
2. Type `./uninstall`, then press **Enter**.
   A message displays asking you to confirm the uninstallation.
3. Type `Y`, and press **Enter**.
   The command-line interface will display a message indicating that the FileAgent uninstallation was successful.

## Upgrade Oracle MaxRep Agents

### Upgrade an Oracle MaxRep Agent on Windows

Ensure that your Windows operating system is running the latest Oracle MaxRep agent software version by following the agent upgrade prompts from the agent setup program.

**Prerequisites**

To avoid the possibility of replication failures, ensure that replication is not in process during the Oracle MaxRep agent upgrade.

When an updated version of an Oracle MaxRep agent is available, you receive a notification from the agent setup program when you run the agent installer.

1. From your Windows operating system, double-click the agent installer.
   You are asked if you would like to proceed with the upgrade of the Oracle MaxRep agent.
2. Click **Yes**.
   You are shown a message that informs you to be patient as the process may take a while.

3 Click **OK**.
You are shown a second message that the next step in the process may take a while.

4 Click **OK**.
The Oracle MaxRep agent setup wizard appears.

5 Click **Next**.

6 Select **I accept the agreement**, then click **Next**.

7 To install the agent upgrade in the default folder, click **Next**. To select an alternative folder, click **Browse** and navigate to the appropriate folder.

8 Click **Install**.

9 In the Host FX Agent Config window, enter the IP address and HTTP port number for the Replication Engine.

10 Navigate to **Log On**, and select **This Account**.

11 Enter the **Login Name** and **Password**, and click **OK**.

12 Click **Finish**.
The upgrade is complete.

## Upgrade the MaxRep Agent on Solaris

Ensure that your Solaris operating system is running the latest Oracle MaxRep agent software version by following the agent installer upgrade prompts at the command-line interface.

**Prerequisites**

To avoid possible replication failures, ensure that replication is not in process during the Oracle MaxRep agent upgrade.

1 Through the change directory command at the command line, type in the Oracle MaxRep agent binary file name, then press **Enter**.

2 To uncompress the binary file, run `gunzip <tarname>; tar -xvf <file name>`, then press **Enter**.

3 Run `./install`.

4 Type `u`, then press **Enter**.
A message displays that states the File Agent service is stopped completely. You are asked if you would like to start File Agent.

5 Type `Y`, then press **Enter**.

## Upgrade an Oracle MaxRep Agent on Linux

Ensure that your Linux operating system is running the latest Oracle MaxRep agent software version by following the agent installer upgrade prompts at the command-line interface.

**Prerequisites**

To avoid possible replication failures, ensure that replication is not in process during the Oracle MaxRep agent upgrade.

1. Through the change directory command at the command line, type in the Oracle MaxRep agent binary file name, then press **Enter**.
2. Run `tar - xvzf <binary file name>`, then press **Enter**.
3. Run `./install`.
4. Type `u`, then press **Enter**.
   A message displays that states the File Agent service is stopped completely. You are asked if you would like to start File Agent.
5. Type `Y`, then press **Enter**.

## Push Installation or Upgrade of Agents

Configure settings in the Oracle MaxRep for SAN GUI to push installations and upgrades to Oracle MaxRep agents.

1. In the Oracle MaxRep for SAN GUI, navigate to **Settings > Agent Installers > Push Install or Upgrade Agents > Install Agent**.
2. Select the Push Server for installation, then click **Next**.
3. Select the **Linus/UNIX OS** type.
4. To select servers, enter the IP address, or IP Range, then click **Submit**.
5. Navigate to **Upgrade Agents**, and select the **Push Server to Upgrade**.
6. Click **Next**.
7. Select the Remote Server to upgrade, then click **Next**.
8. Click **Install**.
9. Enter the **Use Name** and **Password** for the remote server.
10. Select the **Agent Features**.
11. Select the **Build/Rollup** for the remote server.
12. If a reboot is required, select the box for **Reboot Required**, then click **Next**.
13. Review your settings, then click **Submit**.

## Oracle MaxRep Agent Firewall Configuration

If your Oracle Flash Storage System setup uses a firewall at either the primary LUN or the seconday LUN, ensure that the firewall on your operating system is configured to allow access to the required ports.

Transmission Control Protocol/Internet Protocol (TCP/IP) infrastructure is used for primary site and secondary site data protection. When TCP/IP is used for continuous data protection at the primary site, as with Oracle MaxRep for SAN, the communication of both the data and the configuration happens over the local area network (LAN). When TCP/IP is used to implement a remote Disaster

Recovery (DR) solution, the communication of both the data and configuration happens over both the LAN link and the Wide Area Network (WAN) link.

## Firewall Configuration Settings

The Replication Engine user interface is web-based and can be accessed through an HTTP server running on port 80. The following table summarizes the firewall rules that must be configured:

### Table 6: Firewall configuration

| Purpose | Replication Engine | Primary LUN | Secondary LUN |
|---|---|---|---|
| User Interface | Inbound HTTP | | |
| Default: TCP Port 80 | N/A | N/A | N/A |
| Configuration | Inbound HTTP | | |
| Configuration Management: Port 3306 | N/A | N/A | N/A |
| Default: TCP Port 80 | N/A | N/A | N/A |
| Or TCP (21 + configured passive port range) | N/A | N/A | N/A |
| Or TCP (20 + 21) | Outbound FTP or (>1024) | Outbound FTP or (>1024) | N/A |
| Data resync | Inbound TCP Port 873 | N/A | N/A |
| FX data (Push ) | N/A | N/A | N/A |
| FX data (Pull) | N/A | N/A | N/A |

### Table 7: Firewall configuration during installation

| Purpose | Firewall configuration |
|---|---|
| Linux | VNC server with VNC viewer (Port: 5500)<br>Secure shell (SSH) (Port: 22) |
| Windows | Remote desktop connection or terminal client (3389)<br>PC Anywhere (TCP 5631, UDP 5632) |

## Source and Target LUNs

A replication pair is composed of two LUNs: a source LUN and a target LUN.

In most cases, the source LUN already exists and has been mapped to the host that is using the LUN for production work.

The source LUN can be one of the following:

- An existing LUN that resides on the Oracle FS System.
- A new LUN explicitly set up as the source for a replication pair.

The target LUN must be the same size as or larger than the source LUN.

As part of the replication pair creation, Oracle MaxRep for SAN automatically creates the following items:

- All necessary host associations in the Oracle FS System.
- Mappings to the Oracle MaxRep Replication Engines for the source and target LUNs.

During replication pair creation, Oracle MaxRep for SAN also removes any existing LUN mappings of the target LUN to other hosts. For data integrity purposes, the target LUN may only be mapped to the Replication Engine.

**Note:** For multi-hop replication, the target LUN is mapped to two Replication Engines in an asynchronous configuration.

### Related Links

*LUN Management*
*Protection Plans*
*Create a Source LUN*
*Create a Target LUN*

## Create a Source LUN

When creating a replication pair, create the source LUN if the LUN does not already exist on the source Oracle FS System.

1. Start the Oracle FS System Manager GUI from the source system for the replication pair.
2. Follow the instructions for creating a LUN in the *Oracle Flash Storage System Administrator's Guide*.

### Related Links

*Source and Target LUNs*
*Create an Administrator Account*

### Create a Target LUN

When creating a replication pair, create the target LUN if the LUN does not already exist on the target Oracle FS System.

The target LUN must be the same size as or larger than the source LUN. Try to create the target LUN at exactly the correct size. Use the same QoS settings and initial requested LUN size for the target LUN as you used for creating the source LUN. This strategy increases the likelihood of the target being exactly the correct size.

**Note:** If the created target LUN is smaller than the source LUN, modify the target LUN and increase the allocated and addressable logical capacities by 1 GB.

1. Start the Oracle FS System Manager GUI from the target system for the replication pair.
2. Follow the instructions for creating a LUN in the *Oracle Flash Storage System Administrator's Guide*.

After you create the target LUN, manage the Oracle storage by rediscovering the LUN in the Support tab of the Oracle MaxRep GUI using the **Manage Oracle Storage** > **Re-Discover** option.

#### Related Links

*Source and Target LUNs*
*Manage Registered Oracle FS Systems*
*Create an Administrator Account*

## LUN Management

The Oracle MaxRep for SAN provides a variety of tools to administer the LUNs that are managed by the Oracle MaxRep Replication Engine.

The following LUN management tools are available from the **Toolkit for MaxRep** option on the **Settings** tab:

**Map**

Allows you to map retention and home LUNs of the registered Oracle FS System to the Replication Engine.

**Unmap**

Allows you to remove the mapping configuration between the registered Oracle FS System and the Replication Engine. You cannot use this option to remove the mappings on a LUN that is a member of protection plan.

**Detect Resize**

After you have resized a LUN that is associated with a replication pair, this option allows you to adjust the size of your LUNs in your protection plan.

**Clear Write Splits**

Allows you to clear the write split on a LUN that cannot be used in a protection plan.

### Related Links

*Source and Target LUNs*
*LUN Protection Monitoring*
*Detect Resizing of the Home and Retention LUNs*
*Detect Resizing of a Source LUN*
*Detect Resizing of a Target LUN*
*Map LUNs*
*Unmap LUNs*
*Clear Write Splits*

## Map LUNs

Use the Map LUNs feature to map retention, backup, and optional home LUNs. You can also map LUNs that are used for any physical backup copies of a replicated pair.

**Prerequisites**

Before you map a LUN, consider the following points:

- When mapping a LUN, the Oracle FS System deletes any existing host mappings for the LUN.
- Oracle MaxRep for SAN supports third- and fourth-level Linux file systems (*ext3* and *ext4*). The Linux operating system journals the file system so that these file systems might be recovered in the event of data corruption.
- A LUN is always mapped to an appliance initiator for the target (AIT) port group. The AIT port group is used to access the retention and backup LUNs, and optionally the home LUNs, that are mounted on the Replication Engine.

**Note:** The Map LUN feature is not used to map source or target LUNs that are used in replication pairs. These LUNs are mapped automatically during the Create Protection Plan process.

You can format and mount a LUN, mount the LUN if it is already formatted, or map and initiate the scanning from Oracle MaxRep for SAN.

1. Navigate to **Settings** > **Oracle Storage** > **Toolkit for MaxRep**.
2. In the Select MaxRep Option page, select **Map** and click **Next**.
3. From the **Select Oracle Storage** list, choose the Oracle FS System containing the LUN that you want to map.

4 Select the Replication Engine from the **Select MaxRep** list.
The **Select LUNs for Mapping** table lists the available LUNs.

5 Expand the entry for the Oracle FS System containing the LUN.

6 Select the LUNs for mapping and click **Next**.
A warning message displays stating that if the LUN is already mapped, your actions unmaps the selected LUN.

7 For locally-used LUNs, such as retention, backup, or an optional home file system, provide the **Mount Point** path. After mapping the LUN, the system mounts the LUN to the provided path.

8 Specify the **Format Required** option. Select this option if you want the system to format the LUN after mapping.

**Note:** A LUN must be formatted to mount properly.

**Caution:** Formatting removes any filesystem data from the LUN.

9 For locally-used LUNs, such as retention, backup, or an optional home file system, specify whether to **Map to Physical FC Ports**.

**Note:** Oracle recommends this option for the retention, backup, and optional home LUNs.

10 Select the **Filesystem** protocol that is support by the operating system.

**Note:** Oracle recommends that you use the preferred file system (*ext4*) for local (retention, backup, and optional home) LUNs.

11 To initiate the mapping, click **Submit**.

To view the status of the operation, navigate to **Settings** > **Oracle Storage** > **Toolkit for MaxRep**, and click **Show History**. The Status column shows the state of the operation: Pending, In Progress, Success, or Failure.

### Related Links

*LUN Management*
*Source and Target LUNs*
*FC Initiator and Target Ports*
*Unmap LUNs*

## Unmap LUNs

Use the Unmap option to remove LUN mappings from the Oracle MaxRep Replication Engine.

The Oracle MaxRep Replication Engine lists the LUNs that meet the following criteria:

- LUNs that are mapped using the Map LUN option from the Toolkit for MaxRep.
- LUNs that are not members of a protection plan.

1. Navigate to **Settings** > **Oracle Storage** > **Toolkit for MaxRep**.
2. In the Select MaxRep Option page, select **Unmap** and click **Next**.
3. From the **Select Oracle Storage** list, choose the Oracle FS System containing the LUN that you want to unmap.
4. Select the Replication Engine from the **Select MaxRep** list.
   The **Select LUNs for Mapping** table lists the available LUNs.
5. Expand the entry for the Oracle FS System containing the LUN.
6. Select the LUNs for unmapping and click **Next**.
7. Click **Submit**.

To view the status of the operation, navigate to **Settings** > **Oracle Storage** > **Toolkit for MaxRep**, and click **Show History**. The Status column shows the state of the operation: Pending, In Progress, Success, or Failure.

### Related Links

*LUN Management*
*Source and Target LUNs*
*Map LUNs*

## Detect Resizing of the Home and Retention LUNs

Oracle MaxRep for SAN allows you to scan the retention and home LUNs for capacity changes and reflect those changes in the protection plans.

1. Navigate to **Settings** > **Oracle Storage** > **Toolkit for MaxRep**.
2. In the Select MaxRep Option page, select **Detect Resize** and click **Next**.
3. From the **Select Oracle Storage** list, select the Oracle FS System that contains the source LUN for the replication pair to be resized.
4. Expand the entry for the Oracle FS System containing the LUN.
5. From the LUN navigation tree, select the home or retention LUN.

   **Tip:** Click the + sign to expand the list of available LUNs.

   **Note:** The Select LUN Scan Options table only lists the LUNs that are used in replication pairs.
6. After selecting the LUN, click **Next**.
7. Confirm that the correct LUN is selected, and then click **Submit**.
   The system displays the **Policy History for LUN Resize** page.
8. Verify that the **Policy History** status shows **Pending**, followed by **Success**.
9. Click the **Monitor** tab and review the **Alerts and Notifications** for possible errors.

To view the status of the operation, navigate to **Settings** > **Oracle Storage** > **Toolkit for MaxRep**, and click **Show History**. The Status column shows the state of the operation: Pending, In Progress, Success, or Failure.

### Related Links

*LUN Management*

## Detect Resizing of a Source LUN

Modifying the size of the source LUN requires that you update the source LUN size in your protection plan. Use the Toolkit for MaxRep to adjust the size of the source LUN of your protection plan.

When resizing replication pair LUNs, resize the LUNs in the following order:

- Resize the target LUNs
- Detect the target LUN resize in the Oracle MaxRep for SAN GUI
- Resize the source LUN
- Detect the source LUN resize in the GUI

Modify the size of your LUN by following the procedure that is described in the *Oracle Flash Storage System Administrator's Guide*.

1. Navigate to **Settings** > **Oracle Storage** > **Toolkit for MaxRep**.
2. In the Select MaxRep Option page, select **Detect Resize** and click **Next**.
3. From the **Select Oracle Storage** list, select the Oracle FS System that contains the source LUN for the replication pair to be resized.
4. Expand the entry for the Oracle FS System containing the LUN.
5. From the LUN navigation tree, select the source LUN of the replication pair.

   **Tip:** Click the **+** sign to expand the list of available LUNs.
6. After selecting the LUN, click **Next**.
7. Confirm that the correct LUN is selected, and then click **Submit**.
   The system displays the **Policy History for LUN Resize** page.
8. Verify that the **Policy History** status shows **Pending**, followed by **Success**.
9. Click the **Monitor** tab and review the **Alerts and Notifications** for possible errors.

If the system displays the following error, then follow the procedure to resize and detect the resize of the target LUN.

```
The source Device (/dev/mapper/...) has been reconfigured upon resize and the
following replication pair is paused. Please resize your target LUN to greater
than or equal to the source LUN  and then resume the replication pair.
```

### Related Links

*LUN Management*

*Detect Resizing of a Target LUN*

## Detect Resizing of a Target LUN

Oracle MaxRep for SAN allows you to scan the target LUNs for capacity changes and reflect those changes in the protection plans.

When resizing replication pair LUNs, resize the LUNs in the following order:

- Resize the target LUNs
- Detect the target LUN resize in the Oracle MaxRep for SAN GUI
- Resize the source LUN
- Detect the source LUN resize in the GUI

Modify the size of your LUN by following the procedure that is described in the *Oracle Flash Storage System Administrator's Guide*.

1. Navigate to **Settings** > **Oracle Storage** > **Toolkit for MaxRep**.
2. In the Select MaxRep Option page, select **Detect Resize** and click **Next**.
3. From the **Select Oracle Storage** list, select the Oracle FS System that contains the source LUN for the replication pair to be resized.
4. Expand the entry for the Oracle FS System containing the LUN.
5. From the LUN navigation tree, select the target LUN of the replication pair.

   **Tip:** Click the + sign to expand the list of available LUNs.

   **Note:** The Select LUN Scan Options table only lists the target LUNs that are used in replication pairs.
6. After selecting the LUN, click **Next**.
7. Confirm that the correct LUN is selected, and then click **Submit**.
   The system displays the **Policy History for LUN Resize** page.
8. Verify that the **Policy History** status shows **Pending**, followed by **Success**.
9. Click the **Monitor** tab and review the **Alerts and Notifications** for possible errors.

If necessary, resume data protection of the replication pair.

To view the status of the operation, navigate to **Settings** > **Oracle Storage** > **Toolkit for MaxRep**, and click **Show History**. The Status column shows the state of the operation: Pending, In Progress, Success, or Failure.

### Related Links

*LUN Management*
*Detect Resizing of a Source LUN*

## Clear Write Splits

If you have a LUN that is configured on an Oracle FS System and is removed from a replication pair, you might need to clear the write split on that LUN.

When you create a protection plan, the source LUN might already contain a write split. The **Clear Write Split** option clears the write split, which allows you to resume creating the protection plan.

**Note:** A LUN that is blue contains a write split. In the Oracle MaxRep for SAN GUI, navigate to **Protect > Oracle Storage > View Oracle Storage** to view LUNs associated with the system.

1. Navigate to **Settings** > **Oracle Storage** > **Toolkit for MaxRep**.
2. In the Select MaxRep Option page, select **Clear Write Splits** and click **Next**.
3. Enter the **Password** for the current login session.
4. Select the Oracle FS System from the list.
5. Select the Replication Engine from the list.
   The system displays a list of available LUNs.
6. Select the affected LUNs, then click **Force Delete**.

### Related Links

*LUN Management*

CHAPTER 3

# Configure Oracle MaxRep for SAN

## Initial Configuration

The Oracle MaxRep software is pre-installed on your Oracle MaxRep Replication Engines.

Refer to the *Oracle MaxRep for SAN Hardware Guide* for information about hardware installation and initial software installation.

Initial configuration of Oracle MaxRep for SAN includes these tasks:

- Set up user accounts.
- Configure the Replication Engine HBA ports.
- Register your Oracle FS Systems.
- Configure the Replication Engine settings.
- Configure any remote Replication Engines, if installed.
- Install the Oracle MaxRep for SAN license on the Replication Engine where the control service runs.

### Related Links

*Oracle MaxRep Administrator Accounts*
*FC Initiator and Target Ports*
*Oracle FS System Registration*
*Oracle MaxRep Replication Engine Settings*
*Remote Replication Engine Configuration*
*Capacity-Based Licenses and Features*

## Oracle MaxRep Administrator Accounts

The Oracle MaxRep for SAN software has a built-in default administrator account. You can create as many additional administrator and monitor accounts as you want.

The default Oracle MaxRep for SAN administrator account has full administrator privileges. Users with Administrator roles have full access to all the functions of the software. Only an administrator user can create, delete, or edit user accounts.

Users with the Monitor role have limited access to the Oracle MaxRep software. Monitor role privileges include:

- No access to the functions on the Protect tab
- Full access to the functions on the Monitor tab
- No access to the functions on the Recover tab
- Limited access to the functions on the Settings tab

### Related Links

*Create an Oracle MaxRep User Account*
*Create an Administrator Account*
*Log In to an Oracle MaxRep Replication Engine*

## Create an Oracle MaxRep User Account

You can create new administrator or monitor user accounts for the Oracle MaxRep for SAN system.

Use the Add User Account page to create either an administrator user account or a monitor user account.

**Note:** For security reasons, Oracle recommends that you create a separate account for each administrator of the Oracle MaxRep system. Then you can grant the appropriate administrator access rights to each user. Oracle does not recommend the practice of sharing login credentials, nor does Oracle recommend that all administrators log in to the default **admin** user account.

The user roles have the following restrictions:

- Administrator role can edit any user account.
- Monitor role can modify only a few account settings such as their passwords.

1. Navigate to **Settings** > **User Management** > **Manage Users**.
   The **Manage Users** table appears with a list of current users.
2. Click **Add User Account**.
3. Enter the **Full Name** of the new user.
   A **UID** (unique ID) is automatically generated for the user account.
4. Enter a **User Name** for the new user. The user name is used to log into the Oracle MaxRep system.
5. (Optional) To allow this user administrator privileges, select **Admin Access**.

   **Note:** The Administrator role provides the user full access to all Oracle MaxRep functions. Users with the Monitor roles have limited access.
6. To authenticate the user, select **Local database**.

   **Note:** The Microsoft AD (Active Directory) authentication service is disabled in Oracle MaxRep, so **Local database** is the only available option.

7 Enter (and re-enter) a **Password** for the user.

8 Enter an **E-mail Address** for the user.

This is the email address that the Replication Engine uses to deliver email alerts to this user.

9 Click **Save**.

### Related Links

*Oracle MaxRep Administrator Accounts*
*Edit a User Account*
*Delete a User Account*

## Log In to an Oracle MaxRep Replication Engine

To use the Oracle MaxRep for SAN software, you must first log in to an Oracle MaxRep Replication Engine.

1 In the browser address field, enter the IP address or the name of the Replication Engine.
For example,

```
http://10.24.192.154
```

2 Enter the appropriate credentials at the login page.

For the default administrator account, use the following:

- **Username**: **`admin`**
- **Password**: **`password`**

3 Click **Login**.

### Related Links

*Oracle MaxRep Administrator Accounts*
*Edit a User Account*
*Delete a User Account*
*Change Replication Engine Replication Password*

## Change Oracle FS System Replication Password

Change the Oracle FS System replication password when the password expires. This is the password that the Replication Engine uses to access the Oracle FS System.

**Prerequisites**

The IP address or domain name server (DNS) of the Oracle FS System that is registered to the Oracle MaxRep Replication Engine.

For security purposes, the replication password on the Oracle FS System expires on a regular basis, depending on the policies maintained by the system

administrator. The replication account has limited privileges on the Oracle FS System. Change the password from the Oracle FS System Manager GUI.

1. Log in to the Oracle FS System Manager GUI using the primary administrator user name and password.
2. From the **System** tab, click **Global Settings** > **Administrator Accounts**.
3. Select the account name *replication* from the Administrator Accounts list.
4. Click **Actions** > **Modify**.
5. Enter the new password in both of the **Password** and **Confirm Password** fields.
6. To save your changes, click **OK**.

When the replication account password on the Oracle FS System changes, you must also change the password record on the Replication Engine.

### Related Links

*Oracle MaxRep Administrator Accounts*
*Change Replication Engine Replication Password*

## Edit a User Account

Edit a user account to change passwords, define events for notification, and set user account information.

1. Navigate to **Settings** > **User Management** > **Manage Users**.
   The **Manage Users** table appears with a list of current users.
2. Locate the account name that you wish to edit, click **Edit Account**.
3. Update the necessary fields for this user.
4. (Optional) To test the email address configured for alert notifications, click **Test Mail**.

   **Note:** The **Test Mail** button appears when you have entered an email address.
5. To save your changes, click **Save**.

### Related Links

*Delete a User Account*
*Create an Oracle MaxRep User Account*

## Edit Alert Notification Settings

The alert notification settings specify the alerts that the users receive from the Oracle MaxRep Replication Engine.

You can only edit the alert notifications for the current, logged in user. The primary administrator account does not have the rights to edit the Alerts Notification settings for other users.

1. Navigate to **Settings** > **User Management** > **Manage Users**.
   The **Manage Users** table appears with a list of current users.
2. For the user you wish to edit, click **Settings**.
3. From the **Alert Notification** entry, click **Edit**.
4. From the **Alert Category** list, select the items from which to receive alerts.
   Available alert categories:

   **E-mail**

   Sends alerts to the specified email address.

   **Trap**

   Sends the alerts to the configured SNMP trap.

   **Display in Monitor Page**

   Displays the alerts on the Monitor page.

   **Tip:** To select all of the items in the list, click the checkbox at the top of the column.
5. To save your changes, click **Save**.
6. (Optional) From the **E-mail Subject** field, click **Edit**.
7. (Optional) Enter the new text for the email subject and click **Save**.
8. (Optional) From the **Configured Trap Listeners** field, click **Edit**.
9. (Optional) Enter the new trap listener information.
   - **Trap Listener**
   - **Trap Port**
10. To save your changes, click **Add**.

### Related Links

*Alerts*
*Create an Oracle MaxRep User Account*

## Delete a User Account

Delete a user account when you no longer have a use for it.

Only an administrator user can delete a user account. You cannot delete the default administrator account.

1. Navigate to **Settings** > **User Management** > **Manage Users**.
2. Find the user account you want to delete in the Configured System Users table.
3. Click **Delete** in the Delete column on the same row as the user account.

### Related Links

*Edit a User Account*
*Create an Oracle MaxRep User Account*

## Capacity-Based Licenses and Features

All purchased configurations of Oracle MaxRep for SAN include a capacity-based license. Installation of a license key onto the MaxRep configuration is optional as all replication features within the MaxRep configuration are enabled at the time of installation. If installation of a license key is desired, the installation is performed on the control service Replication Engine. The control service Replication Engine becomes a License Server for all other Replication Engines within the configuration.

Synchronous and asynchronous replication licenses with or without application protection are available for Oracle MaxRep for SAN. The available licenses include the following:

- Synchronous data protection
- Asynchronous data protection
- Synchronous data protection with application consistency
- Asynchronous data protection with application consistency

In addition to enabling the type of replication that is used, each license specifies the data capacity you are authorized to use for replication. Capacity-based licenses are sold in terabyte (TB) increments.

The license you requested when you purchased Oracle MaxRep for SAN comes separately. To obtain your license, contact licensecodes_ww@oracle.com and include your Oracle sales order number.

If you have any questions, or need assistance, contact your Oracle account representative.

### Related Links

*Upload Your Capacity-Based License*
*Apply Your License*

## Upload Your Capacity-Based License

To install, upgrade, or replace your capacity-based license, you need to upload the new license to the Oracle MaxRep Replication Engine on which the control service runs. The control service is the primary service used to configure the replication process and policies.

When you receive your license file, copy it to your local workstation and log in to Oracle MaxRep for SAN GUI on the control service Replication Engine.

**Note:** The IP address for the control service Replication Engine is located on the Monitor page under the Control Service tab.

1. Navigate to **Settings** > **Settings** > **License Management**.
2. In the **License Upload** table, click **Browse**, and navigate to your license file.
3. Navigate to and select the license filename.
4. Click **Upload**.

Your license is installed and ready to be applied to your Replication Engines and to your hosts.

### Related Links

*Capacity-Based Licenses and Features*
*Apply Your License*

## Apply Your License

After you have uploaded your license, you can apply it to your Oracle MaxRep Replication Engine, and to other process service Replication Engines.

Use the Oracle MaxRep for SAN software to apply your license.

1. Navigate to **Settings** > **Settings** > **License Management**.
2. Click the **Apply License** tab.
3. In the **Unlicensed Hosts** table, select the Replication Engine that you want to apply the license, and click **Set License**.
   If you want to apply the license to all the hosts in the **Unlicensed Hosts** table, click **Apply License to All Hosts**.
4. Select the license and click **Apply**.
   The name of the server, the license name, the type of agent, and other details are displayed in the **Licensed Hosts** table.
5. (Optional) To release a license for use on a different Replication Engine or host, select the server in the **Licensed Hosts** table and click **Release License**.

   **Note:** Releasing a license on a Replication Engine deletes any active protection plans on that Replication Engine.

### Related Links

*Capacity-Based Licenses and Features*
*Upload Your Capacity-Based License*

# FC Initiator and Target Ports

The Oracle MaxRep Replication Engine can be configured with Fibre Channel (FC) interfaces to Oracle FS Systems. The following describes configuring FC interfaces.

Before you can create and use protection plans, you must configure the FC ports in the Replication Engine. Configuring the ports is a simple operation, however the following information is useful to understand when there are configuration

issues. Upon installation, all four FC ports are configured as initiator ports. For replication, the Replication Engine requires initiator FC ports for source and target LUNs, and target FC ports.

Replication Engines that are configured for FC connectivity, contain two FC HBAs with two FC ports, for a total of four FC ports.

To provide expanded LUN access support and reduce the number of physical ports required by each Replication Engine, Oracle MaxRep for SAN uses Node Port (or N_Port) ID Virtualization (*NPIV*) to create virtual initiators across two of the FC ports on the installed HBAs.

The Replication Engines are further divided into three types of host bus adapter (HBA) ports.

**Initiator Ports (AIS)**

The default configuration for a port on a Replication Engine is an appliance initiator port for source LUN access (AIS). An initiator port communicates only with zoned target ports within the SAN fabric. After proper configuration, the Replication Engine has four virtualized NPIV ports that are available as AIS ports. Zone the AIS ports to all of the Controller ports on the Oracle FS Systems that are registered to the Replication Engine.

Initiator ports are used for the following communications:

- During resynchronization Step 1 or Step 2 of an initial synchronization, the AIS port is used for read-only access to a source LUN.
- During Step 1 or Step 2 of a resynchronization, the AIS port is used for read-only access to a source LUN.
- In the differential synchronization mode, if the used cache for a protection plan exceeds the Differential File Threshold setting for the protection plan, the AIS port is used for read-only access to a source LUN.
- The AIS port is used to read data from a target LUN during a data recovery.

**Initiator for Target LUN Mapping Ports (AIT)**

The appliance initiator port for target LUN access (AIT) communicates only with zoned target ports within the SAN fabric. Zone the AIT port to all Controller ports on the Oracle FS Systems that are registered to the Replication Engine. After proper configuration, the Replication Engine has four virtualized NPIV ports that are available as AIT ports.

Initiator for target ports is used for the following types of communications:

- Write access to a target LUN during all phases of initial synchronization, resynchronization, and differential synchronization mode.
- Read-write access to the home, back up and retention LUNs on the Oracle FS System.
- Write operations to a source LUN during a data recovery.

**Target Ports (AT)**

An appliance target (AT) port communicates only with zoned initiator ports within the SAN fabric. After proper configuration, the Replication Engine has two physical ports that are available as AT ports. The zoned initiator ports include the following:

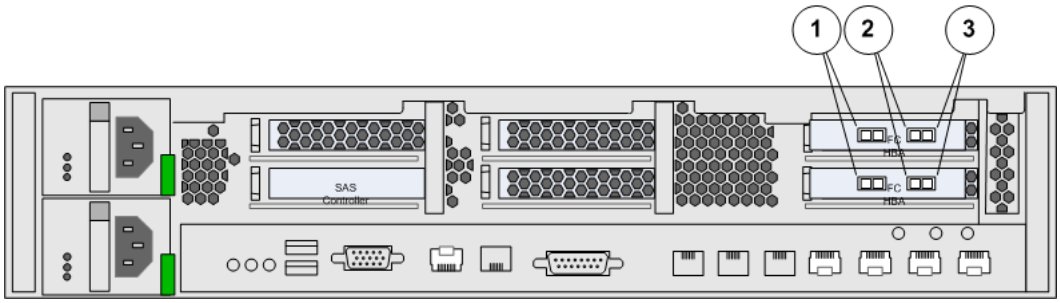
- All Controller ports from the Oracle FS Systems that are registered to the Replication Engine.
- Any hosts that mount virtual snapshots that are exported from the Replication Engine.

Target ports are used for the following types of communications:

- During the differential synchronization mode, the AT port accepts writes to a source LUN by way of the splitter driver on the Controller of the primary Oracle FS System.
- After a virtual snapshot is exported to a host, the host accesses the virtual snapshot through the AT port.

*NPIV* provides multiple virtual ports form a single physical FC port. NPIV does not create virtual ports across multiple physical ports. On each HBA, port 1 is used as the physical ports for four virtualized AIS and four virtualized AIT ports. All 16 total (8 AIS and 8 AIT) virtualized NPIV ports are configured on these two physical ports. The Replication Engine uses port 2 on each HBA as a dedicated AT port.

Figure 11: Replication Engine physical FC ports and virtual ports




**Legend**

| | |
|---|---|
| 1 AT ports | 3 AIT, virtual ports 1-8 |
| 2 AIS ports, virtual ports 1-8 | |

For more information on zoning and SAN fabric management, refer to the SAN switch user manuals for your SAN fabric.

**Note:** SAN best practices should always be followed. Best practice is always single initiator to single target zoning, or single initiator to multiple target zoning. Do not configure a zone containing multiple initiators.

**Note:** The fabric that the Replication Engines are connected to must support NPIV and have NPIV enabled on the ports that the Replication Engines are connected to.

### Related Links

*How Oracle MaxRep for SAN Works*
*Supported Fabric Zoning*
*Verify All FC Ports Discovered as Initiator Ports*

## Verify All FC Ports Discovered as Initiator Ports

During the initial installation, all FC ports on the Oracle MaxRep Replication Engine are configured as initiator ports. You need to verify that all HBA ports on the Replication Engine are discovered and are configured as initiator ports.

Verifying that all FC ports on the Replication Engine appear in the Initiator Ports table validates that the hardware has been detected properly.

1. Navigate to **Settings** > **Advanced Configuration** > **Replication Engine Ports Configuration**.
2. Expand the entry for the Replication Engine you are configuring.
3. Verify that all FC ports appear in the Initiator Ports table.

   **Note:** Contact Oracle Customer Support if any ports are missing from the Initiator Ports table.

### Related Links

*FC Initiator and Target Ports*
*Configure FC Ports*

## Configure FC Ports

After you have verified that the Oracle MaxRep Replication Engine has recognized all of the Fibre Channel (FC) initiator ports, configure the appliance initiator ports for source (AIS) and target (AIT), and the appliance target (AT) ports for use by the Replication Engine.

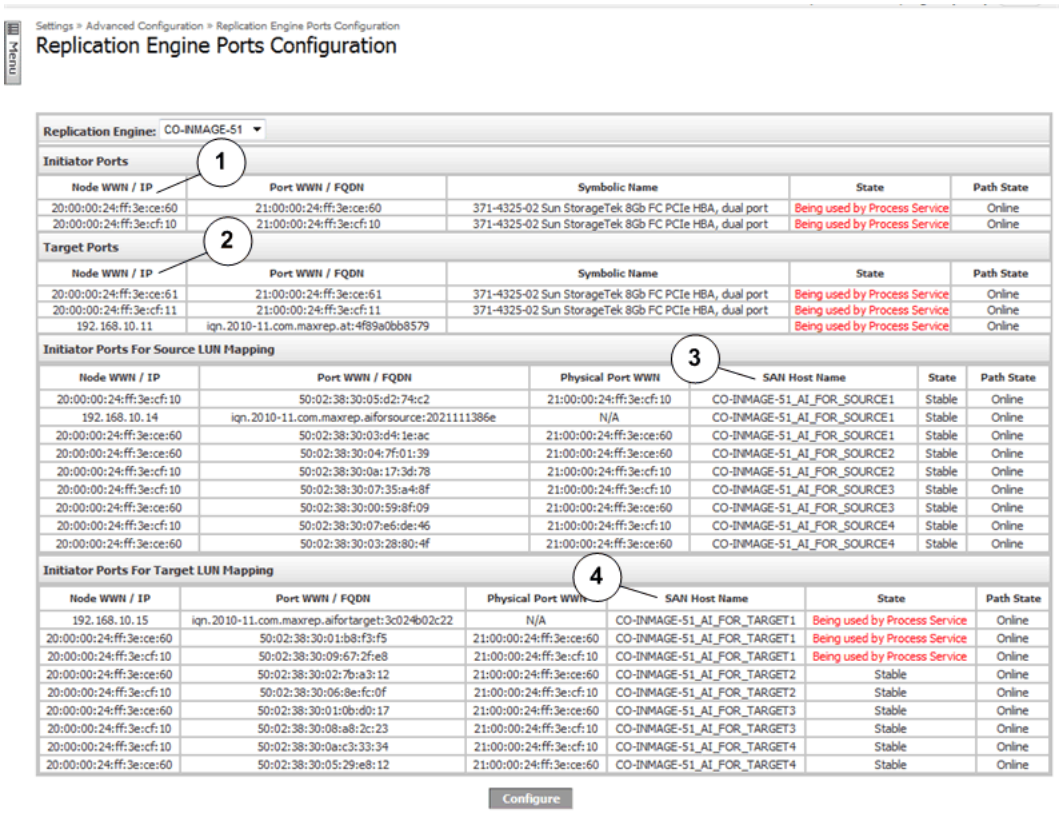
Configuring the FC initiator ports is an automatic process.

1. Navigate to **Settings** > **Advanced Configuration** > **Replication Engine Ports Configuration**.
2. From the **Replication Engine** list, select the Replication Engine that you are configuring.
3. Click **Configure**.
   The system displays the **Replication Engine Ports Configuration** dialog, then updates the table with the target (AT), appliance initiator source (AIS), and appliance initiator target (AIT) ports.
4. Click **Done**.

**Note:** It might take several minutes for this operation to complete. While the system configures the ports, the port state is listed as `Transient Pending`.

The following image illustrates a list of configured FC ports.

**Figure 12: Replication Engine FC port configuration page**




### Legend

| | |
|---|---|
| 1 FC Port 2 world-wide names (WWN) or IP addresses | 3 AIS ports, virtual ports 1-8 |
| 2 FC Port 2 AT ports | 4 AIT ports, virtual ports 1-8 |

### Related Links

*FC Initiator and Target Ports*

*Verify All FC Ports Discovered as Initiator Ports*

## Supported Fabric Zoning

Each Oracle MaxRep Replication Engine ships with two HBAs. Oracle recommends using a separate, redundant, SAN fabric for each HBA.

The following recommendations apply:

- The supported SAN fabric zoning is to zone each HBA port and each NPIV port to each of the Oracle FS System Controller ports.

- Supported configurations is to connect all ports from the first HBA to one SAN fabric, and all ports from the second HBA connected to a separate SAN fabric.

### Related Links

*FC Initiator and Target Ports*
*Verify All FC Ports Discovered as Initiator Ports*

## Oracle FS System Registration

Before the Oracle MaxRep for SAN replicates your data, register your Oracle FS Systems with the Oracle MaxRep Replication Engine.

Registering the Pilot IP addresses of your Oracle FS Systems enables Oracle MaxRep to discover the Oracle FS Systems.

After an Oracle FS System has been registered, LUNs on that system can be used to map retention LUNs or configure protection plans. You can view registered Oracle FS System details or histories, modify registered Oracle FS System addresses and credentials, and unregister previously registered Oracle FS Systems. You can register multiple Replication Engines to a single Oracle FS System.

### Related Links

*View Oracle FS System Details*
*Register the Oracle FS Systems*
*Manage Registered Oracle FS Systems*

### Register the Oracle FS Systems

Register each Oracle FS System that you are using for replication with the Oracle MaxRep Replication Engine.

**Prerequisites**

Password for the Oracle FS System replication account name. For first-time registration, the default password is TwinPeaks.

Each Oracle FS System that you register to the Replication Engine uses a specific account name, *replication*. The replication account performs specific replication functions on the Oracle FS System, such as creating write splits on the LUNs and map LUNs for replication.

Log in to the control service Replication Engine to begin Oracle FS System registration.

1. Navigate to **Settings** > **Oracle Storage** > **Register Oracle Storage**.
2. To register Oracle FS System, enter the **Oracle Storage IP** address.
   Use the IP address of the public interface to the Oracle FS System Pilot.

3 Enter the Oracle FS System **Password**.

4 From the **Process Service** menu, select the IP address of the Replication Engine that will serve as the control service Replication Engine for this Oracle FS System.

5 Click **Submit**.

In the Manage Oracle Storage page, the Oracle FS System that you just registered appears first in the **Deregistered Oracle Storage** table as **Pending**. After the registration task completes, the Oracle FS System appears in the **Registered Oracle Storage** table.

### Related Links

*Oracle FS System Registration*
*View Oracle FS System Details*
*Manage Registered Oracle FS Systems*
*Change Oracle FS System Replication Password*

## Manage Registered Oracle FS Systems

After registering the Oracle FS System with the Oracle MaxRep Replication Engine, you can manage the Oracle FS System from the Oracle MaxRep for SAN graphical user interface (GUI).

The Manage Oracle Storage page provides options that allow you to perform the following activities:

- Discover newly added LUNs.
- Register multiple Replication Engines to a single Oracle FS System.
- Modify the Oracle FS System IP address.
- Update Replication Engine user password.
- Review Oracle FS System information and details.
- Review activity history.

1 Navigate to **Settings** > **Oracle Storage** > **Manage Oracle Storage**.

2 In the **Action** column of the **Registered Oracle Storage** table, choose one of the following:

**View**

Displays the Oracle Storage LUN Explorer page where you can view LUN information from the registered Oracle FS System.

**Re-Discover**

Discovers any LUNs that were created after the selected Oracle FS System was registered. The Replication Engine automatically discovers new LUNs every six hours.

**Unregister**

Removes the selected Oracle FS System from the **Registered Oracle Storage** list.

**Modify**

Changes the IP address or credentials for the selected Oracle FS System.

**Information**

Displays detailed status information about the selected Oracle FS System.

**History**

Displays historical information about the selected Oracle FS System.

### Related Links

*Oracle FS System Registration*
*View Oracle FS System Details*
*Register the Oracle FS Systems*
*Change Oracle FS System Replication Password*

## Change Replication Engine Replication Password

Change the Oracle MaxRep Replication Engine replication password when the Oracle FS System password expires.

**Prerequisites**

The IP address or domain name server (DNS) of the Oracle FS System that is registered to the Oracle MaxRep Replication Engine.

For security purposes, the replication password on the Oracle FS System expires on a regular basis, depending on the policies maintained by the system administrator. Update the Replication Engine password that is registered in the Oracle FS System.

1. Navigate to **Settings** > **Oracle Storage** > **Manage Oracle Storage**.
2. Select **Modify** for the Replication Engine that you need to update.
3. Enter the new **Password**.
4. To save your changes, click **Submit**.

### Related Links

*Oracle MaxRep Administrator Accounts*
*Change Oracle FS System Replication Password*

## View Oracle FS System Details

View details about the Oracle FS System that are registered with an Oracle MaxRep Replication Engine.

To see the Oracle Storage system details navigate to **Protect** > **Oracle Storage** > **View Oracle Storage**.

The Oracle Storage system details are shown in the **Oracle Storage LUN Explorer**. The **Oracle Storage LUN Explorer** (explorer) displays detailed information about the registered Oracle FS Systems and the replication LUNs.

The explorer allows you to perform the following activities:

- Filter the list of Oracle FS Systems to a single Oracle Storage system.
- Collapse the hierarchal tree that displays the LUNs.
- Manage the Oracle FS Systems.
- Update the list of discovered host bus adapter (HBA) ports and available LUNs.
- Scroll through the list of Oracle FS System, HBAs, and LUNs. Selecting an item displays detailed information on the right side of the explorer page.

The **Oracle Storage LUN Explorer** displays the following information in a hierarchical manner:

**Oracle Storage system name**

Identifies the information about the registered Oracle FS System:

- Oracle FS System serial number
- Model number
- IP address

**HBA port worldwide names (WWN)**

Identifies the discovered HBA port WWN. The ports are grouped as follows:

**Unmapped**

Indicates a list of LUNs that are not associated with a SAN host.

**Globally Mapped**

Indicates a list of LUNs that are mapped to more than one SAN host.

**LUN**

Identifies the detailed LUN information. Each LUN in the list contains an icon that identifies the availability status. The following table describes the icons.

**Table 8: LUN availability status icons**

| Icon | Description |
|---|---|
|  | Indicates that the LUN is protected by the current Replication Engine. |
|  | Indicates that the LUN is protected by another Replication Engine and is not available for protection. |
|  | Indicates that the LUN is available for protection. |

### Related Links

*Oracle FS System Registration*
*Manage Registered Oracle FS Systems*
*Register the Oracle FS Systems*

## Oracle MaxRep Replication Engine Settings

The Oracle MaxRep for SAN GUI provides options for configuring the Oracle MaxRep Replication Engine for operational use. Before and after making changes to the Replication Engine, protect your configuration settings with a back up copy.

Oracle MaxRep provides various methods of configuring the Replication Engine, including:

- Backup and restore the Replication Engine settings

  Backs up your Replication Engine configuration to an Oracle FS System so you can restore the Replication Engine configuration after a disruptive update or repair.
- Clear file replication log

  Specifies the maximum age of file replication logs after which they are deleted by the system.
- Drive space warning threshold

  Specifies the percentage of drive space usage that triggers an email alert.
- FTP mode

  Allows you to choose the type of file transfer protocol (FTP) that the Replication Engine uses for file transfers.

### Related Links

*Oracle MaxRep Replication Engine Thresholds*
*Back Up the Replication Engine Settings*
*Restore the Replication Engine Settings*

## Back Up the Replication Engine Settings

After configuring the Oracle MaxRep Replication Engine settings, backup the configuration to a file. You can use the file to restore the configuration settings when necessary.

1. Navigate to **Settings** > **Settings** > **Replication Engine Settings**.
2. In the Backup/Restore Replication Engine Settings table, type the name for the configuration backup file.
3. Click **Backup** to create a new configuration backup.
   The system creates the backup file and allows you save the file to your workstation for safe keeping.
4. From the file download dialog, click **Save**.
5. Select the destination path name to your local workstation, and then click **OK**.

### Related Links

*Oracle MaxRep Replication Engine Settings*
*Restore the Replication Engine Settings*

## Restore the Replication Engine Settings

You can restore the Oracle MaxRep Replication Engine settings to the original location.

1. Navigate to **Settings** > **Settings** > **Replication Engine Settings**.
2. In the Backup/Restore Replication Engine Settings table, click **Browse**.
3. From the Choose File to Upload dialog, navigate to and select the backup file, then click **OK**.
4. Click **Restore** to restore the configuration from a previous backup.

### Related Links

*Oracle MaxRep Replication Engine Settings*
*Back Up the Replication Engine Settings*

## Oracle MaxRep Replication Engine Thresholds

Set the Oracle MaxRep Replication Engine thresholds to alert subscribed users that specific events have exceeded set limits.

The following thresholds can be set in the Replication Engine. Refer to the Description for default settings. Refer to the Location for where to change the settings.

**Note:** Unless otherwise stated, the threshold settings are located on the Add Protection, Replication (Step 3) options page.

### Table 9: Oracle MaxRep Replication Engine threshold settings

| Threshold | Description | Location |
|---|---|---|
| **Resync File** | During initial sync of a protection plan, if either the resync file threshold or the differential file threshold are exceeded, or the cache directory on the Replication Engine exceeds 80% capacity, the LUN pairs enter Data flow controlled mode.<br>In data flow controlled mode, the process of syncing data from the source LUN to the target LUN is slowed in order keep the amount of data being process within predetermined levels and to prevent the Oracle MaxRep cache requirements from exceeding available capacity.<br>The default resync file threshold for a protection plan is 64 GB (65,536MB). | Set the default resync file threshold in the protection plan Replication Options. |
| **Differential** | During initial sync of a protection plan, if either the resync file threshold or the differential file threshold are exceeded, or the cache directory on the Replication Engine exceeds 80% capacity, the LUN pairs enter Data flow controlled mode.<br>In data flow controlled mode, the process of syncing data from the source LUN to the target LUN is slowed in order keep the amount of data being process within predetermined levels and to prevent the Oracle MaxRep cache requirements from exceeding available capacity.<br>The default resync file threshold for a protection plan is 64 GB (65,536MB). | Set the default resync file threshold in the protection plan Replication Options. |
| **RPO** | When the recovery point objective (RPO) exceeds the specified limit, the system sends an email alert to the users who have subscribed to the RPO warning alert. | Set the RPO threshold in the protection plan Replication Options. |
| **Disk Space Warning** | When the disk usage exceeds 80% of the available capacity, the system sends an email alert to the users who have subscribed to the disk space warning alert. | Set the default threshold in **Settings** > **Replication Engine Settings**. |

## Related Links

*Oracle MaxRep Replication Engine Settings*

# Remote Replication Engine Configuration

The Oracle MaxRep Replication Engine that runs the control service is referred to as the control service Replication Engine. The license installed on the control service Replication Engine is applied to any other Replication Engines.

The Remote Replication Engine advanced configuration settings page on the Settings tab lists the remote Replication Engine that have been discovered by the control service.

### Related Links

*Oracle MaxRep Replication Engine Settings*
*Capacity-Based Licenses and Features*
*Configure Remote Replication Engines*
*Verify Remote Replication Engine Connection*
*Apply Your License*

## Configure Remote Replication Engines

Configure the HBA ports on the secondary Oracle MaxRep Replication Engine as initiator ports, initiator ports for target LUN mapping, and target ports.

In a remote replication scenario, complete the following remote Replication Engine setting from the control service Replication Engine.

Set the initiator ports, target ports, and target ports for LUN mapping from the Port Configuration page of the Settings tab.

### Related Links

*FC Initiator and Target Ports*
*Apply Your License*
*Verify Remote Replication Engine Connection*

## Verify Remote Replication Engine Connection

After installing a remote Oracle MaxRep Replication Engine in the system, verify the status of the control service.

1. Navigate to **Settings** > **Advanced Configuration** > **Remote Replication Engine**.
2. Verify that the Replication Engine status displays correctly.
   Valid status includes:

   **Configured Replication Engine**

   Displays when the engine is running the control service.

   **Standby Replication Engine**

   Displays when the engine is not running the control service.

### Related Links

*Remote Replication Engine Configuration*
*Configure Remote Replication Engines*

## Replication Engine Cluster Database Sync

Disable the database synchronization between the Oracle MaxRep Replication Engine cluster when this link is no longer required. Enable the database synchronization, as necessary.

1. Navigate to **Settings** > **Oracle Storage** > **Toolkit for MaxRep**.
2. Navigate to **Settings** > **Advanced Configuration** > **Replication Engine Cluster**.
3. To disable the database synchronization, select **Disable DB Sync**.
4. (Optional) To enable the database synchronization, select **Enable DB Sync**.
5. From the confirmation dialog, click **OK**.

# Remote Replication Engine Backup Protection

A backup protection plan ensures that configuration data on the control service Replication Engine is protected. Asynchronous environments include at least one process service Replication Engine that points to the control service Replication Engine. Create a backup protection plan for the control service Replication Engine and each process service Replication Engine for complete data protection.

### Related Links

*#unique_83*
*#unique_84*

## Map the Backup LUN

Mapping the backup LUN allows you to associate the LUN to a specific mount point and physical FC port. A backup LUN must be mapped to a mount point and physical FC port before you can create a backup protection plan.

**Prerequisites**

- A designated backup LUN exists on the Oracle FS System or the Pillar Axiom system.
- The Oracle MaxRep Replication Engine has been registered to the Oracle FS System or the Pillar Axiom system that hosts the backup LUN. Refer to the *Oracle MaxRep for SAN User's Guide* for Release 3.0 for Replication Engine registration instructions.
- The world-wide names (WWNs) in the Fibre Channel switch Name Server match the Node Port ID Virtualization (NPIV) connection status in the Oracle FS System or system GUI, confirming that the Replication Engine and Oracle FS System FC zoning has been verified.

1. In the Oracle MaxRep for SAN GUI, navigate to **Settings > Oracle Storage > Toolkit for MaxRep**.
2. From the Select MaxRep Option screen, select the **Map** option, then click **Next**.
3. From the Select LUNs for Mapping screen, navigate to the Select Oracle Storage menu, and then select the Oracle FS System or the Pillar Axiom system that is hosting the backup LUN.
4. From the Select MaxRep menu, select the Oracle MaxRep Engine to which the backup LUN is mapped.
5. In the LUN list that displays, scroll to the bottom and expand the **UnMapped** list.
6. Click the check box that is next to the appropriate backup LUN, verify the name and LUN ID (LUID), then click **Next**.

   **Note:** If the backup LUN does not display in the LUN list, perform the following actions:

   a) Navigate to the Settings tab and click **Manage Oracle Storage**.

   b) In the Registered Oracle Storage table, locate the Oracle FS System or Pillar Axiom system that is hosting the backup LUN.

   c) Click the corresponding **Re-Discover** action.

   d) Wait until the storage rediscovery task completes, and then restart the LUN mapping procedure at Step 1.
7. When the Select Options for Mapping page is displayed, enter the path to the mount point for the backup LUN.
8. Ensure that **Map to Physical FC Ports** is selected.

   **Note:** If the backup LUN is not mapped to the physical ports, the backup protection plan will not be created successfully.
9. Click **Submit**.

The Policy History for LUN Mapping screen displays. The status of the LUN is Success.

**Note:** If the status of the LUN you mapped reads Pending, wait a few minutes, then refresh your screen.

After you have mapped the backup LUN, create the backup protection plan.

## Create a Backup Protection Plan

Having a backup protection plan in place helps to ensure that the data on a control service Replication Engine or on a process service Replication Engine is

protected. Configuring a backup plan allows you to back up configuration data through scheduled intervals that enable automatic, continous data protection.

1. In the Oracle MaxRep for SAN GUI, navigate to **Settings > Advanced Configuration > Configure Replication Engine Backup**.
2. From the Select MaxRep drop-down list, select the Replication Engine that you mapped and mounted.

   **Note:** Each Replication Engine that has been configured for asynchronous replication needs to have its own backup LUN mapped and mounted before the Replication Engine is included on the drop-down list.
3. In the Configure Replication Engine Backup Job screen, fill in the required fields under Select LUNs for Backup.

   **Note:** For **Schedule Interval**, schedule Replication Engine backup protection to run, at minimum, once each day.
4. Click **Save**.
5. Click the **Protect** tab.
6. Click **More**, then click **Manage Protected Files/Folders** to verify that the Replication Engine backup protection plan that you created exists.
7. When the protection plan list is displayed, click the icon next to the plan to view the configuration details and manage the protection plan as needed.

The Manage Protected Files/Folders displays, from which you can select and manage the backup protection plan that you created.

CHAPTER 4

# Configure Data Protection

## Protection Plans

Create a protection plan to configure the protection of one or more replication pairs.

If an application or a collection of data (called *data sets*) contains several volumes that need to be replicated, and the same protection policies apply to each of these volumes, you can place the replication pairs for those volumes in the same protection plan. If the volumes in other applications or data sets require different protection policies, you can create separate protection plans for these volumes.

Protection plans make it possible to apply different protection policies to different groups of replication pairs and to apply policy changes to the entire group at one time.

> Example:
>
> Because volumes of data associated with application A have the same protection requirements, you can group the replication pairs for these volumes together in the same protection plan. Because volumes associated with application B have different protection requirements, you can include the replication pairs for these volumes in a different protection plan.
>
> When you need to make a protection policy change such as a performance improvement change for volumes associated with application A, you can make that change once to the performance plan rather than making the same change to each replication pair individually. The replication pairs in the application B protection plan are unaffected.

### Related Links

*Application Consistency Protection Plans*
*Protection Plan Creation*
*Data Protection Plan Management*

# Protection Plan Creation

Data protection plans specify the parameters for replication. Creating a protection plan is the same process for a synchronous or asynchronous Oracle MaxRep for SAN system.

Creating a protection plan is a five-step process:

- Select the source LUNs
- Select the target LUNs
- Specify the replication options
- Define the retention policies
- Activate the protection plan

### Related Links

*Application Protection Monitoring*
*Protection Plan Prerequisites*
*Create a Data Protection Plan*
*Register the Oracle FS Systems*

## Protection Plan Prerequisites

Before creating a protection plan, ensure that your system is ready to replicate your LUNs.

Verify that you have addressed the following items in your system:

**Oracle FS Systems**

- For synchronous replication, register the source and target Oracle FS Systems with the same Oracle MaxRep Replication Engine.
- For asynchronous replication, register the source Oracle FS System with the primary Replication Engine, and register the target Oracle FS System with the secondary Replication Engine.

**Replication Engine ports**

Configure the Replication Engine ports with at least one of each of the following port types:

- Initiator ports
- Initiator ports for target LUN mapping
- Target ports

Zone the Replication Engine ports to the Oracle FS System Controller ports.

- For synchronous replication, all four physical HBA ports and all 16 NPIV ports of the Replication Engine must be zoned to each SAN port of the primary and secondary Oracle FS Systems.

- For asynchronous replication, all four physical HBA ports and all 16 NPIV ports of the primary Replication Engine must be zoned to each SAN port of the primary Oracle FS System, and all four physical HBA ports and all 16 NPIV ports of the secondary Replication Engine must be zoned to each SAN port of the secondary Oracle FS System.
- Oracle strongly recommends single initiator to single target zoning as a best practice. Note that single initiator zoning is always a requirement.

**Table 10: Supported zoning methods**

| Zoning method | Oracle best practice | Supported? |
|---|---|---|
| Single initiator to single target | Yes | Yes |
| Single initiator to multiple targets | No | Yes |
| Multiple initiators to multiple targets | No | No |

**Retention LUN**

Configure a retention LUN to an appropriate size and ensure that it is mapped to the target Replication Engine using the Toolkit for MaxRep option under the Settings tab.

**Source and Target LUNs**

Identify the source and target LUNs that form the replication pairs.

**Note:** The protection plan removes any host mappings of a target LUN. Mappings to source LUNs are not affected by the protection plan.

### Related Links

*Protection Plan Creation*

*Create a Data Protection Plan*

## Create a Data Protection Plan

Creating a protection plan starts with selecting your source LUNs from the primary Oracle FS System.

Log into the control service Oracle MaxRep Replication Engine to create your protection plan.

1. Navigate to **Protect** > **Oracle Storage** > **Create Protection Plan**.
2. Provide a name for the protection plan, and then click **Next**.
3. From the Add Protection page, enter a description for the plan.
4. Select the primary Oracle FS System from the **Select Oracle Storage** list. After you select the Oracle FS System, the Select Primary LUN table provides you with a list of available primary LUNs.

5 From the **Select Primary LUNs** list, select each source LUN to protect.

**Note:** A check mark displays next to the LUN name of the selected LUN.

6 (Optional) Select the Network Address Translation IP (NAT IP) option for either source or target.

Valid options:

**Use Primary Replication Engine NAT IP address for Source**

When the primary Oracle FS System and the Replication Engine are in different networks, enable this option to establish communication between the primary Oracle FS System and the Replication Engine. You also need to update the Replication Engine NAT IP address in the Agent Settings page.

**Use Primary Replication Engine NAT IP address for Target**

When the Replication Engine and the secondary Oracle FS System are placed in different networks, you need to update the NAT IP of the Replication Engine's NAT IP in the Agent Settings page and enable this option. This option establishes communication between the Replication Engine and the secondary Oracle FS System.

7 Click **Next**.

To continue creating the protection plan, select the target LUNs.

**Note:** At some point, you might delete a protection plan either intentionally or in error. If you want to recreate a protection plan that has been deleted, and use the same name as the deleted plan, you might receive an error message `Protection plan name already exists`, which will prevent you from performing the task of recreating the plan. If you receive this error message, wait one hour before attempting to recreate the protection plan, then try again.

### Related Links

*Protection Plans*
*Protection Plan Creation*
*Protection Plan Prerequisites*
*Select Target LUNs*

## Select Target LUNs

After you select the source LUNs, select the corresponding target (secondary) LUNs from the target Oracle FS System.

1 From the **Secondary Oracle Storage** list, select an Oracle FS System.

**Important:** Do not select **Allow smaller sized targets to select**. This option is reserved for data recovery.

2 In the **Select Secondary LUNs** table, choose the secondary LUN.

Possible methods:

**Select**
Displays a list of available LUNs.

**Use Best-fit LUNs**
Allows the system to choose the secondary LUN.

3 (Optional) Select the Network Address Translation IP (NAT IP) option for either source or target.

Possible options:

**Use Secondary Replication Engine NAT IP address for Source**
When the primary Oracle FS System and the Replication Engine are in different networks, enable this option to establish communication between the primary Oracle FS System and the Replication Engine. You also need to update the Replication Engine NAT IP address in the Agent Settings page.

**Use Secondary Replication Engine NAT IP address for Target**
When the Replication Engine and the secondary Oracle FS System are placed in different networks, you will need to update the NAT IP of the Replication Engine's NAT IP in the Agent Settings page and enable this option. This option establishes communication between the Replication Engine and the secondary Oracle FS System.

4 Click **Next**.

To continue creating the protection plan, select the replication options.

### Related Links

*Source and Target LUNs*
*Create a Data Protection Plan*
*Select the Options for Replication*

## Select the Options for Replication

After you select the source and target LUNs, you can set various options for the replication pairs that are controlled by the protection plan.

1 (*Asynchronous replication*) Click the **Secure data transfer from Primary Replication Engine to Secondary Replication Engine** checkbox.

2 Specify the number of concurrent pairs to resynchronize in the **Batch Resync** field.

3 To automatically resynchronize your protection plan, in the event that a resynchronization is necessary, set the time frame in the **Start automatic resync** field.
Choose a time that has minimal impact on system resources. For example, during off hours or after business hours.

**Note:** Not setting a time frame will require manual intervention if the protection plan requires resynchronization.

4 Verify the **Sync options**.

Depending on the type of replication, the system automatically selects the sync option:

- **Direct Copy** for synchronous replication
- **Fast Copy** for asynchronous replication

5 (*Asynchronous replication*) Select the **Compression** option.
Valid options:

- **Disable**
- **Enable**

6 Set the **Resync File Threshold**. In most cases, the default setting of 16 GB (16,384 MB) is sufficient.

**Note:** Setting the **Resync File Threshold** too high might have a negative impact on available Replication Engine resources. Setting the threshold too low might result in increased recovery point objective (RPO) times during high data loads.

7 Set the **RPO Threshold** to limit on how much data can be in the source Replication Engine cache before switching from data mode to metadata mode.
When the pair falls behind synchronous mode, the Replication Engine starts sending alerts to the administrator.

8 (Optional) Set the **Differential File Threshold** as directed by Oracle Customer Support. In most cases, the default setting of 64 GB (65,536 MB) is sufficient.

9 Click **Next**.

To continue creating the protection plan, define the retention policy.

### Related Links

*Replication Options*
*Define Retention Policy*
*Create a Data Protection Plan*

## Replication Options

You can configure the replication pairs for different patterns of replication through the Oracle MaxRep for SAN protections plan options.

Available replication options include the number of pairs to resynchronize simultaneously and compressed data transfer from the primary Oracle MaxRep Replication Engine to the secondary Replication Engine. These options are described in the following list.

**Note:** The synchronous or asynchronous configuration of the Replication Engines determines the available replication options. Not all options are available for all configurations.

**Secure data transfer from Primary Process Service to Secondary Process Service**

Encrypts data before transferring it to a process service Replication Engine.

Important: Because encrypted transmissions can have performance penalties when compared to unencrypted transmissions, we do not recommend encryption in cases where the WAN link between the source and target storage is a dedicated secure WAN. Enable encryption if you are using a public common carrier for WAN attached asynchronous replication.

**Batch Resync**

Specifies the number of replication pairs in a protection plan that are resynchronized simultaneously.

For example, if the batch resynchronization value is 2 and you have four pairs in a protection plan, resynchronization starts for two of the pairs while the other two pairs remain in a **Queued** state. After the pair reaches differential sync, the next pair starts step 1 of the resynchronization process. The recovery point originates only from the resynchronization start time, not the pair configuration time.

**Automatic Resync Options**

Specifies whether to correct any replication data inconsistencies automatically. When an inconsistency occurs, a warning message displays on the Alerts and Notifications panel of the Monitor page and the pair is marked as resynchronized required.

When you enable the **Automatic Resync Option** and set the **Resync required** option to **Yes**, the system waits for a specified period of time (by default it is 30 minutes) before performing a forced resynchronization within the **Start between hours** time frame. This wait ensures data consistency and minimizes manual intervention.

Note: When the **Automatic Resync Option** is not configured for a protection plan, manual intervention will be required if resynchronization is required.

**Sync Options**

Sync options define how the Replication Engines ensure that the data on the source and target LUNs initially synchronize with one another. If the source and target LUNs do not synchronize, these LUNs can return to a synchronized state in the future.

**Fast Sync**

Performs a faster resynchronization than the basic resynchronization at the cost of using more CPU resources on the primary server.

Note: The Fast Sync option is only available for asynchronous configurations.

The Fast Sync option specifies that Oracle MaxRep reads a data block on the source LUN and calculates the unmatched data in a hash. The system then reads the same blocks of data on the target LUN and

calculates a corresponding hash. The hash is transferred over the network between the source and target Replication Engines.

If the data hashes match, no data is transferred to the target LUN. When the data hashes do not match, the data is transferred over the network between the Replication Engines.

This process minimizes the network traffic between the systems and can greatly reduce resynchronization times because only differing data are transmitted between the Replication Engines.

**Direct Copy**

Copies data directly between source and target LUNs without requiring verification.

**Note:** The Direct Copy option is only available for synchronous configurations.

This option is available when both source and target LUNs are accessible from the same Replication Engine or clustered high availability pair of Replication Engines. A direct copy occurs only in synchronous replication configurations.

**Compression**

Defines whether compression is used for data transmitted across the WAN. Because compression can consume valuable system resources on the Replication Engines, Oracle recommends that you use the Replication Engines only in asynchronous replication environments across a limited bandwidth WAN. For sizing considerations, contact Oracle Customer Support.

Data compression effectiveness varies widely depending on the type of data being compressed. Typically, you can plan on the compression ratios for various data types as defined in the following table.

**Table 11: Compression ratios by file type**

| File type | Compression ratio |
|---|---|
| General files | 2:1 |
| Database | 4:1 |
| Graphics and media | 1:1 |
| Messaging, such as email | 4:1 |

**Resync File Threshold**

Specifies the folder size of the threshold resynchronization cache. When the resynchronization cache folder exceeds this size, the data transfer rate between the source and target LUNs is throttled. The default value is 16 GB.

**Note:** Setting the Resync file threshold too high might have a negative impact on available system resources on the Replication Engines. Setting the

threshold too low might result in increased recovery point objective (RPO) times during high data loads.

**Differential File Threshold**

Specifies the folder size of the threshold differential synchronization cache. When the differential cache folder exceeds this size, the data transfer rate between the source and target LUNs is throttled. The default value is 65 GB for all LUNs except for LUNs with high data change rates.

**Note:** Do not set the Differential File Threshold option unless directed by Oracle Customer Support.

**RPO Threshold**

Specifies the threshold recovery point objective (RPO) in minutes. The RPO represents the maximum amount of time that the replication pair is allowed to fall behind synchronous mode. If RPO increases beyond this limit, the Oracle MaxRep system sends a message to the GUI interface. This setting has no affect on replication.

**Note:** Do not set the RPO Threshold option unless directed by Oracle Customer Support.

### Related Links

*Application Consistency Protection Plans*
*Data Protection Plan Management*
*Select the Options for Replication*

## Define Retention Policy

The final step in creating a protection plan is to define a retention policy, which specifies how long to keep your protected data.

The amount of space required by the retention policy varies widely and depends on the following factors:

- The amount of data being replicated
- The change rate of that data
- The amount of time that the replicated data is stored
- Whether sparse retention is used

Define your retention policy in the **Retention Policy** and **Specify Retention Storage Path** sections of the Add Protection page.

1. From the Retention Policy table, define the initial Continuous Data Protection (CDP) retention window in the **Retain all data for** field.

   This field indicates the period of time to maintain write fidelity between the source and target LUNs. Enter a number and specify whether it is the number of hours, days, weeks, months, or years. This number indicates the period during which you would like to keep all data changes. The exact

length of time defined for this setting is dictated by the application recovery requirements, but typically is limited to 48 hours, or less.

2 Select **Retain only bookmarks for older data** if you want to keep sparse data for data older than the initial CDP retention window.

By retaining just the bookmarks, the Oracle MaxRep Replication Engine maintains only the historical write data to restore the LUN to specific defined points in time rather than saving every write that occurs on the LUN in the retention log.

3 Specify the amount of storage space for the retention logs in the **Restrict retention storage space to** field.

Use this storage space restriction to not allow protected LUNs within a single protection plan to take an unnecessary proportion of the retention log space.

**Note:** To specify how the system processes the **Restrict retention storage space to** warning, set the **On insufficient storage space** option.

4 Select the insufficient storage space option from the **On insufficient storage space** list.

Valid choices:

- **Purge older retention logs**
- **Pause replication**

When there is insufficient storage space, you can purge older retention logs or pause replication. For synchronous replication, Oracle recommends that you select **Purge older retention logs**. In the event that the Oracle MaxRep Replication Engine deletes older retention logs, the system sends an alert indicating that the retention window is not being met.

5 On the **Alert when storage space utilization reaches** field, set the threshold for sending an alert when retention logs reach a percentage of the available storage.

Oracle recommends keeping the default 80% setting.

6 From the **Storage path** list in the Specify Retention Storage Path table, select a path to the appropriate retention volume.

The volume appears in the **Retention Volumes** table. If the table is empty, check the following:

- Ensure that the retention LUN is created on the target Oracle FS System. In the Oracle MaxRep GUI use the **Settings > Manage Oracle Storage > Re-Discover** option.
- Ensure that the retention LUN is mapped to the secondary Replication Engine. Use the Map LUN option of the Toolkit for MaxRep under the Settings tab.

7 Click **Next**.

To complete the protection plan, save your settings and activate the plan.

### Related Links

*Capacity-Based Licenses and Features*
*Data Protection Plan Management*
*Create a Data Protection Plan*
*Save and Activate a Protection Plan*

## Save and Activate a Protection Plan

The final step in creating a protection plan is to review your settings and save the protection plan. When you save the protection plan, you have the option to activate the protection policies immediately or at a later time.

1. From the Summary page, review the settings in the **Protection Plan** table.
2. In the Protection Details table, review the settings about the primary and secondary LUNs and the Oracle MaxRep Replication Engine.
3. (Optional) To make changes to the protection plan, click **Back**.
4. Save the protection plan settings.

   Valid save options:

   **Save, Activate Later**

   Saves the protection plan without starting the data protection.

   **Save and Activate**

   Saves the protection plan and starts data protection immediately.

After you save the protection plan, the system displays the Manage Protection Plan page. This page allows you to review the progress of the protection plan and edit the plan details, if necessary.

### Related Links

*Protection Plans*
*Data Protection Plan Management*
*Create a Data Protection Plan*

# Application Consistency Protection Plans

When a protected pair contains data from an application that is supported by an Oracle MaxRep agent, the agent can be installed on the host server. The Oracle MaxRep agent creates bookmarks, which are used in the retention log to create an application consistent copy. You can use these bookmarks to roll back the target LUNs to a previous point in time, or you can use the bookmarks to mount virtual snapshots to validate that the replication is working as expected.

Application consistency depends on the following factors:

- Oracle MaxRep agent is installed on the server that accesses the protected LUNs.

**Note:** You can install the Oracle MaxRep agent after you have created the protection plan.

- The Oracle MaxRep agent is registered with the control service Replication Engine.
- The protection plan is created and configured with a consistency policy.
- The application consistency setup is tested with a recovery snapshot.

### Related Links

*Oracle MaxRep Agents*
*Verify Oracle MaxRep Agent Installation*
*Create a Data Protection Plan*

## Verify Oracle MaxRep Agent Installation

Verify that the application host, which is running the Oracle MaxRep agent, is registered with the control service Oracle MaxRep Replication Engine.

1. Log in to the Oracle MaxRep for SAN GUI on the control service Replication Engine that is running the control service.
2. Navigate to **Settings** > **Settings** > **License Management** > **Apply License**.
3. Verify that the name of the host appears in the list of **Licensed Hosts**.

### Related Links

*Oracle MaxRep Agents*
*Oracle MaxRep Agent Settings*

## Create an Application Consistency Protection Plan

By adding a consistency policy to an existing data protection plan, you can specify which data to protect and create bookmarks in the data as roll back targets.

**Prerequisites**
Before you create an application consistency protection plan, you must first create either a synchronous or asynchronous data protection plan.

1. Navigate to **Protect** > **Manage Protection Plan** and locate your previously created data protection plan.
2. Click **Manage Consistency Policy**.
3. Click **Add Consistency**.
4. In the **Consistency Options** table, select the name of the application server from the **Select Host** drop-down list.
5. Select the type of application consistency policy to set up.

**Application Agent**

To protect data for a specific operating system, select one of the following applications:

- Microsoft Exchange Server 2003, 2007, or 2010
- Microsoft SQL Server 2000, 2005, or 2008
- Oracle (Unix/Linux), RAC, CFS

**Other Volumes**

To create consistency bookmarks for a particular volume rather than for a specific application, specify the actual volumes on the host in the field.

6 Click **Save**.
Your consistency policy appears in the **Consistency Policies** list with a command line in the **Consistency Option** column that corresponds to the information you entered in the **Consistency Options** table.

7 Click **Activate** in the **Action** column of the **Consistency Policies** list to activate your consistency policy.

8 Verify that the consistency policy has been activated.

- Navigate to **Monitor** > **File Replication**.
- In the File Protection Status table, expand the consistency policy job that you created.
- Verify that the job **Status** is **Completed** and that the **Start Time** and **End Time** correspond with the creation of your consistency policy.

9 In the host application event log, verify that an event that reports the tag was sent successfully.

Display the properties for the `InMageVssProvider` event, and verify that the bookmark tags were successfully sent to the remote server.

### Related Links

*Application Consistency Protection Plans*
*Create a Data Protection Plan*

## Confirm Application Consistency Virtual Snapshot

Verify that you can roll back to a bookmark on the disaster recovery (DR) side or your network by creating a virtual snapshot and confirming that application consistency bookmarks were created as expected.

1 Navigate to **Recover** > **More** > **Disk/Volume Recovery** > **Create Recovery Snapshots**.

2 Select the replication pair that you want to validate, and then click **Recover**.

3 In the Recovery Options table, select **Using Application consistency** and **Event based** in the Recovery Based On column.

4 Scroll down to verify that bookmarks exist for the replication pairs, and that these bookmarks are marked with green flags in the Accuracy column.

5 Click **Cancel**.

### Related Links

*Application Consistency Protection Plans*
*Create a Virtual Snapshot*

## Data Protection Plan Management

After you have successfully created a protection plan, the Oracle MaxRep for SAN GUI displays the Manage Protection Plan page. This page allows you to view details about the protection plan, check its status, and modify and delete the plan.

To navigate to the Manage Protection Plan page, choose **Protect** > **Oracle Storage** > **Manage Protection Plan**.

### Protection

The Protection table displays information about the protection plan and provides actions that allow you to manage the protection plan properties:

- Display all the protection plans.
- Add protection to an already completed plan.
- Create a recovery scenario for an existing protection plan.
- Manage the consistency policy of a protection plan.
- Modify a protection plan.
- Delete a protection plan.
- Edit the name of a protection plan.
- View the summary of a protection plan.
- Activate and deactivate a protection plan.
- Reactivate a plan.
- Check the current state of a protection plan.

The following buttons allow you to modify the protection plan:

**Add Protection**

Creates protection plans from one or more source LUNs.

You create a one-to-many protection plan when you take any of these actions on an existing plan:

- Add another secondary Oracle FS System.
- Add a target LUN on an existing secondary Oracle FS System.

**Create Recovery Scenario**

Defines the type of recovery scenario for the protection plan. The available scenarios include:

**Create Rollback Scenario**

Allows you to manage the target LUNs that are write protected during replication.

**Create Data Validation and Backup**

Allows you to manage the virtual and physical backups of your data.

**Manage Consistency Policy**

Allows you to create a new application consistency policy and run it or to manage an existing application consistency policy.

**Plan Details**

Displays an overview of the protection plan settings and replication health.

The Protection table shows the following details about the protection plan:

**Protection Type**

Displays the type of protection chosen for the protection plan.

**Servers**

Displays the Replication Engines that are part of protection plan.

**Application**

Displays the chosen application for the protection plan.

**Action**

Provides the following protection plan operations:

**Summary**

Provides a read-only summary of the protection plan. After reviewing the summary, click **Back** to return to the Manage Protection Plan page.

**Activate**

Activates the protection plan.

You can also review the protection plan options and run a readiness check.

From the Manage Protection Plan page you can also activate or reactivate a failed protection plan. Prompts on the page allow you to resolve specific problems with a failed protection plan.

**Modify**

Allows you to make changes to the protection plan. When you click **Modify**, a dialog displays the following options:

**Modify Replication Options**

Allows you to modify the protection plan replication options.

**Modify Retention Policy**

Allows you to specify retention policies for the protection plan.

The retention storage path cannot be altered for a protection plan that is backing up data.

**Pause/Resume Protection**

Allows you to pause, resume, or restart the protection plan.

**Restart Resync**

Allows you to start data protection after the replication has stopped.

If during the protection plan creation process, you selected a secondary Oracle FS System, but did not complete all of the fields in the protection plan, the **Modify** action provides the following protection plan states.

**Create Incomplete**

Indicates that the protection plan is incomplete. Selecting the link allows you to edit the protection plan starting with the last incomplete field.

**Inactive**

Indicates that the protection plan is complete, but not active. Selecting this link allows you to edit all of the protection plan.

**Active**

Indicates that the protection plan is complete, and active.

Selecting this link allows you to edit the protection plan, however, you cannot select a new primary Oracle FS System, or modify the retention storage path.

**Delete**

Allows you to view a protection plan or a protection scenario for deletion. Deleting a protection scenario also deletes any replication pairs managed by the protection plan. This option also allows you to purge the CDP Retention logs.

Note: Deleting a protection plan without purging the retention journal creates legacy journaled data on the retention storage path that the Replication Engine does not release.

This legacy journaled data reduces the available storage capacity for retention journals of other protection plans. Contact Oracle Customer Support for clearing residual journals from the Replication Engine.

A red cross icon **(x)** indicates an incomplete protection plan. Click this icon to delete the plan.

**Deactivate**

Allows you to suspend the protection plan as necessary. This option also allows you to purge the CDP retention logs.

**Activation Status**

Displays the state of the protection plan. For the Inactive status, you can activate the plan using the Activate action. For Incomplete status, you can complete the protection plan creation using the Modify action. Refer to the table below for the appropriate action that is required for each Activation Status.

**Creation Incomplete**

Protection is not fully created. Use the **Modify** action to complete the protection plan.

**Inactive**

The protection plan is completed but not activated. When the plan is not activated, no data protection occurs. Use the **Activate** option to start data protection.

**Active**

The application data is being protected with the protection details and policies. Selecting this status provides you with the following possible actions:

- Modify protection settings
- Delete the protection
- Create a recovery scenario
- Run an existing recovery scenario

**Deactivation Pending**

An administrator has initiated the deactivation of the protection plan. Selecting this status provides you with the **Force Deactivation** link that allows you to force delete the plan.

Note: A force delete will not purge the CDP retention logs and reduces the retention storage capacity that is available for other protection plans.

**Deletion Pending**

An administrator has initiated the deletion of the protection plan. Selecting this status provides you with the **Force Deactivation** link that allows you to force delete the plan.

**Last Modified Time**

Indicates the most recent time that the protection plan was modified.

## Related Links

*Protection Plans*

*Create a Data Protection Plan*

## Display Protection Plan Summary

You can view a summary of an Oracle MaxRep for SAN protection plan. Display this page when you want a quick overview of the protection plan contents.

**Note:** You cannot make changes to the protection plan from the Summary page.

1. Navigate to **Protect** > **Oracle Storage** > **Manage Protection Plan**.
2. From the Protection table, select the protection plan to edit.
3. Click **Summary**.
   The system displays details about the protection plan.

### Related Links

*Data Protection Plan Management*
*Application Protection Monitoring*

## Display Protection Plan Details

You can view the details of an Oracle MaxRep for SAN protection plan. The information includes replication pair health status, retention policies applied to the plan, and any recovery scenarios that are applicable to the protection plan.

This page includes actions to manage the protection plan. Valid actions include:

- Manage a protection plan.
- Manage a recovery scenario.
- View replication pair summary.
- View replication pair details.

1. Navigate to **Protect** > **Oracle Storage** > **Manage Protection Plan**.
2. Select the protection plan to edit from the Protection table.
3. To view the plan details, click **Plan Details**.
   The system displays details about the protection plan.

### Related Links

*Data Protection Plan Management*
*Application Protection Monitoring*

## Activate a Protection Plan

You can create as many protection plans as you like and activate them when you need them. Activation of a protection plan begins replication of the data for the replication pairs included in the plan.

1. Navigate to **Protect** > **Oracle Storage** > **Manage Protection Plan**.
2. Locate the protection plan that you wish to activate from the **Protection** table.

3 From the **Action** column of the protection plan, click **Activate**.

4 From the Summary page, click **Save**.
The **Activation Status** changes to **Prepare Target Pending** for newly created protection plans or to **Active** for existing protection plans you have activated.

### Related Links

*Data Protection Plan Management*
*Create a Data Protection Plan*

## Modify Protection Plan Replication Options

Modify the protection plan replication options when changes are desired to an existing protection plan. Changes might include securing transport to the secondary Oracle FS System or setting automatic resynchronization.

1 Navigate to **Protect** > **Oracle Storage** > **Manage Protection Plan**.

2 Select the protection plan to edit from the Protection table.

3 Click **Modify**.

4 From the Modify Protection Options table, select **Modify Replication Options**.

5 Make the necessary changes in the Replication Options table.

6 To keep your changes, click **Save**.

### Related Links

*Data Protection Plan Management*
*Replication Options*

## Modify Protection Plan Retention Policy

Modify the policy settings for protection plan retention when you want to change the length of time that the Oracle MaxRep Replication Engine should keep the data for the replication pairs or to change the sparse retention settings.

1 Navigate to **Protect** > **Oracle Storage** > **Manage Protection Plan**.

2 Select the protection plan to edit from the Protection table.

3 Click **Modify**.

4 From the Modify Protection Options table, select the **Modify Retention Policy** option.

5 Make the necessary changes in the Retention Policy section of the page.

6 To keep your changes, click **Save**.

### Related Links

*Data Protection Plan Management*
*Define Retention Policy*

## Deactivate a Protection Plan

Deactivating a protection plan suspends replication and allows you to clean the Continuous Data Protection (CDP) logs.

1. Navigate to **Protect** > **Oracle Storage** > **Manage Protection Plan**.
2. Select the protection plan to edit from the Protection table.
3. Click **Deactivate**.
4. Review the protection plan details.
5. (Optional) To clear the contents of the CDP retention logs, click the **Clean CDP Retention logs** checkbox.
6. To suspend replication, click **Deactivate**.

### Related Links

*Data Protection Plan Management*
*Application Protection Monitoring*

## Resync a Protection Plan

Loss of network connection between primary and secondary sites, or other changes in the replication environment might cause the resynchronization process to slow down or stop. Restarting the resynchronization process ensures that the protection plan runs properly.

1. Navigate to **Protect** > **Oracle Storage** > **Manage Protection Plan**.
2. From the Protection table, select the protection plan to edit.
3. Click **Modify**.
4. From the Modify Protection Options table, select **Restart Resync**.
5. Select the protection details as necessary.
6. To restart resynchronization, click **Restart Resync**.

### Related Links

*Data Protection Plan Management*
*Application Protection Monitoring*
*Map LUNs*

## Delete a Protection Plan

Delete a protection plan when it is no longer needed for replication. Deleting a protection plan deletes all the replication pairs that are associated with the plan.

1. Navigate to **Protect** > **Oracle Storage** > **Manage Protection Plan**.
2. Select the protection plan to edit from the Protection table.
3. Click **Delete**.
4. Review the protection plan details.

5 (Optional) To clear the contents of the CDP retention logs, click the **Clean CDP Retention logs** checkbox.

**Note:** Oracle recommends that you select the Clean CDP Retention logs option. When this option is deselected, the Replication Engine does not purge the retention journal, which keeps legacy journaled data on the retention storage path. Keeping the journaled data reduces the overall storage capacity that is available for retention journals of other protection plans. Contact Oracle Customer Support for clearing residual journals from the Replication Engine.

6 To remove the protection plan and any replication pairs, click **Delete**.

### Related Links

*Data Protection Plan Management*
*Application Protection Monitoring*

## Pause or Resume a Protection Plan

You might need to pause the data protection for an indefinite time. When you are ready, you can resume data protection.

1 Navigate to **Protect** > **Oracle Storage** > **Manage Protection Plan**.

2 Select the protection plan to edit from the Protection table.

3 Click **Modify**.

4 From the Modify Protection Options table, select **Pause/Resume Protection**.

5 Select the protected LUNs, as necessary.

6 Change the replication mode.
Valid options:

- **Pause Replication**
- **Resume Replication**

### Related Links

*Data Protection Plan Management*
*Application Protection Monitoring*

## Balance Process Service Loads

When many Oracle MaxRep Replication Engines use a single process service, degraded performance occurs.

You can add additional network interface cards (NICs) to the process server and assign the additional ports to the network. Bandwidth control becomes possible if the Replication Engines use separate NIC cards for communication.

By default all the replication traffic is handled by eth0 Ethernet port.

1. Navigate to **Settings** > **Advanced Configuration** > **Process Server Load Balancing**.
   The Process Service Traffic Load Balancing page displays.
2. Select the replication agent from the **Select Volume Replication Agent** list.

   **Note:** After selecting an item from the list the system displays the details in the **Details** table.
3. Select the process service from the **Select Process Service** from the available list.
4. Select the NIC card that the process service and Oracle MaxRep agent uses from the **Select NIC to Map** list.
5. To save your configuration, click **Save**.
6. When prompted by the system to confirm your settings, click **OK**.
7. (Optional) To delete any of the previously configured mappings, select the mapped item from the **Already Configured Agent-Process Server NIC Mapping** table and then click **Delete**.

### Related Links

*Balance Traffic Loads Settings*
*Oracle MaxRep Agent Settings*
*Display Host Logs*

## Process Service Failover

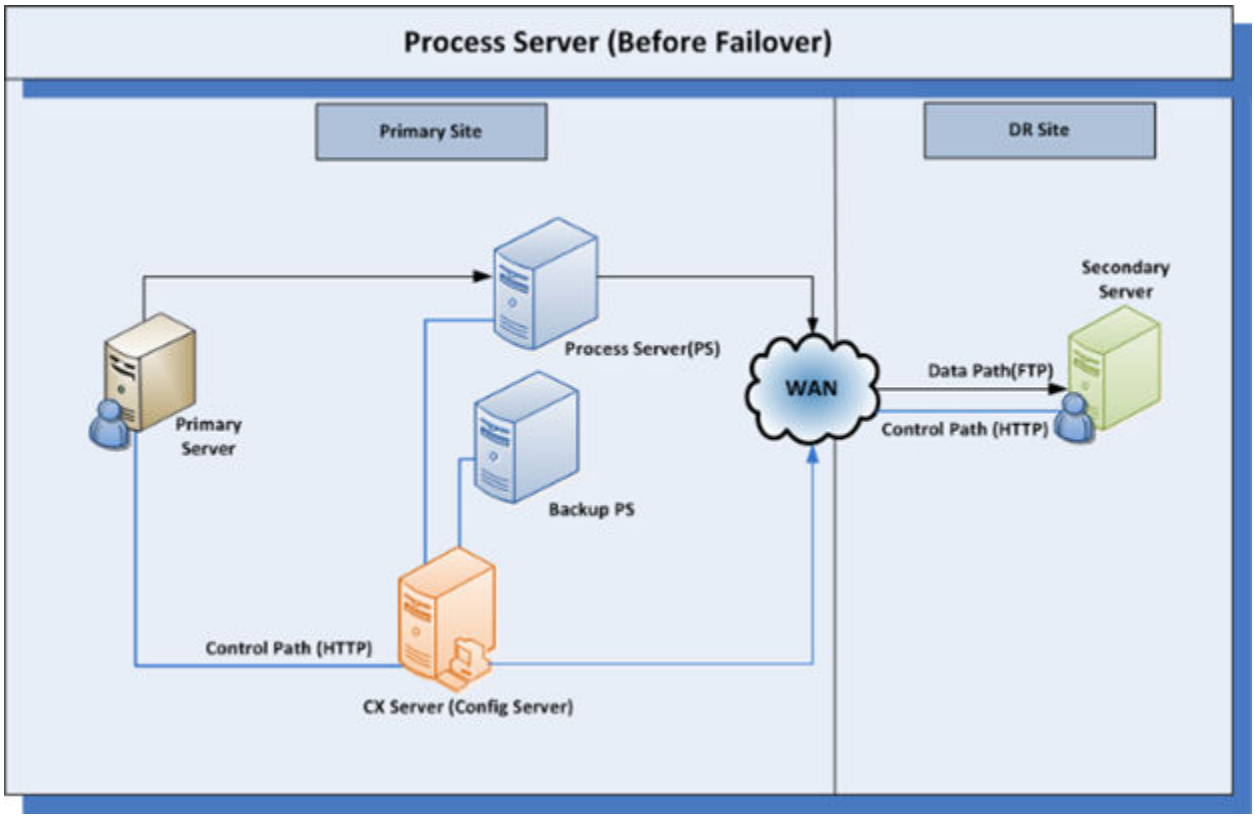
At times, you might need to move replication pairs handled by one process service Replication Engine to another process service Replication Engine. This is called process service failover.

Reasons to for performing a process service failover include:

- A process service Replication Engine is overloaded
- A process service Replication Engine is low on resources
- A process service Replication Engine has gone down or has lost its connection

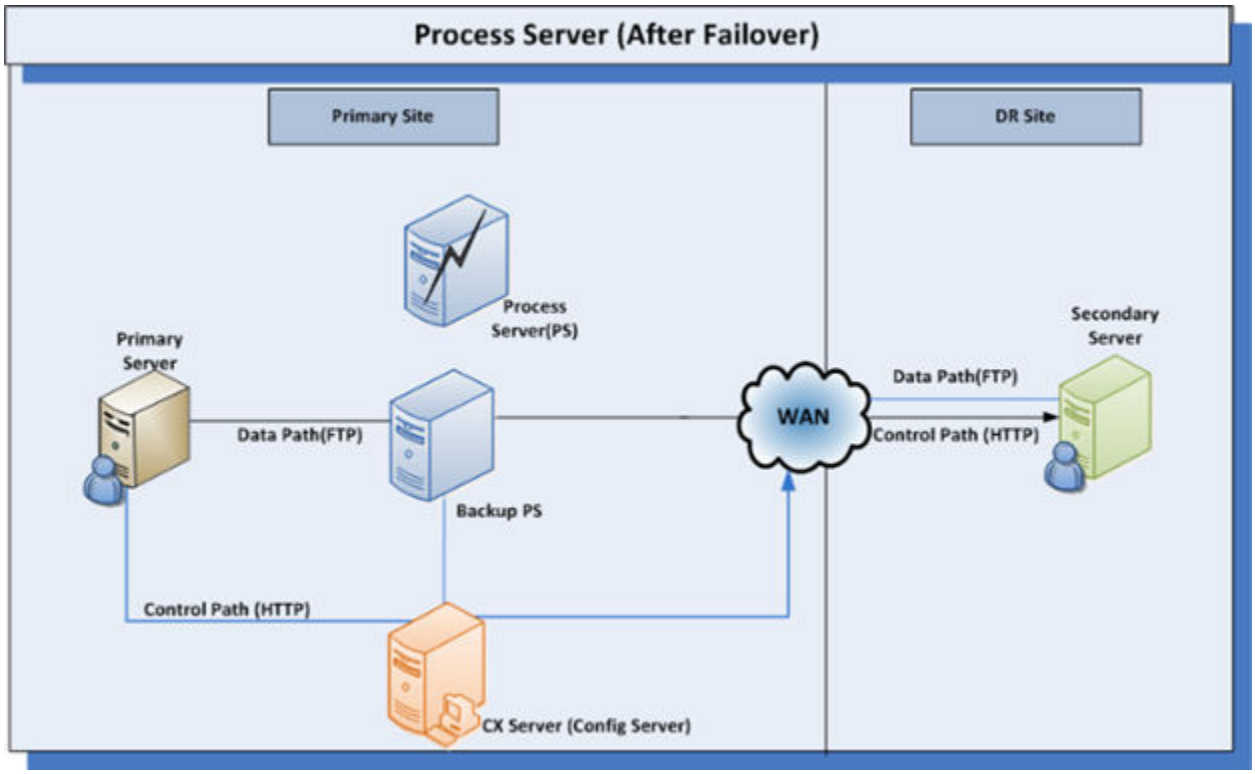
The following figures represent a control service Replication Engine that is communicating with two process service Replication Engines, and production server, and a Disaster Recovery (DR) server.

Figure 13: Process server before failover




In the preceding image, the primary server is actively managing the replication pair, an the backup process server is idle.

Figure 14: Process server after failover




In the preceding image, the primary server is actively managing the replication pair, and the backup process server has taken over the process server, making the backup process server the active process server in the pair.

## Perform a Process Service Failover

Shift a replication pair off one process service Replication Engine onto a backup process service Replication Engine when needed by performing a process service failover.

1. In the Oracle MaxRep for SAN GUI, navigate to **Settings** > **Advanced Configuration** > **Process Service Failover**.
2. In the **Current Process Service** list, select the process service Replication Engine for failover.
3. In the **Failover Process Service** list, select the new process service Replication Engine for which you want to move the replication pair.
4. To begin the Failover process, click **Failover**.
   You receive a message asking if you want to proceed with the process service failover.
5. Click **OK**.

**Note:** Replication pairs from the old process service Replication Engine moves to the new process service Replication Engine. These replication pairs require a Resync.

6 To move the replication pairs back to the old process service Replication Engine, click **Reset**.

## Balance Traffic Loads Settings

Allows you to specify the parameters for balancing traffic loads on the Oracle MaxRep Replication Engine.

### Agent-Process Service NIC Mapping

Specifies the available parameters for assigning the process service and replication agent to a network interface card (NIC) port. Available options:

**Select Volume Replication Agent**

Lists all the volume replication agents that use the process service. The details of a selected volume replication agent appears in the **Volume Replication Agent Details** table. This table shows the Replication Engine name and IP address.

**Select Process Server**

List all the process services that use the Replication Engine. The details of a selected process service appears in the **Process Server Details** table. This table shows the host name, IP address, and heartbeat of the process server.

**Select NIC to Map**

Lists all the NIC cards that are attached to the selected process service. The details of a selected NIC appears in the **NIC Details** table. This table shows the device name and IP address.

**Save**

Saves your changes.

**Reset**

Discards your changes.

### Already Configured Agent-Process Service NIC Mapping

Provides details about the existing load balancing configuration. Configured items:

- Volume replication agent
- Process service
- NIC port

**Delete**

Removes the current configuration.

### Related Links

*Balance Process Service Loads*

## Manage Bandwidth Usage

You can manage bandwidth usage by creating bandwidth policies.

The Bandwidth Shaping page contains the Configure Bandwidth Utilization table that displays the process services for all known Oracle MaxRep Replication Engines.

1. Navigate to **Protect** > **Provisioning** > **Manage Bandwidth Usage**.
   The Bandwidth Shaping page displays a list of process service Replication Engines.
2. To display all existing policies for this entry, select a Replication Engine to manage and then click **Next**.

   **Note:** If there are no existing policies, click **Create**.
3. To create a new bandwidth policy, click **Create Policy**.
4. Give the new policy a **Policy Name** and **Description**.
5. Enter the available bandwidth in the **Cumulative Bandwidth (kbps)** field.
6. Allocate a percentage of the bandwidth for each secondary Oracle FS System that appears as a **Target** in the **Allocate Bandwidth** table.
7. (Optional) Select **Share Unused Bandwidth** to share the unused bandwidth between the two bandwidth shaping pairs.
8. To schedule when your policy is enforced, click **Set Schedule**.
   For example, you could schedule your bandwidth policy to be enforced between 7:00 a.m. and 5:00 p.m., on a certain day of the week, or on a certain day of the month.
9. To commit your changes, click **Save**.
   The **Policy Confirmation** page indicates that the policy was created successfully.
10. To display the Existing Policies table, click **Next**.
11. In the Actions column, select one of the following:

    **View**

    To view details for the policy.

    **Edit**

    To modify the policy.

    **Delete**

    To remove the policy.
12. Click **Next**.
13. To return to the **Bandwidth Shaping** page and select **Enable Policy**, click **Back**.

### Related Links

*System Reports*
*View Bandwidth Reports*

CHAPTER 5

# Monitor Data Protection

## Monitor Data Protection

When you log in to Oracle MaxRep for SAN GUI the Monitor summary page displays. The page displays a high-level overview of the health of your Oracle MaxRep Replication Engines, and an overview of the current status of your protection plans. The Monitor page also displays any alerts or notifications that may need your attention.

### Protection Health

Displays the healthy, warning, critical, or inactive status of the protection plans, volumes, replication pairs, and file replication jobs in your system. Click on the name of a particular Protection Plan to view detailed information regarding that plan. The information is also shown in summary as percentages in the form of a pie chart.

Use the Plan Health filter to only display the plans that meet a desired criteria. Select any of the plans in the list to display the protection plan details.

Click the **Refresh** or **Settings** icon in the upper right corner of each section to refresh the display or to modify the properties of the display.

### Alerts and Notifications

Displays the events that need your attention. They are listed in descending order of occurrence. Each event has a brief header followed by a description and the number of occurrences in the last 24 hours.

You can edit the notifications to this page from the **Manage Users** option of the **Settings** tabs.

### Control Service/Process Service Health

Displays information about the Replication Engines and contains one tab for the control service that runs on the control service Replication Engine and one tab for each process service that runs on each active Replication Engine.

Click a tab to display the control service or process service statistics, system performance, and the status of the services running on the selected Replication Engine. Click any of the links to see detailed information.

**Control Service**

The tab shows the health of the control service processes. The control service is the service used to configure the replication process and policies.

**Statistics**

Indicates information about the control service and the agents that are using this service. You can view the health of the agent and the process service heartbeat.

**System Performance**

Indicates information about the control service performance, Replication Engine memory usage efficiency and disk activity.

Click any of the links to display information about the item.

The Hardware Status icon indicates the overall condition of the Replication Engine hardware. Health states include:

**Green**

Indicates healthy Replication Engine hardware.

**Red**

Indicates a hardware failure on the Replication Engine. Additional information is available in a system alert or by way of the ILOM user interface of the Replication Engine. The red icon also indicates that a Call-Home was performed.

**Services**

Indicates the health of the Replication Engine control services. Access these services from the Oracle MaxRep Support User Interface.

**Process Service**

The tabs show the status of the Process Services that run on active Replication Engines. The Process Service is the service used for the replication process.

**Note:** Your system might have more than one Process Service tabs.

**Statistics**

Indicates information about the process service and the replication pairs that are using this service.

**System Performance**

Indicates information about the process service performance, Replication Engine memory usage efficiency and disk activity.

Click any of the links to display information about the item.

The Hardware Status icon indicates the overall condition of the Replication Engine hardware. Health states include:

**Green**

Indicates healthy Replication Engine hardware.

**Red**

Indicates a hardware failure on the Replication Engine. Additional information is available in a system alert or by way of the ILOM user interface of the Replication Engine. The red icon also indicates that a Call-Home was performed.

**Services**

Indicates the health of the Replication Engine process services.

Click any of the links to display information about the item.

### Related Links

*Application Protection Monitoring*
*Display Application Protection Pairs*

## Application Protection Monitoring

In the Application Protection page, you can review the overall status of the replication to see the details of its progress.

Click the protection plan name to display the Plan Details page, which provides the following information:

**Volume Agent Pair**

Displays the LUN name and LUID of the source and target LUNs that are included in the protection plan.

Note: The last four digits of the LUID associates with the last four digits of the Oracle FS System serial number.

**Health**

Displays the health status of the volume replication pair and its associated Oracle FS System:

- Green = healthy
- Yellow = warning
- Red = critical
- Gray = inactive

**Health Issue**

Displays the reason for any critical, warning, or inactive status. An **N/A** entry indicates a healthy replication pair.

**RPO**

Displays the recovery point objective (RPO), in units of time. When the current protection plan RPO exceeds the defined RPO value for the plan, the GUI displays the alert in red text.

Note: When the RPO exceeds 120 minutes, the numeric units of the display switches to hours.

**Resync Progress**

Displays the progress of the resynchronization operation in terms of percent complete.

**Status**

Displays the status of the resynchronization operation:

- Resyncing (Step I)
- Resyncing (Step II)
- Differential Sync

**Resync Required**

Indicates whether the pair needs a resynchronization: **YES** or **NO**. Can also show **N/A** to indicate that the plan is inactive.

**Resync Data in Transit (in MB)**

Displays the number of megabytes of data in transit for Step 1 or Step 2 of a resynchronization.

Note: If the data that is in transit exceeds the Resync File Threshold that is set in the replication settings for the protection plan, the resynchronization stops. As data is flushed to the target, the resynchronization resumes.

**Differential Data in Transit (in MB)**

Displays the number of megabytes of data in transit on an Oracle MaxRep Replication Engine process service or on a secondary server.

Note: If the data that is in transit exceeds the value set in the Differential File Threshold option, then replication stops. The replication stops while the data transitions from data mode, which includes write order fidelity, into meta data mode, which is not write order fidelity. When the replication stops, it is an indication of the importance of the Differential Data in Transit option.

**View**

Provides different options for viewing information about the protection plan:

- Click **Summary** to see the replication options that are set in the protection plan.
- Click **Details** to see statistics, reports, and settings for the protection plan.

Protection Policies include the following information:

**Policy Type**

Identifies the policy types that are applicable to the protection of your application.

**Last Run Time**

Identifies the last time the policy instance ran.

**Status**

Indicates the status of the specified protection policy:

- Pending
- In progress
- Success
- Failed

**History**
Displays the log history.

Recovery Scenarios include the following information:

**Recovery Scenario Type**
Lists the names of the recovery scenarios that exist for the application:

- Data validation and backup
- Rollback

**Status**
Displays the status of the recovery job:

- Ready
- Pending
- In progress
- Completed
- Failed

**History**
Displays a history of the recovery scenario status.

### Related Links
*Monitor Data Protection*
*Display Protection Plan Details*
*Display Protection Plan Summary*

## Display Application Protection Pairs

Displays the replication pairs that are managed by a protection plan.

1. Navigate to **Monitor** > **Protection Status** > **Application Protection**.
2. To display details about the protection plan, click **Summary**.
3. To expand the plan details, click the plus sign beside the name of a protection plan.

   The system displays the following plan information:

   - Protection plan summary
   - Forward retention details

- Consistency details
- Forward protection details

4 When you have finished reviewing the protection plan details, click **Back**.

### Related Links

*Application Protection Monitoring*

## LUN Protection Monitoring

Allows you to display details about the replication pair LUNs.

To display the Volume Protection page, choose **Monitor** > **Protection Status** > **Volume Protection**. The **Source Host** and **Target Host** options list the names of the primary and secondary the replication pairs. By default, all of the volume replication pairs display. Use the Plan Name, Source Host, Target Host, and Volume Name filters to narrow the search, and click **Search**.

Protected volume replication pairs are listed in the **Volume Protection** table. Click the plus sign (+) located next to the name of a protection plan to expand the plan details.

**Note:** If the list is too long, you can filter the search results.

The Volume Protection page displays the following:

**Server**

Names the primary and secondary Replication Engines.

**Volume Agent Pair**

Displays the LUN name and LUID of the source and target LUNs that are included in the protection plan.

**Note:** The associated Oracle FS System can be determined by the last four digits of the LUID, which would match the last four digits of the serial number of the Oracle FS System.

**RPO**

Displays the recovery point objective (RPO), in units of time.

**Note:** When the RPO exceeds 120 minutes, the numeric units of the display switches to hours.

**Resync Progress**

Displays the progress of the resynchronization operation in terms of percent complete.

**Status**

Displays the status of the resynchronization operation:

- Resyncing (Step I)
- Resyncing (Step II)
- Differential Sync

**Resync Required**

Indicates whether the target LUNs in the protection plan need to be resynchronized with the source LUNs: **YES** or **NO**. Can also show **N/A** to indicate that the plan is inactive.

**Resync Data in Transit (in MB)**

Displays the number of megabytes of data in transit for Step 1 or Step 2 of a resynchronization.

**Differential Data in Transit (in MB)**

Displays the number of megabytes of data in transit on a Replication Engine process service or on a secondary server.

Note: If the data that is in transit exceeds the value set in the Differential File Threshold option, then replication stops. The replication stops while the data transitions from data mode, which includes write order fidelity, into meta data mode, which is not write order fidelity. When the replication stops, it is an indication of the importance of the Differential Data in Transit option.

**Action**

Displays the protection plan and volume details when **Summary** is clicked.

The Volume Summary page provides the following **Pair Settings** information:

**Primary Volume Size (MB)**

Displays the primary server LUN capacity in megabytes.

**Process Service**

Identifies the name and IP address of the Replication Engine that is running the process service for this volume.

**Secure data transfer Replication Engine Process Service to Secondary Server**

Indicates whether encryption is enabled from the process service Replication Engine to the secondary server.

**Resync Mode**

Indicates the type of resynchronization used for this replication pair.

- Resync I
- Resync II
- Differential Sync

**Target Volume Visible**

Indicates whether the secondary volume on the secondary server is in read-only mode.

**RPO Threshold**

Sends alerts if the recovery point objective (RPO) exceeds the selected threshold as defined during protection plan creation. The system sends alerts to the designated user and to the Alerts and Notifications section in the Oracle MaxRep GUI.

**Replication Pool**

Identifies the number of the replication pool, possibly one of many, to which this replication pair belongs.

**Resync File Threshold (MB)**

Indicates the maximum storage capacity on the process service Replication Engine to use for storing files during resynchronization, in MB.

**Differential File Threshold (MB)**

Indicates the maximum storage capacity to use for storing files during the differential synchronization, in MB.

**Compression**

Indicates whether to compress the protected data. Yes indicates whether compression takes place at the process service Replication Engine or at the primary server.

**CDP Retention**

Indicates whether continuous data protection (CDP) retention is configured for this replication pair.

**Retention Window Size**

Indicates the period of time that data is retained at the target location as defined during the creation of the protection plan.

The Volume Summary page provides the following **Resync Details**:

**Resync Start Time (Step 1)**

Indicates when the initial resynchronization starts.

**Resync End Time (Step 1)**

Indicates when the initial resynchronization ends.

**Resync Start Time (Step 2)**

Indicates when the resynchronization Step 2 starts.

**Resync End Time (Step 2)**

Indicates when the resynchronization Step 2 ends.

The Volume Summary page provides the following **Differential Sync Details**:

**Start Time**

Indicates when the differential synchronization starts.

**Last Update Time**

Displays the last updated time from the Replication Engine.

**Agent Log**

Displays as enabled if logs are present.

### Related Links

*Application Protection Monitoring*
*Display Replication Pair Statistics*

## File Replication Monitoring

The File Replication page enables you to monitor the file replication activities.

To display the File Replication page, choose **Monitor** > **Protection Status** > **File Replication**. The names of the primary server and secondary server of existing

volume replication pairs are listed under the **Source Host** and **Target Host** menus respectively.

The **File Protection Status** table lists all of the file replication pair. Click the plus sign (+) located next to the name of a protection plan to expand the plan details.

**File Replication Search Criteria**

The file replication details allow you to select filters to narrow your search results. Valid search filters:

- Job Description
- Application Agent
- Status
- Group ID
- Job ID
- Exit Code

Note: Explanations for each search filter are provided below.

## File Protection Status

Indicates the details about the selected file replication pair.

**View Details**

Displays log and trending information, and other related information when the plus symbol (+) is clicked.

**Job Description**

Displays the name of the job description given while configuring the file replication job.

**Application Agent**

Displays the name of the application agent while configuring the file replication job.

**Status**

Indicates the status of file replication job. Valid states:

- Starting
- Secondary server target starting
- Running
- Completed
- Failed

**Source Host**

Indicates the primary server name. The primary server is the server that is hosting the source data to be replicated in the protection plan.

**Source Directory**

Indicates the primary server directory, which contains the source data that is replicated from the Source Host.

**Target Host**

Indicates the secondary server name. This secondary server is the server that hosts the replicated data from the source host in the protection plan.

**Target Directory**

Indicates the secondary server directory where the replicated data is stored.

**Scheduled Type**

Displays the file replication job scheduled information.

**GID**

Displays the numeric identifier of the group to which the file replication pair belongs.

**JID**

Identifies the numeric identifier of the job.

**Job Instance**

Indicates the number of times the file replication pair job has run.

**Exit Code**

Identifies the file replication job failure code.

Note: A value of 0 indicates a successful completion.

The View Details navigation tree provides the following information:

**More Details**

Contains links to log and trending information.

**Start Time**

Indicates the time when the file replication starts.

**End Time**

Indicates the time when the file replication ends.

**Last Updated Time**

Indicates the time of the last activity.

**Data Compression**

Displays the amount of data compressed for transmission from the primary server to the secondary server.

**Sync Compression**

Displays the reduction in the amount of data transferred, expressed as a percentage, that is achieved by transferring differentials (transferring only the changed bytes). The formula is as follows:

```
1 - (Transfered / Total) x 100
```

Where:

- *Transfered* = The number of bytes transferred
- *Total* = Total replication size

The closer the percentage is to 100 the better the efficiency of the data transfer.

**Bytes Changed**

Total number of bytes transferred from the primary server to the secondary server during that particular schedule.

To delete a job history, select the particular job by selecting the check box at the end of each job column and then click **Delete Job History**.

To clear logs for a file replication job, select the particular job by checking the check box at the end of each job column and then click **Clear Logs for Selected Job**.

**Tip:** If the FX log option in the protection status contains a value that is greater than 1 GB, Internet Explorer will not be able to process the file. However, Firefox supports a file size up to 2 GB. To work around this limitation, use low verbosity in the job options.

**Note:** The **Data Compression**, **Sync Compression**, and **Trending** fields become active when the status of the job is **Completed**.

### Related Links

*Oracle MaxRep Logs*
*Application Protection Monitoring*

## Monitor Rollback or Snapshot Progress

You can monitor the progress of a rollback or snapshot operation. The information displays until the operation is complete.

To monitor the rollback or snapshot progress, go to **Monitor** > **Protection Status** > **Rollback/Snapshot Progress**.

The following information is available on this page:

**Host**

Indicates the name of the target host for the monitored snapshot or recovery pair.

**Host Drive**

Indicates the name of the SAN host LUN from which the snapshot or recovery was taken.

**Snapshot/Recovery/ Rollback Drive**

Indicates the name of the disk drive from which the snapshot or recovery was taken.

**Drive Type**

Indicates the type of drive used for the snapshot or recovery. Valid option types:

- Virtual
- Physical

**Progress**

Displays the progress of the operation in percentage of task complete.

**Start Time**
Indicates the time at which the operation started.

**End Time**
Indicates the time at which the operation ended.

**Recovery Point**
Displays the time and tag to which recovery should be done.

**Status**
Indicates the current state of the operation. Valid states:

- Queued
- Ready
- In Progress
- Completed
- Failed

**Info Message**
Displays any error message resulting from an operation failure.

**Auto Refresh**
Specifies the interval at which the information on the page is updated. Select the check box to enable the feature. Select the number to edit the value. Click **Save** to retain your changes.

### Related Links

*Monitor Rollback Progress*
*Monitor Snapshot Progress*

## Monitor Rollback Progress

You can monitor the progress of a secondary Oracle FS System LUN rollback operation.

1. Navigate to **Recover** > **More** > **Monitor Snapshot/Rollback Progress**.
2. Click the **Monitor Rollback** tab to monitor the progress of all rollback drives in the Target Drive Rollback Status table.

### Related Links

*Monitor Rollback or Snapshot Progress*

## Monitor Snapshot Progress

You can monitor the progress of a recovery snapshot or scheduled snapshot operation.

1. Navigate to **Recover** > **More** > **Monitor Snapshot/Rollback Progress**.
2. Click the **Monitor Recovery Snapshots** tab to monitor the progress of all recovery snapshots in the Recovery Pair Status table.

3 (Optional) To force a deletion of a snapshot, select one or more pairs and click **Force Delete**.

### Related Links

*Monitor Rollback or Snapshot Progress*

## Monitor Scheduled Snapshots

You can monitor a list of scheduled snapshots to be sure the schedules reflect the current replications needs.

1 Navigate to **Recover** > **More** > **Monitor Snapshot/Rollback Progress**.

2 Click the **Monitor Scheduled Snapshots** tab to display a list of scheduled snapshots.

3 (Optional) Filter the list using one or more of the following methods:

- Select a Target Host to display only the schedules associated with the host.
- Enter a Target Volume name.
- Enter a Schedule Drive name.

4 (Optional) To delete the schedule, select one or more schedules, and then click **Delete Scheduled Jobs**.

### Related Links

*Monitor Rollback or Snapshot Progress*

## Monitor Snapshot Drives

You can monitor the list of snapshots created by a scheduled job to make sure that snapshots are taken at intervals that meet the current needs. From this page, you can also delete snapshots when they are no longer needed.

1 Navigate to **Recover** > **More** > **Monitor Snapshot/Rollback Progress**.

2 Click the **Monitor Snapshot Drives** tab to display the list of snapshots.

3 (Optional) Filter the list using one or more of the following methods:

- Select a Target Host to display only the schedules associated with the host.
- Enter a Target Volume name.
- Enter a Schedule Drive name.

4 (Optional) To delete the recovery snapshots from the secondary Oracle FS System, select one or more pairs and click **Release Drive**.

5 (Optional) To force the deletion of the recovery snapshots from the Oracle MaxRep Replication Engine, select one or more pairs and click **Force Delete**.

### Related Links

*Monitor Rollback or Snapshot Progress*

## Monitor Replication Engine Communication

Using the Oracle FS System Manager GUI, you can check the communication between the registered Oracle FS System and the Oracle MaxRep Replication Engine.

From the Oracle FS System Manager GUI, choose **SAN** > **Data Protection** > **Replication Engines**.

The Replication Engines overview page shows the following information:

**Service Status** — Identifies the health of the processes running on the Replication Engine.

Valid states:

- Normal
- Warning
- Unknown

**Agent Status** — Identifies the communication status of the Oracle MaxRep for SAN agents registered with the Oracle FS System.

Valid states:

- All Communicating
- Warning
- Unknown

**Name** — Identifies the name of the Replication Engine.

**IP Address** — Identifies the IP address of the Replication Engine or high availability Replication Engine cluster.

**Version** — Identifies the Oracle MaxRep for SAN software version that is running on the Replication Engine.

If the system time of the last communication from an agent is older than the current system time by 15 minutes or more, Oracle MaxRep sends the designated user an alert email. The Replication Engine also sends an SNMP trap to the Oracle FS System for Call-Home processing. You can configure the amount of time before an alert is sent by setting up user account notifications from the Settings tab from the Oracle MaxRep for SAN GUI.

The reasons for the Oracle FS System losing communication with the control service and process service Replication Engines include:

- The agent service might be down.
- The firewall is blocking the agent.

- The network link is broken.
- The system is down.

### Related Links

*Oracle MaxRep Replication Engine Settings*
*Application Protection Monitoring*
*Configure the System to Receive SNMP Traps*

## Versions and Updates

The Versions and Updates page provides the version numbers that are currently running on the Replication Engines.

To display versions and updates, choose **Monitor** > **Protection Status** > **Versions and Updates**.

The following information is available on this page:

**Control Service Update History**

Displays the Replication Engine on which the control service is running. Click the plus symbol (+) to expand and display details.

**Process Service Update History**

Displays a history of all updates to the Replication Engines on which the process service is running. Details include:

**Update History**

Displays a history of updates to the process service Replication Engines.

**Host Name**

Indicates the host name of the agents.

**Process Engine Version**

Indicates the version of the process service Replication Engines.

**Process Engine Installation Date**

Indicates the date the Replication Engines were installed.

**Installation Path**

Indicates the installation path location of the process server Replication Engines.

**Agent Version and Update History**

Displays a history of the versions and updates to all agents running on your system. Details include:

**Update History**

Displays a history of patches that are applied to the agents.

**Host Name**

Indicates the host name of agents.

**Volume Replication**

Indicates the version of volume replication agent. A volume replication agent is a host-based volume splitter that enables application protection and replication.

**File Replication**

Indicates the version of file replication agent. A file replication agent is a host-based file system splitter that enables application protection and replication.

**Sentinel Driver**

Indicates the version of sentinel driver.

**Product Version**

Indicates the product version.

### Related Links

*Monitor Data Protection*

## Display Network Configuration

The network configuration page provides details about the process services running on the Oracle MaxRep Replication Engine.

1. Navigate to **Settings** > **Advanced Configuration** > **Network Configuration**.
2. Review the following information about the network configuration.

**Process Service**

Indicates the IP address or domain name service (DNS) of the Replication Engine.

**Interface**

Indicates the process service network port number.

**Type**

Indicates the Ethernet port number.

**IP Address**

Indicates the IP address of the network port.

### Related Links

*Oracle MaxRep Agent Settings*
*Balance Process Service Loads*
*Display Host Logs*

# System Reports

Oracle MaxRep for SAN provides two types of reports: bandwidth reports and health reports.

**Bandwidth Reports**

- Provides information on the incoming and outgoing network traffic for each Replication Engine on your system.
- Provides the network traffic that is associated with your primary Replication Engine.
- Provides tabular and graphical views of data traffic by day, week, month, or year.
- Provides custom bandwidth reports for a specific period of time.

**Health Reports**

- Provides consolidated information on the status and performance of each replication pair on your system.
- Provides tabular and graphical views of data change rates, RPO, retention, and health status.
- Provides tabular and graphical views by day, week, month, or year.
- Allows you to download the complete health report as a comma separated value (CSV) file to your local workstation.
- Allows you generate custom reports of health information for a specific period of time.

### Related Links

*View Bandwidth Reports*
*View Health Reports*
*Generate Custom Reports*
*Display Replication Pair Reports*

## View Bandwidth Reports

Default bandwidth reports provide tabular and graphical information about data flow and replication pair status.

1. Navigate to **Monitor** > **Reports**.
2. Click **Bandwidth Reports** to view the default bandwidth report for your primary Oracle MaxRep Replication Engine.

   If necessary, select a different Replication Engine from the **Select Host** list.
3. View the bandwidth report time span.

   Possible options:

   **Last Day**

   Charts traffic arriving and leaving the selected Replication Engine from the previous day.

**Last Week**

Charts traffic arriving and leaving of the selected Replication Engine from the previous week.

**Last Month**

Charts traffic arriving and leaving of the selected Replication Engine from the previous month.

**Last Year**

Charts traffic arriving and leaving of the selected Replication Engine from the previous year.

4 To export the bandwidth report as a comma-separated value (CSV) file, click **Export to CSV**.

### Related Links

*System Reports*
*Display Replication Pair Reports*
*View Health Reports*
*Generate Custom Reports*

## View Health Reports

Default health reports provide tabular and graphical information about data flow and replication pair status.

You can view data that has collected during the time period since the replication pair was created.

1 Navigate to **Monitor** > **Reports**.

2 Click the **Health Reports** tab to view the default health report for all of your replication pairs.

3 Select the type of health report you want to see.

Valid report types:

**Change Rate**

Charts the frequency of data changes in compressed and uncompressed data for the protection plan during the time period.

**RPO**

Charts the recovery point objective (RPO) performance of the protection plan in minutes during the time period.

**Retention**

Charts the retention window of the protection plan measured in days during the time period.

**Health**

Charts the health status of the replication pairs during the time period.

4 To export the health report as a comma-separated value (CSV) file, click **Export to CSV**.

### Related Links

*System Reports*
*Display Replication Pair Reports*
*View Bandwidth Reports*
*Generate Custom Reports*

## Generate Custom Reports

You can generate custom reports that are specifically tailored to your needs.

1. Specify what to include in your custom report in the Custom Report **Query Form**.
2. Click **Custom Report** on the Bandwidth Report or Health Report page.
3. Select the name of the primary Replication Engine in the **Select Hosts** text box.
4. Click the calendar icon and then specify a start date and an end date.

   **Note:** For bandwidth reports, you can also specify start and end times.
5. For bandwidth reports, select **Complete Host Report** to include data for all the previous time periods in your report.
6. Click **Generate Report**.
7. Click **Print Report** to print a hard copy of the report.

   **Note:** You can also export health reports as CSV files by clicking **Export to CSV**. You can open the exported CSV file or save it on your workstation.

### Related Links

*System Reports*
*Display Replication Pair Reports*
*View Health Reports*
*View Bandwidth Reports*

## Display Replication Pair Reports

You can view detailed reports about the LUNs of a replication pair. Options available on this page allow you view additional detailed health reports.

1. Navigate to **Protect** > **Oracle Storage** > **Manage Protection Plan**.
2. From the Protection table, select the protection plan to view.
3. To view the plan details, click **Plan Details**.
4. Under the View column, select **Details**.
5. From the Replication Statistics details page, click the **Reports** tab.
   The system displays health reports and settings for the replication pair.

### Related Links

*System Reports*
*Replication Reports Settings*
*Configure Replication Pair Settings*

## Configure Replication Pair Settings

You can specify the settings that apply to the replication pair statistics and reports. The options that are available on this page allow you to apply your settings, pause replication, create a new protection plan, and move your settings to an existing plan.

1. Navigate to **Protect** > **Oracle Storage** > **Manage Protection Plan**.
2. From the Protection table, select the protection plan to view.
3. To view the plan details, click **Plan Details**.
4. From the Plan Details page, click **Details**.
5. From the Replication Statistics page, click the **Settings** tab.
6. Make the necessary changes to the replication pair settings.
7. (Optional) To suspend the protection plan replication, click **Pause Replication**.
8. To keep your changes, click **Accept Changes**.

### Related Links

*Replication Reports Settings*
*Display Replication Pair Reports*

## Replication Reports Settings

Allows you to review the replication pair settings of a selected LUN. You can also select options from this page that display custom reports.

### Health Report Actions

The Health Report banner contains links that allow you to display custom detailed reports.

**Change Rate**

Displays the Change Rate custom report.

**RPO**

Displays the recovery point objective (RPO) custom report.

**Retention**

Displays the retention policy custom report.

**Health**

Displays the health custom report.

## Health Report

Displays a list of registered Oracle FS Systems. Select the target LUN for which you want to display its health report details.

**Date**

Indicates the date of the report.

**Data Changes**

Indicates the data changes in compressed and uncompressed data, in megabytes.

**Retention Window**

Indicates the retention policy setting and the days remaining for the replication pair.

**RPO**

Indicates the recovery point objective (RPO) threshold in minutes and the maximum number of minutes recorded for the replication pair.

**No. of hours RPO not met**

Indicates the maximum number of hours for which RPO has not been met.

**Throttled Duration (Hours)**

Indicates the duration in hours that the replication pair has been in data flow controlled (throttled data) mode. This value includes cumulative, resynchronization and differential synchronization throttling.

**Retention Log Reset?**

Indicates whether the retention log was reset during replication.

**Available Consistency Points**

Indicates the number of consistency points that are available in the LUN.

**Protection Coverage**

Indicates the cumulative protection coverage, which consists of the following statistics:

- RPO Health
- Throttle Health
- Retention Health
- Resync Health
- Replication Accuracy

### Related Links

*Log Management*
*Display Replication Pair Reports*
*Display Host Logs*
*Display Oracle MaxRep Replication Engine Logs*
*Display Audit Logs*

## Oracle MaxRep Logs

Oracle MaxRep for SAN collects a variety of logs that collect user actions, and the activities of the host and the Oracle MaxRep Replication Engine.

The host logs includes a record of activities for the Oracle MaxRep agents, the Replication Engine, and user actions.

The system provides separate pages for viewing or downloading host logs, Replication Engine logs, and audit logs. A page is also available for downloading host or Replication Engine logs.

You can view the information contained in the various logs in their display pages. The log display pages are located at **Monitor** > **Logs**. Included pages:

**Host Logs**
Lists the Replication Engine activity logs for the Oracle MaxRep agents that are running on the hosts.

**Replication Engine Logs**
Lists the logs that are associated with data statistics, data transfer, debugging, and auditing actions that are available for the current Replication Engine.

**Download Logs**
Lists the host and Replication Engine logs that are available for downloaded.

**Audit Logs**
Lists all user actions on the current Replication Engine.

### Related Links

*Log Management*
*Download Logs*
*Display Host Logs*
*Display Oracle MaxRep Replication Engine Logs*
*Display Audit Logs*

## Log Management

Allows you to review the exception events that have occurred in the Oracle MaxRep Replication Engine. You can also edit the settings for log collection and retention from this page.

Navigate to **Settings** > **Settings** > **Log Management** to display the list.

**Log Name**

Indicates the name of the log file.

**Policy Type**

Identifies the type of policy that is associated with log retention or log file size. Valid policy types:

- Time based: Log retention is based on a number of days.
- Space based: Log retention is based on the size of the log file.
- Composite based: Log retention is based on a combination of the time and space options.

**Policy Unit**

Identifies values of the **Policy Type** setting.

**Edit**

Allows you to modify the log rotation policy settings.

### Related Links

*Oracle MaxRep Logs*
*Edit Log Rotation Settings*
*Download Logs*

## Edit Log Rotation Settings

Allows you to specify the policy type of the log collection.

Navigate to **Settings** > **Settings** > **Log Management** > **Edit** to display the policy update page.

**Log Name**

Identifies the name of the edited log.

**Policy Type**

Identifies the type of policy that is associated with log retention or log file size. Valid types:

**Time-based**

Log retention is based a number of days.

**Space-based**

Log retention is based on the size of the log file.

**Composite-based**

Log retention is based on a combination of the time and space options.

**Policy Unit**

Identifies values of the **Policy Type** setting.

**Time-based**

Allows you to specify the number of days to retain the data log.

**Space-based**

Allows you to limit the size (in MB) of the data log.

**Save**

Allows you to retain your changes.

**Back**

Allows you to return to the Log Management page without saving your changes.

### Related Links

*Log Management*

## Display Host Logs

The Host Logs contain a record of the Oracle MaxRep agent activities.

1. To select a host, navigate to **Monitor** > **Logs** > **Host Logs**.
2. In the Host - Log Details table, click the name of the host to expand the host entry.
3. Click the name of the LUN for which you want to view the log.
4. Click **Open** to view the log.
   The log displays in your default text editor.

   **Note:** If the default text editor does not format the text properly, save the log file and open it in another text editor, such as gVim or Notepad++.
5. To save the log file to your system, save it from the text editor window.

### Related Links

*Oracle MaxRep Logs*
*Log Management*
*Download Logs*

## Display Oracle MaxRep Replication Engine Logs

The Replication Engine log displays the data statistics, data transfer, debugging, and auditing actions that take place in the Oracle MaxRep Replication Engine.

1. To select a Replication Engine log, navigate to **Monitor** > **Logs** > **Replication Engine Logs**.
2. Click the name of the log in the Replication Engine Logs table.
3. Click **Open** to view the log.
   The log displays in your default text editor.

**Note:** If the default text editor does not format the text properly, save the log file and open it in another text editor, such as gVim or Notepad++.

4 You can view the following logs as needed:

**Table 12: Available Replication Engine logs**

| Log name | Description |
|---|---|
| `tman_volsync` | Data file processing operation (file renames or file compression), failures, or user debugs. |
| `tman_monitor_ps` | Process service registration related messages including user debugs. |
| `tman_monitor_disks` | Replication Engine internal database connectivity, logs offline disks. |
| `audit` | User actions (all of the GUI audits are captured in this log file). |
| `tman_monitor` | Monitor event exceptions and user debugs. |
| `Message` | Logs of all the scheduler messages. |
| `bpmtrace` | BPM service activity messages, including user debugs. |
| `network_trends` | Error or debug messages for network trending. |
| `tman_healthmonitor` | Log error or debug messages of the health monitor thread. |
| `perf` | Size of data coming from the Oracle MaxRep agent after compression or decompression at the Replication Engine. |
| `Traplog` | Replication Engine trap event generated messages. |
| `rsyncd` | Remote synchronization related messages. |
| `FX job logs` | Logs related to FX job logs. |
| `Application` | Logs of application protection. |
| `array_register` | Logs of array registration. |
| `array` | Logs of array protection. |
| `array service` | Logs of array services. |

Table 12: Available Replication Engine logs (continued)

| Log name | Description |
|---|---|
| dpsglobal | Volume protection logs. |
| fabricservice | Fabric service logs. |
| xferlog | Log of details of all data file uploads, downloads, and deletes. |
| gentrends | Trending graph generation logs. |
| ha_failover | High availability failover logs. |
| itldiscovery | Initiator and target port discovery logs. |
| itldiscovery | Initiator and target LUN discovery log. |
| itlprotector | Pair configuration logs for LUNs. |
| perl_sql_error | SQL errors generated from Perl. |
| prismprotector | Prism pair activation log. |
| prism service | Prism service log. |
| request enable | Agent request log. |
| ResyncStartNotify | Logs of resync start. |
| Unregister | Host unregistration log. |
| volume_register | Volume registration log. |
| VolumeProtection | Volume protection log. |
| tman_monitor_agents | Agent monitor logs. |
| tman_monitor_alerts | Logs for alerts. |
| tman_monitor_disks | Disk monitoring logs. |
| tman_monitor_ha | Logs for high availability service. |
| tman_monitor_protection | Logs for monitor protection. |
| tman_monitor_ps | Logs for process service monitor. |
| tman_monitor_reports | Logs for report generation. |

Table 12: Available Replication Engine logs (continued)

| Log name | Description |
|---|---|
| `tman_volsync` | Logs for volsync. |
| `Vsnapprocess_vsnap log` | Virtual snapshot process logs. |

### Related Links

*Oracle MaxRep Logs*
*Log Management*
*Download Logs*

## Display Audit Logs

The Oracle MaxRep Replication Engine audit logs display the administrator interactions with the Oracle MaxRep for SAN GUI.

1. To view the audit logs, navigate to **Monitor** > **Logs** > **Audit Logs**.
   All actions by all users are displayed in the Audit Logs table by default.
2. To filter the audit logs displayed in the table, enter a user name, keyword, or start and end time, and then click **Search**.

   **Note:** To navigate through multiple pages, use the **FIRST**, **NEXT**, **PREVIOUS**, and **LAST** selections at the top right of the page.

   The Audit Logs table contains the following information about each user action:

   **User**

   Indicates the name of the administrator who performed the action.

   **Date/Time**

   Indicates the date and time of the administrator action.

   **IP Address**

   Indicates the IP address from which the action was performed.

   **Log Details**

   Indicates the description of the administrator action.

### Related Links

*Oracle MaxRep Logs*
*Log Management*
*Download Logs*

## Download Logs

The Download Logs page allows you to download the host and Oracle MaxRep Replication Engine logs.

You can download all or some of the logs, as necessary.

1. Navigate to **Monitor** > **Logs** > **Download Logs**.
2. From the Host - Download Logs table, select the following items, as needed.
   - Select **Host Logs** to download host logs.
   - Select **Perf Logs** to download performance logs of Oracle MaxRep agent activity.
   - Select the name of the host from which to download the host or Oracle MaxRep agent logs.
   - Select the type of archive file to create (zip or tar) and then click **Archive Logs**.
3. From the Replication Engine - Download Logs table, select the following items, as needed.
   - Select the type of logs (Replication Engine, File Agent, Xferlog, Proftpd, or Resync) that you want to download from the Replication Engine.
   - Select the type of archive file to create (zip or tar) and then click **Archive Logs**.

   The screen refreshes after the download completes.
4. Click **Download Logs** to download the newly created archive.
5. Choose to open or save the file.

### Related Links

*Oracle MaxRep Logs*
*Log Management*

# Alerts

Alerts provide important information about Oracle MaxRep for SAN. The system sends alert notifications from Simple Network Management Protocol (SNMP) traps when events occur. Administrators can specify which notifications they wish to receive.

New administrator accounts contain a default set of notifications. Each administrator can determine which Oracle MaxRep for SAN alerts trigger a notification.

The following events trigger an event notification by default. You can edit this list, as necessary.

- RPO SLA Threshold Exceeded
- Resync Required
- Agent/Process Service Not Responding
- Replication Engine Secondary Storage Warning
- File Agent Job Error
- Agent Has Logged Alerts
- Bandwidth Shaping Alerts
- Daily Protection Health Report Day(s)
- Insufficient Retention Space
- Source Volume Resized
- Process Service Uninstalled
- Replication Engine Debug Info
- Application Protection Alerts

### Related Links

*Alerts and Notifications*
*Configure Email Notifications*
*Configure SNMP Notifications*

## Configure Email Notifications

You can configure Oracle MaxRep for SAN to notify email recipients of various alerts.

Successful email delivery of alert notifications requires that you configure at least one mail server with a valid email address.

1. Navigate to **Settings** > **Replication Engine Settings** > **Mail Settings**.
2. To set the email addresses, navigate to **Settings** > **User Management** > **Manage Users**.
3. Configure the email address depending on the administrator status. Status options:
   - For a new administrator, select **Add User** and enter the valid email address. Enter the remaining required information to add the administrator and activate the email notification settings.
   - For an existing administrator, select **Edit User** and enter a new email address or update the existing address.
4. From the **Alert Notification** section, **E-mail** column, select or deselect the Alert Category for which to receive notifications.

5 (Optional) For an existing administrator, modify the text for the default **E-Mail Subject**.

6 To keep your settings, click **Save**.

### Related Links

*Alerts*

*Alerts and Notifications*

## Configure SNMP Notifications

You can configure Oracle MaxRep for SAN to notify administrators of Oracle MaxRep Replication Engine events through Simple Network Management Protocol (SNMP) traps. Each administrator configures their own SNMP notifications.

**Prerequisites**

- You are logged in to the Replication Engine under the user name for which the SNMP setting are configured.

  **Note:** The primary administrator cannot set SNMP traps for other administrators of the system.

- A network monitoring server, known as a *trap listener*, is required on the network, which will allow the Replication Engine to send SNMP traps to the trap listener email address.

1 Navigate to **Settings** > **User Management** > **Manage Users**.

2 From the User Accounts table, select **Settings** for the active user.

3 From the Configured Trap Listeners table, click **Add**.

4 Enter the IP address (or the DNS host name of the host running the SNMP trap listener) and the trap port number, then click **Add**.

5 (Optional) If you have more than one SNMP trap server, click **Add** and enter the additional host information.

6 From the Alert Notification table, click **Edit**.

7 Select or deselect the Alert Notifications for which you want to receive notifications.

8 To keep your settings, click **Save**.

### Related Links

*Alerts*

*Alerts and Notifications*

*Configure ILOM Network*

*Configure Email Notifications*

## Configure the System to Receive SNMP Traps

Configure the Simple Network Management Protocol (SNMP) trap of the to send software fault notices to the Call-Home server.

**Prerequisites**

- Log in as the primary administrator for the .
- IP address to the Oracle FS System Pilot management interface.

  **Note:** Use the Pilot that is registered to the so that Call-Home notifications and replication logs originate from the same .
- ILOM network settings are configured from the (Support UI).

The uses the Integrated Lights Out Manager (ILOM) port to send notifications to the Call-Home server.

1. Navigate to **Settings** > **User Management** > **Manage Users**.
2. From the User Accounts table, select **Settings** for the active user.
3. From the Configured Trap Listeners table, click **Add**.
4. Enter the IP address of the Oracle FS System Pilot and the trap port number, then click **Add**.
5. To keep your settings, click **Save**.

### Related Links

*Alerts*

*Configure ILOM Network*

## Alerts and Notifications

By default, Oracle MaxRep for SAN sends email alerts and SNMP traps for notifications of situations that might require corrective action.

The following table provides a list event notifications, the cause of the notification, and actions to correct the problem.

Table 13: Email alerts and notifications

| Event | Cause | Corrective action |
|---|---|---|
| RPO SLA threshold exceeded | A performance bottleneck is preventing the target LUNs included in the protection plan from keeping up with the change rate occurring on the source LUNs. | Monitor the services at the Replication Engine and ensure that the services are running. Review the network, SAN, and target storage for potential performance bottlenecks. |
| Resync required | Possible causes:<br>• Resynchronization required might be set due to data inconsistency.<br>• Primary Oracle FS System LUN has been resized.<br>• Secondary Oracle FS System LUN is exposed in read-write mode.<br>• Configuration server failover during high availability (HA) scenario.<br>• Manual resynchronization has been requested through the GUI.<br>• Protection plan has been manually deactivated through the GUI. | If a resynchronization was requested manually from the GUI, no action is required. The Plan will resynchronize automatically.<br>In all other cases, if automatic resynchronization options were set in the replication configuration, the protection plan automatically resynchronizes when the resynchronization window is reached.<br>Restart a resynchronization from the Oracle MaxRep Replication Engine GUI. |

Table 13: Email alerts and notifications (continued)

| Event | Cause | Corrective action |
|---|---|---|
| MaxRep agent not responding | This email is sent when the agent is unable to communicate with the Replication Engine within 900 seconds. Possible causes:<br>• Agent service may not be started.<br>• A firewall may be blocking the agent.<br>• Network failure.<br>• The host may be down. | Possible actions:<br>• Disable any firewalls.<br>• Ensure that the Agent service is running.<br>• Check if the Oracle FS System is connected to the correct Replication Engine. |
| Replication Engine secondary storage warnings and alerts | The storage capacity of a file system mounted on the Replication Engine exceeds the storage capacity warning threshold that is configured in the GUI.<br>**Note:** In the Replication Engine settings option of the Settings tab, configure the storage capacity usage limit. | An email alert is sent when the storage usage has reached 80% for the following volumes on the Replication Engine:<br>• `/`<br>• `/home`<br>Possible actions:<br>• Increase the threshold.<br>• Open a service request with the support center. |
| File agent job error | A File agent encounters an error. | Check the Agent log for additional information. |
| Agent logged alerts | A Volume or File agent encounters an error. | Check the Agent log for additional information. |
| Daily Protection Health Report <number of days> | Health reports can be configured to be sent by email automatically. (This is an email event only; no SNMP trap can be sent or configured for this alert.) | No corrective action is required. |

**Table 13: Email alerts and notifications (continued)**

| Event | Cause | Corrective action |
|---|---|---|
| Insufficient Retention Space | Insufficient capacity is available in one or more retention LUNs for the specified protection plan. | Possible actions:<br>• Edit the retention policy and increase the retention space to accommodate more logs.<br>• Reduce the retention window. |
| Source Volume Resized | The source LUN capacity has been resized to a capacity greater than the current configured pair. | Detect whether the source LUN has been resized. |
| Process Service Uninstalled | A process service pointed to this control service has been uninstalled. | This message is for information only. |
| Control Service Node Failover Alert | A Replication Engine HA failover has occurred. | Bring the failed Oracle FS System online and perform a failback. |
| Replication Engine Debug Info | An email is sent when errors exist in the host logs. (This event only permits email alerts to be sent. The trap listener alert is not available.) | Check the Replication Engine logs. |
| Application Protection Alerts | No common consistency point is available for the specified Protection Plan. A common consistency point is needed for failover and failback operations. | Check your retention and consistency policies. |

### Related Links

*Alerts*

*Detect Resizing of a Source LUN*

## Protection Plan Error Resolution

Occasionally, issues with the protection plan can arise that prevent timely replication.

Errors might occur during the following replication stages.

- Resynchronation
- Differential synchronization

### Related Links

*Alerts and Notifications*
*Unable to Write Replication Data*
*Slow Replication During Resynchronization*
*Slow Replication During Differential Sync*

## Unable to Write Replication Data

An error occurs when the retention LUNs (also called cache LUNs) become read only, which means that the replication data cannot be written to the LUNs.

### Error Received

```
Received a file of lesser timestamp or sequence.
```

### Symptoms

The following symptoms might occur:

- Unable to write replication data to a LUN.
- The protection plan **Resync** field is set to **Yes**.

### Resolution

Restart the resynchronization operation.

### Related Links

*Protection Plan Error Resolution*

## Slow Replication During Resynchronization

During a resynchronization operation, the rate at which a replication pair generates the protection files might decrease or replication might stop completely after you have remapped a source or target LUN.

### Errors Received

One of the following errors might occur:

- `The source LUN cannot be read and due to that resync files are not reaching to appliance.`

  You might have received the error after unmapping the source LUN.

- `Target is not able to apply the differentials/resync files.`

### Symptoms

One or more of the following symptoms might be present:

- Resynchronization operation is not progressing: RPO is increasing.

- The number of replication files during differential synchronization is increasing.
- No communication from the source LUN to the Oracle MaxRep Replication Engine exists because the differential throttle delay and resynchronization is not progressing.

### Resolution

One of the following resolutions apply:

- Map the source LUN to the Replication Engine.
- Map the target LUN to the Replication Engine.

### Related Links

*Protection Plan Error Resolution*

## Slow Replication During Differential Sync

During a differential synchronization operation, the rate at which a replication pair generates the protection files might slow down or stop after you have remapped a source or target LUN.

### Error Received

One of the following errors occurs:

- Data mode: `Differentials reach to appliance and continue to progress. There is no impact on pair progress.`
- Metadata or bitmap modes: `S2 is not able to read source LUN, because of LUN Unmap.`
- `Target is not able to apply the differentials/resync files.`

### Symptoms

One or more of the following symptoms might be present:

- Resynchronization operation is not progressing: RPO is increasing.
- The number of replication files during differential synchronization is increasing.
- No communication from the source LUN to the Oracle MaxRep Replication Engine exists because the differential throttle delay and resynchronization is not progressing.

### Resolution

One of the following resolutions apply:

- Map the source LUN to the Replication Engine.
- Map the target LUN to the Replication Engine.

### Related Links

*Protection Plan Error Resolution*

## Statistics

Oracle MaxRep for SAN GUI provides two types of statistics: data change rates and network traffic rates.

**Date Change Rates**

Provides daily and monthly statistical charts about the compressed and uncompressed data changes on the primary Oracle MaxRep Replication Engine. Pie charts represent the compressed and uncompressed data capacity for each Replication Engine. Oracle MaxRep for SAN stores detailed trending charts that contain historical change rates as well.

**Network Traffic Rates**

Provides statistical charts about the bandwidth usage for each process server. The types of charts include views of the following earlier time periods:

- Day
- Week
- Month
- Year

### Related Links

*Protection Plans*

*Network Traffic Rates*

*View Trending Data Change Rates*

## View Trending Data Change Rates

You can monitor the data changes on the primary Oracle MaxRep Replication Engine. The details include compressed and uncompressed data in daily and monthly increments. This page displays two types of graphs: bar graphs and pie charts.

1. To display the data change rates, navigate to **Monitor** > **Statistics** > **Data Change Rates**.
2. View the data change rate details.

   **Daily Data Change (bar graph)**

   Displays the compressed and uncompressed data change rate in hourly increments for the current day.

   **Monthly Data Change (bar graph)**

   Displays the compressed and uncompressed data change rate in daily increments for the current month.

**Cumulative Data Distribution - Compressed (pie chart)**

Displays the compressed data distribution for each SAN host.

**Cumulative Data Distribution - Uncompressed (pie chart)**

Displays the uncompressed data distribution for each SAN host.

3 (Optional) Select the legend detail at the top to hide the selected data on the graph.

### Related Links

*Statistics*

*View Trending Data Change Rate Details*

## View Trending Data Change Rate Details

You can view historical records of daily and monthly data change rates.

1 To display the data change rate details, navigate to **Monitor** > **Statistics** > **Data Change Rates** > **Detailed Trending**.

2 Select a trending chart to view its details. Available charts include:

**Daily Cumulative Data Change Graphs**

Displays a historical record of the cumulative daily change rate.

**Monthly Cumulative Data Change Graphs**

Displays a historical record of the cumulative monthly change rate.

### Related Links

*View Trending Data Change Rates*

## Network Traffic Rates

Allows you view graphs of the bandwidth usage for each process service.

To display the bandwidth usage charts, navigate to **Monitor** > **Statistics** > **Network Traffic Rates**.

Select a process service from the available list.

**Select Process Service**

Displays a list of available hosts that contain bandwidth charts to view.

**Process Service**

Displays the date and time of the bandwidth charts.

**Last Day Graph**

Displays the bandwidth usage of the previous day in one-hour increments.

Each graph contains the following information for data that has been exchanged on the host:

**Note:** All of the graphs display data in the number of bytes each second.

- Maximum bandwidth usage
- Average bandwidth usage
- Current bandwidth usage
- Total bandwidth usage

**Last Week Graph**

Displays the bandwidth usage for each day in a seven-day period.

**Last Month Graph**

Displays the bandwidth usage for each day in a four-week period.

**Last Year Graph**

Displays the bandwidth usage for a year in a 12-month period.

**Year**

Allows you to select a year for which you want historical network traffic rates displayed.

### Related Links

*Statistics*

## Display Replication Pair Statistics

You can view statistical information about the replication pair and review the specifications for how this information displays on the page.

1. Navigate to **Protect** > **Oracle Storage** > **Manage Protection Plan**.
2. Select the protection plan to view from the Protection table.
3. To view the plan details, click **Plan Details**.
4. From the Replication Statistics details page, click the **Details** tab.
   The system displays statistics about and settings for the replication pair.

### Related Links

*Statistics*

*Replication Statistics Settings*

## Replication Statistics Settings

Allows you to review the settings for replication pair statistics of a selected LUN. You can also view the daily and monthly change graphs and recovery point objective (RPO) graphs from this page.

### Pair Details

**Primary Server**

Indicates the name of the primary Oracle FS System.

**Primary Volume**

Indicates the name of the source LUN of the replication pair.

**Remote Server**

Indicates the name of the secondary or remote Oracle FS System.

**Target Volume**

Indicates the name of the target LUN of the replication pair.

**Process Service**

Indicates the name and IP address of the Replication Engine that is running the process service for this volume.

**Replication Pool**

Indicates the identifier of the replication pool, possibly one of many, to which this replication pair belongs.

**Fast Resync Unmatched**

Indicates the percentage of unmatched data blocks between the source and target LUNs.

**Agent Log**

Indicates whether the Agent logs are written for the replication pair.

## Pair Settings

**Visible**

Not applicable for Oracle MaxRep for SAN.

**Visible Drive Mode**

Not applicable.

**Mount Point**

Not applicable.

**Profiling Mode**

Indicates whether the source LUN is profiled during replication.

**Secure Replication Engine-Process Service to Destination**

Indicates whether secure transport, or encryption, from the process service to the secondary Oracle FS System is enabled.

**Secure Source to Replication Engine-Process Service**

Indicates whether secure transport, or encryption, from the primary Oracle FS System to the process service is enabled.

**Resync Mode**

Indicates the identifier of the replication pool, possibly one of many, to which this replication pair belongs.

**RPO Threshold**

Indicates the threshold recovery point objective (RPO) in minutes. If RPO increases beyond this limit, email alerts are sent to the configured email address.

**Replication Pool**

Indicates the name of the Agent log that contains more information about the replication.

**Resync Files Threshold**

Indicates the name of the Agent log that contains more information about the replication.

**Differential Files Threshold**

Indicates the maximum amount of storage space (in MB) for the Process service that is used for storing files during differential sync operations.

**Compression Enable**

Indicates whether data will be compressed at the Process service system or at the primary Oracle FS System.

## Retention Settings

**Retention**

Indicates whether the replication pair is configured with a retention policy applied.

**Retention Log Size Limit**

Indicates the capacity limit of the retention logs.

**Retention Time Limit**

Indicates the duration to retain the replication pairs.

**Log Data Directory**

Indicates the location of the replication logs.

**Disk Space Threshold**

Indicates the limit of capacity that can be used for the replication pairs.

**Unused Space**

Indicates the limit of capacity that can be used for the replication pairs.

**On Insufficient Disk Space**

Indicates the action to take when the storage capacity threshold is met.

## Data Change and RPO Graphs

**Daily - Data Change (bar graph)**

Displays the compressed and uncompressed data change rate in hourly increments for the current day.

**Monthly - Data Change (bar graph)**

Displays the compressed and uncompressed data change rate in daily increments for the current month.

**Daily - RPO Graph (pie chart)**

Displays the minutes of RPO in hourly increments for the current day.

**Monthly - RPO Graph (pie chart)**

Displays the minutes of RPO in daily increments for the current month.

**Target Space Savings**

Displays the cumulative target LUN usage with and without thin provisioning applied.

### Related Links

*Display Replication Pair Statistics*

## Profiling

The Profiler is a tool to help identify resource requirements. Create a profile of your primary Oracle MaxRep Replication Engine to gain valuable insights to information such as data change rates on the primary LUN, data compressibility, required bandwidth to achieve the given recovery point objective (RPO), and required storage.

Profiling helps to accurately predict resource requirements between sites and on the secondary Oracle FS System. During the profiling process only data change rates at the primary Replication Engine are observed. No actual data replication occurs.

To attain higher levels of accuracy, profiling should span at least two weeks. Ideally you should capture relevant daily, weekly, and monthly processing jobs that might impact the source LUN data. Expanding your profile criteria provides you with a statistically significant amount of data.

High availability disaster recovery and backup administrators can use profiling results to answer questions such as:

- What is the total storage capacity required for backup and disaster recovery of selected LUNs?
- What is the bandwidth required for a near zero RPO?
- What is the amount of bandwidth saved due to compression?
- Does the currently provisioned bandwidth suffice for a continuous backup or disaster recovery (DR) implementation?
- What is the storage required on the secondary server for the desired retention window?
- How are the data changes distributed throughout the day, week, or month?
- What is the bandwidth requirement for a desired RPO?

### Related Links

*Set Up Profiling*
*View Trending Data Change Rates*
*Manage Bandwidth Usage*
*View Bandwidth Reports*

## Set Up Profiling

Profiling generates information that you can analyze and use to set up your Oracle MaxRep for SAN.

When you set up profiling, you create a protection plan to gather information about the protected LUNs on your control service Oracle MaxRep Replication Engine.

1. Log in to the control service Replication Engine.
2. Navigate to **Protect** > **Profiling** > **Setup Profiling**.
3. On the Create Protection Plan page, provide a name for your profile in the **Protection Plan Name** field.
4. Select **Oracle Storage LUNs Profiling** from the **Proceed With** list to create a profile for your primary Oracle FS System and then click **Next**.
5. Provide a description for your profile and then select the name of your **Primary Oracle Storage** from the list.
6. Select the LUNs on the primary Oracle System that you want to protect in the **Select Primary LUNs** tree and then click **Next**.
7. Select the appropriate options for your profile in the Replication Options table and click **Next**.

   For information about the replication options, see Protection Plan Replication Options.
8. Review the protection plan options that you have chosen for your profile.

   To make changes to options in previous pages, click **Back**.
9. To begin collecting profiling information, click **Start Profiling**.

### Related Links

*Profiling*
*Analyze Your Profile Results*

## Analyze Your Profile Results

Analyze your profile results to find the bandwidth required to maintain a desired recovery point objective (RPO) for a single or a group of replication pairs.

The required bandwidth is calculated using the values for the following items:

- Last seven days of the data change rates for the replication pair
- Compression achieved
- Retention storage used
- Other factors

**Note:** For replication pairs that are less than seven days old, the calculation is performed based on their age.

1. Navigate to **Protect** > **Profiling** > **Analyze Your Results**.
2. In the **Protection Options** table, define values for the bandwidth parameters.
   - **Cumulative bandwidth available** in Kb/s.
   - **Desired Worst Case RPO** in minutes.
   - **Bandwidth Adjustment Factor** for network latency. The default is 0.35.
   - **Retention Window** in days. The default is 3.
3. Select one or more of the replication pairs in the **Pairs Configured** table and then click **Analyze**.
   The Pairs Configured table shows the results of the analysis. Use the results to determine if further actions or adjustments are necessary to achieve the desired RPO.
4. To see the configuration recommended for the data change rate, click **View Configuration** in the Recommended Replication Engine Configuration table.
5. To download the result to your workstation as a comma-separated value (CSV) report, click **Export to CSV**.

### Related Links

*Profiling*
*Set Up Profiling*

CHAPTER 6

# Recover Protected Data

## Data Recovery

Oracle MaxRep for SAN allows you to create and manage data recovery scenarios for Oracle FS Systems.

You can recover data by creating either physical snapshots or virtual snapshots. This data is restored from backup and rollback recovery scenarios. You can also use the disk, volume, or LUN recovery mechanisms to create or schedule recovery snapshots.

A snapshot is an accessible replica of data as it existed at a single point-in-time in the retention window. There are two types of snapshots available on the Oracle MaxRep Replication Engine: physical snapshots and virtual snapshots.

**Physical Snapshots**

A physical snapshot is a copy of the physical LUN that is created on the primary Oracle FS System. The size of the copy is equal to, or larger than, the target LUN in the replication pair. A physical snapshot creates a LUN on the target Oracle FS System that matches the state of the source LUN at the time interval specified in the recovery procedure.

The benefit of creating a physical snapshot is that you can create a LUN that is separated from the Replication Engine or replication pair. A physical snapshot creates a LUN of the same size as the original source LUN. Therefore, ensure that the target Oracle FS System has sufficient capacity to accommodate the LUN before creating the copy. For large volumes, creating the physical snapshot requires several hours to complete.

**Virtual Snapshots**

A virtual LUN is also known as a virtual snapshot, or *Vsnap*. You create virtual snapshots from the Replication Engine, not on the target Oracle FS System. Virtual snapshots require minimal system resources and load and unload quickly. Virtual snapshots use the target LUN and the data in the retention logs at a specified point in time when recovering the LUN. You can mount the virtual snapshot to any host that is mapped to the AT port of the Replication Engine.

Creating a virtual snapshot enables the recovery of the replicated LUN at any point in time that is within the protection plan retention window or sparse retention policy. Virtual snapshots are ideal for single file recovery or for verifying data integrity because they are quick to create and occupy no disk space on the target Oracle FS System.

### Related Links

*Virtual Snapshots*
*Physical Snapshots*
*Backup Recovery*
*Drive and Volume Recovery*
*Protection Plans*

## Virtual Snapshots

Virtual snapshots provide point-in-time access to a replicated LUN without the need to roll back the data on the source or target Oracle FS System or to create a LUN copy.

A virtual snapshot, called a *Vsnap*, is a virtual LUN that is created on the Oracle MaxRep Replication Engine, which then can be mounted to a host through an iSCSI target port. Virtual snapshots use the target LUN and the data in the retention logs to create a virtual image of the LUN at a specified point in time. Virtual snapshots are ideal for single file recovery or for verifying data integrity because they are quick to create and occupy no disk space on the target Oracle FS System.

Creating a virtual snapshot does not interfere with the current replication. However, writing to the virtual snapshot can affect the retention log LUN.

If a readable and writable virtual snapshot shares a LUN with the retention log of a replication pair, the capacity of the retention log LUN can fill up as changes are made to the virtual snapshot.

### Related Links

*Data Recovery*
*Create a Virtual Snapshot*
*Test a Virtual Snapshot*

### Create a Virtual Snapshot

You can create a virtual snapshot of a LUN and mount the snapshot on any host. Creating a virtual snapshot allows you to recover the replicated LUN easily at any point in time that is within the protection plan retention window or sparse retention policy.

Create virtual snapshots from the Create Recovery Snapshots page in the Oracle MaxRep GUI.

1. Navigate to **Recover** > **More** > **Create Recovery Snapshots**.
2. Select the replication pair from which to create the virtual snapshot, and then click **Recover**.
3. In the Recovery Options table, select **Recovery Based On**.

**Using Time**

Displays the **Recovery Point** options. You can specify the recovery point using one of the following methods:

- Select the tabs that specify the year, month, day, and seconds.
- Select the option **Recovery Point Accuracy** to display a graphical image of the recovery period. Use the slide bars that are located under the graph to narrow down the recovery dates. To update the graphic with your changes, click **Generate Graphs**. Continue to adjust the Recovery Point until the graphic displays the time frame that you want.

  Note: Select a recovery time that is represented as green on the graph. Data integrity is not guaranteed when you select a recovery time that is represented by any other color, such as yellow or red.

**Using Application Consistency and Event-Based**

Displays the Recovery Tag options. You can specify the search criteria to locate a specific recovery tag, or you can select a recovery tag from the available list.

Note: Select a tag that contains a green accuracy flag to ensure data integrity.

4 In the Drive Type section, select **Virtual**.

5 To enable read or write capabilities to your virtual snapshot, select **Read/Write**.

To make the virtual snapshot read only, clear the selection.

The Read/Write option requires that you provide the path location for the retention LUN.

6 (Optional) In the **Data Log Path** field, enter the data log path for the retention LUN, then click **Next**.

The retention LUN stores any writes from the host while the virtual snapshot is mapped. All such writes are deleted when the virtual snapshot is deleted.

7 To create the snapshot to the specified retention LUN, click **Export**, then click **Next**.

Note: You can make changes to the exported retention LUN. If the retention LUN does not have enough storage capacity, protection plans that use the retention LUN might pause or purge old data. The actions are defined by the protection plan retention policy.

8 Under Access Control Group Name, select the access control group to which the snapshot will be exported.

The access control group (ACG) defines the hosts that have the ability to mount and use the virtual snapshot.

9 Select a LUN number for the virtual snapshot and click **Next**.

**Note:** You cannot use LUN number 0.

10 To create the virtual snapshot, click **Finish**.

11 Review your selections, then click **Finish**.

**Important:** Mapping a virtual snapshot to the same host that has access to the source LUN of the replication pair is not a supported configuration. Virtual snapshots must be mapped to an alternate host for host access.

**Caution:** Data corruption can occur if you map the virtual snapshot to the same host as the source LUN.

**Note:** To simplify the management of the access control groups (ACGs), all the hosts present in the registered the Oracle FS System are listed under Access Control Group Information.

**Note:** Make sure that the ports of the host to which the recovery snapshot is exported are zoned in the SAN fabric using the target (AT) ports on the Replication Engine.

### Related Links

*Virtual Snapshots*
*Test a Virtual Snapshot*

## Test a Virtual Snapshot

After you have exported and mapped the virtual snapshot, you can verify that the new volume appears as a drive on the host.

1 After the system scans the host, you should see a new drive.

In Windows 2008, you might need to put the drive online by right-clicking the drive and selecting **Online**. This action should not be necessary in Windows 2003, unless the volume being replicated is a dynamic drive.

**Note:** When mapping a virtual snapshot to a host, the Replication Engine contains a LUN 0 that is visible from the Disk Management software. This LUN is for administrative purposes only; do not attempt to map to this LUN or bring it online.

2 When the drive is online, verify that it contains the following:

- A drive letter
- A visible drive label

3 Browse to the drive and verify that its contents are what you expect.

### Related Links

*Virtual Snapshots*
*Create a Virtual Snapshot*

### Delete a Virtual Snapshot

You can delete, or release, a virtual snapshot of a LUN that was previously created.

Delete a virtual snapshot from the Monitor Snapshots/Rollback Progress page located in the Oracle MaxRep GUI.

1 Navigate to **Recover** > **More** > **Monitor Snapshots/Rollback Progress**.

2 Select the virtual snapshot that you want to delete.

3 Select **Release Drive**.

**Note:** The virtual snapshot must be unexported before being deleted. To ensure that the virtual snapshot is unexported, check the box next to the vsnap, then select **Unexport**.

4 To confirm, click **OK**.
The status of the virtual snapshot displays Unmounting, and is then removed from the list. The virtual snapshot is deleted.

## Physical Snapshots

A physical snapshot is full copy of the physical source LUN on the primary Oracle FS System at a specified point in time. You can map the LUN copy from the Oracle FS System to any host that has access to the Oracle FS System SAN.

To create a physical snapshot, you capture a given point in time and create a full copy of a physical source LUN on either the primary or the secondary Oracle FS System.

From the Oracle FS System Manager, you first create a LUN on the secondary Oracle FS System. This LUN must be the same size or larger than the target LUN on the secondary Oracle FS System. Then, on the secondary Oracle FS System, you map the LUN to an appliance initiator for a target (AIT) port. The mapping enables the Oracle MaxRep Replication Engine to see the LUN, so that you can create the physical snapshot. After you release the physical snapshot, you can map the snapshot to a different host for validation.

#### Related Links

*Data Recovery*
*Create a Physical Snapshot*
*Test a Physical Snapshot*

### Create a Physical Snapshot

Create a physical snapshot of the physical source LUN to protect the data from disaster at the primary site. When the replication is local, the target LUN created from the snapshot is local; otherwise, the target LUN is remote.

1 Using the Oracle FS System Manager GUI, create a LUN on the target Oracle FS System that is the same size or larger than the target LUN.

You could thinly provision the target LUN as well. Refer to the *Oracle Flash Storage System Administrator's Guide* for information about Thin Provisioning.

2 Map the new LUN to the appliance initiator (AIT) port that is located on the target Oracle MaxRep Replication Engine.

3 Make note of the new LUN ID (LUID) of the newly created LUN to be used for the physical snapshot.

4 From the Oracle MaxRep for SAN software on the control service Replication Engine, navigate to **Recover** > **More** > **Create Recovery Snapshots**.

**Note:** You might need to rescan the Replication Engine HBAs and Oracle FS System LUNs.

5 In the Replication Pair Details table, select the replication pair for which you want to create the physical snapshot and then click **Recover**.

6 Under Recovery Options, choose whether to create the physical snapshot for a specific point in time or for an application consistency bookmark.

7 Specify the time or select a bookmark.

8 Under Drive Type, choose **Physical**.

9 Under Physical Drives, select the destination LUN.

Use the LUID you noted in Step 3 to identify the correct destination LUN.

10 Click **Next**.

**Note:** You might need to scan the Oracle Storage system and the Replication Engine to view the LUN.

11 Verify the Recovery Details and click **Finish**.

Wait until the progress reaches 100% before continuing to test the physical snapshot.

12 Using the Oracle FS System Manager, check the LUN activity in the Oracle FS System.

Look at the average I/Os and throughput values for the physical snapshot volume. Both values should be zero for the physical snapshot volume before you proceed.

**Note:** The Oracle MaxRep for SAN software prevents you from releasing the volume when the volume is busy. Verify whether the volume is busy on the Oracle FS System before you proceed.

13 From the Oracle MaxRep for SAN software, navigate to **Recover** > **More** > **Monitor Snapshot/Rollback Progress**.

14 To release the physical snapshot from the Replication Engine, select the recovery pair and click **Release Drive**.

The Release Drive process prepares the volume for use by a recovery server. The process includes unmapping the drive from the Replication Engine.

### Related Links

*Physical Snapshots*
*Test a Physical Snapshot*
*Confirm Application Consistency Virtual Snapshot*

## Test a Physical Snapshot

After you have created and released the physical drive, you can verify that the new volume appears on the host as a drive.

Validate the physical copy from the Oracle FS System Manager GUI.

1. From the Oracle FS System Manager software on the secondary Oracle FS System, navigate to **SAN** > **Storage** > **LUNs**.
2. Right-click the physical snapshot LUN and select **Modify LUN**.
3. In the Mapping tab, remove the mapping for the Oracle MaxRep Replication Engine and create the mapping for the host you will use to validate the data.
4. Perform a rescan operation to discover new volumes.
5. Assign this volume, or partition, a drive letter.

   If you have already assigned a drive letter on this server, the server might reuse your settings automatically when the drive comes online. Otherwise, assign an unused drive letter.
6. Inspect the drive and verify the data.

### Related Links

*Physical Snapshots*
*Create a Physical Snapshot*

# Backup Recovery

You can use rollback scenarios to set up an automated backup policy that creates a physical snapshot or a virtual snapshot on a backup media server. Virtual snapshots are preferred for backups.

**Important:** A data rollback can be only performed once. After the data is rolled back, the protection plan cannot be rolled back to another point in time. Before performing a rollback, use a virtual snapshot or a physical snapshot first to ensure that you are selecting the appropriate rollback time period.

When you create a rollback scenario, the protection plan status does not change. The rollback has no affect on the protection plan until you run it. This means you can create the rollback scenario for the protection plan before you need it for disaster recovery. The rollback scenario saves you recovery time at the secondary

location in the event of a disaster. To run a rollback scenario, see *Run a Backup/Rollback Scenario*.

Use rollback scenarios in an asynchronous replication configuration to set up a policy for rolling back data that is saved on the secondary site.

### Related Links

*Data Recovery*
*Virtual Snapshots*
*Create a Backup Scenario*
*Create a Rollback Scenario*

## Create a Backup Scenario

You can create a continuous backup of the replicated data of the secondary Oracle MaxRep Replication Engine without disrupting ongoing replication.

1. Navigate to **Recover** > **Data Validation and Backup** > **Create Backup Scenario**.
2. Select the protection plan to which you want to add the backup scenario from the **Select Plan** drop-down list and then click **Next**.
3. Select the **Drive Type**.
   Valid types:
   - **Virtual** (recommended for backups)
   - **Physical**
4. Select **Read/Write** to provide read and write access to the backup snapshot.

   **Tip:** For backups, you might not want to select this option unless your backup software requires read and write access to the source data.
5. Click **Next**.
6. Choose the **Execution Type**.
   Valid types:
   - **Scheduled**
   - **Run On demand**
7. (Optional) If you selected **Scheduled**, choose the basis for the scenario in the Recovery Based On table.
   Valid schedule types:

   **Time-Based**

   Schedules the scenario to run on a regular basis. Specify when and how often to run the scenario.

**Event-Based**

The scenario is run once when the specified application consistency bookmark is received. Select **Standard bookmark prefixes** to display a list of event-based prefixes.

8 To run one or more scripts on your specified backup server before or after the scenario runs, specify the fully qualified path for the scripts.

9 Click **Save**.
The backup scenario displays in the Recovery Scenarios table.

### Related Links

*Backup Recovery*
*Create a Rollback Scenario*

## Create a Rollback Scenario

You can create a scenario whereby the target LUNs are designated for backup but not made available to administrators or applications. The LUNs can be recovered (rolled back) to a point in time for recovery purposes.

During normal replication, a target LUN is reserved and not accessible by administrators or applications. If there is a disaster at the source location, create a rollback scenario of the LUN. A rollback scenario allows you to recover the data at any historic point-in-time that has been stored in the retention period. The rollback process promotes the target LUN as the new source LUN. You can then mount this LUN to a host until the primary location is fully recovered and available.

During the rollback, replication stops and suspends any policies that are associated with the replication pair. When the rollback completes, the changes from the retention log are applied to the target LUN for the replication pair.

**Note:** LUN rollback is an irreversible process. The data on the target LUN is permanently modified and the retention log data is lost for that LUN. Perform the rollback only if you are certain that the data for the particular rollback period is needed.

**Note:** Oracle recommends that you create a virtual snapshot of the historical data. The virtual snapshot retains the integrity of the target LUN and permits you to verify the integrity of the data that you want to roll back.

1 Navigate to **Recover** > **Create Rollback Scenario**.

2 Select the protection plan to which you want to add the rollback scenario from the **Select Plan** list.

3 Select the primary server and failover server for the rollback in the Select Protection list.

4 Click **Next**.

5 Verify the rollback options in the Pair Details listing and then click **Next**.

6 Verify the rollback plan and rollback scenario details and then click **Save**.

### Related Links

*Backup Recovery*

*Run a Backup or Rollback Scenario*

## Run a Backup or Rollback Scenario

Run a backup or rollback scenario when you need to recover a LUN from a specific point in time of a recovery period. The backup or rollback scenario is actived when you set the scenario to an active run state.

**Note:** LUN rollback is an irreversible process. The data on the target LUN is permanently modified and the retention log data is lost for that LUN. Perform the rollback only if you are certain that the data for the particular rollback period is needed.

1 Navigate to **Recover** > **Data Validation and Backup** > **Manage Backup/ Rollback Scenarios**.

2 From the **Recovery Scenarios** table, click **Run** for the protection plan that contains the desired scenario.

**Tip:** You can filter the protection plan list by selecting the **Plan Name** or the **Recovery Scenario** options that are located above the **Recovery Scenarios** table.

3 From the **Use custom consistent point/time** table, click **Select** for whether you want to use consistency point or time-based recovery methods.

**Consistent Point Based Recovery**

Displays the Recovery Tag options. You can specify the search criteria to locate a specific recovery tag, or you can select a recovery tag from the available list.

**Note:** Select a tag that contains a green accuracy flag to ensure data integrity.

**Recovery Time**

Displays the **Recovery Point** options. You can specify the recovery point using one of the following methods:

- Select the tabs that specify the year, month, day, and seconds.
- Select the option **Recovery Point Accuracy** to display a graphical image of the recovery period. Use the slide bars that are located under the graph to narrow down the recovery dates. To update the graphic with your changes, click **Generate Graphs**. Continue to adjust the Recovery Point until the graphic displays the time frame that you want.

**Note:** Select a recovery time that is represented as green on the graph. Data integrity is not guaranteed when you select a recovery time that is represented by any other color, such as yellow or red.

4 Verify the information on the Review page, and then click **Run**.
The system displays the Recovery Scenarios table again.

5 Verify that the backup scenario Execution Status field displays **Active**.

### Related Links

*Backup Recovery*
*Recovery Point Accuracy Page*
*Create a Rollback Scenario*

## Recovery Point Accuracy Page

Allows you to accurately select the recovery point for your rollback scenario.

### Pair Details

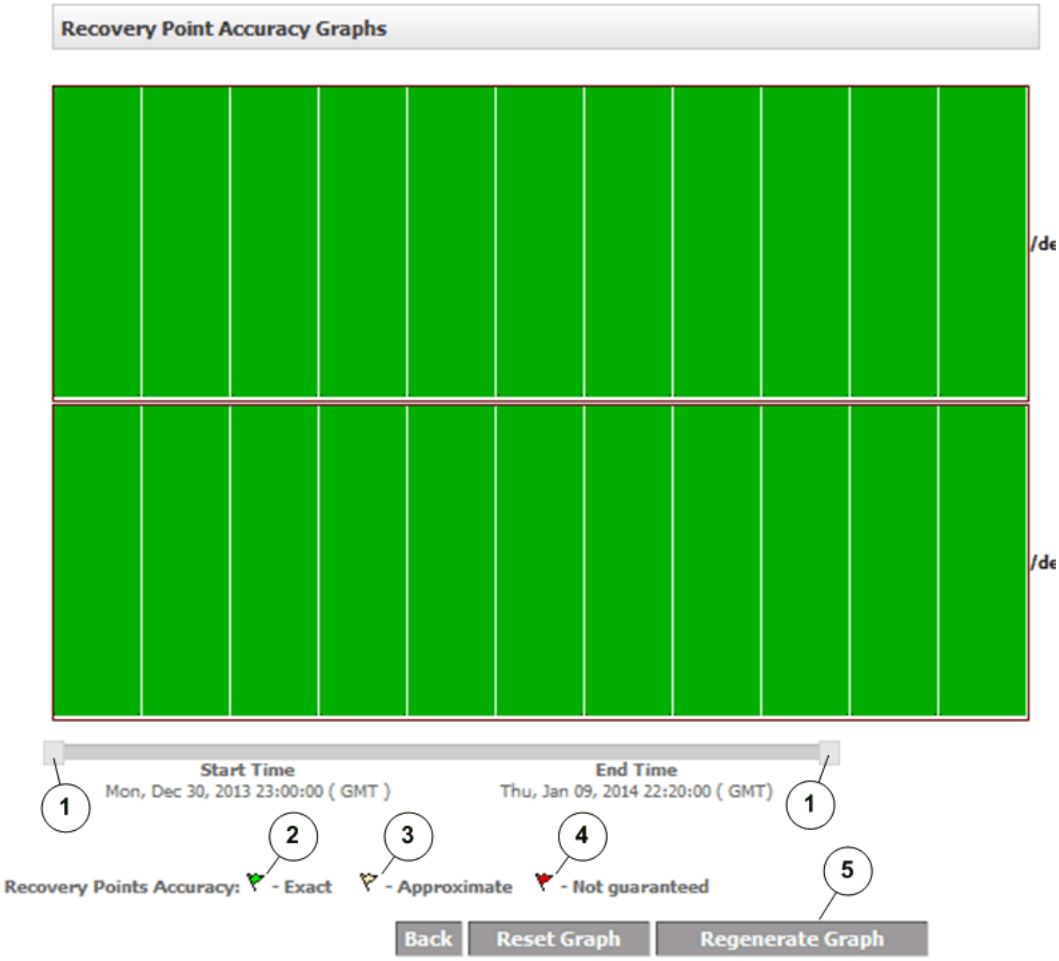
Provides the details about the selected replication pair.

| | |
|---|---|
| **Server** | Indicates the name of the server that contains the source LUN of the replicated pair. |
| **Primary Volume** | Indicates the source LUN ID (LUID) of the replication pair. |
| **Remote Server** | Indicates the name of the server that contains the target LUN of the replicated pair. |
| **Target Volume** | Indicates the target LUN ID (LUID) of the replication pair. |

### Recovery Point Accuracy Graphs

Provides a detailed graph that represents the start and end dates and times for the recovery period.

Figure 15: Recovery point accuracy graph




**Legend**

| | |
|---|---|
| 1 Start and end time slider bar handles | 4 Data integrity is not guaranteed |
| 2 Data integrity is guaranteed | 5 Refreshes the graph |
| 3 Data integrity is approximate and not guaranteed | |

# Drive and Volume Recovery

You can create a snapshot schedule that creates recovery snapshots on a regular basis. You can also roll back a LUN on your secondary Oracle FS System to a previous time or to a recovery point.

**Scheduled snapshot**

Creates a scheduled recovery snapshot for a specified time and frequency.

**Secondary Oracle Storage rollback**

Creates a LUN on the secondary Oracle FS System you can roll back to a specified time or to a specific application consistency bookmark.

### Related Links

*Data Recovery*
*Schedule Recovery Snapshots*
*Perform Secondary LUN Rollback*

## Schedule Recovery Snapshots

You can schedule a recovery snapshot, which is an exact replica or point-in-time copy of the target LUN. A recovery snapshot provides uninterrupted replication.

When the continuous data protection (CDP) retention option is set for the replication pair, recovery is possible for any point in time within the retention window. A *retention window* is the time span that the retention logs are available on the target Oracle FS System. Without the recovery snapshot, data recovery only includes the data at the time the replication was initiated.

1. Navigate to **Recover** > **More** > **Create Scheduled Snapshots**.
2. Select the replication pair and click **Create Snapshot**.
3. Follow the instructions for creating a physical snapshot or a virtual snapshot.

   **Important:** You must select the **Time Based** option under Type of Snapshot and press enter to create a scheduled copy or snapshot.
4. In the Snapshot Schedule table, select **Scheduled** and specify a frequency and time for the scheduled copy or snapshot to be created.
5. To export your scheduled copy or snapshot, select **Export** under Export Options.

### Related Links

*Drive and Volume Recovery*
*Replication Options*
*Create a Physical Snapshot*
*Create a Virtual Snapshot*

## Perform Secondary LUN Rollback

After creating the rollback scenario, you can rollback a secondary LUN to a specified recovery point.

The Replication Pair Details table lists all of the replication pairs that are not included in a protection plan.

1. Navigate to **Recover** > **More** > **Disk/Volume/LUN Recovery** > **Perform Secondary LUN Rollback**.
2. Select a replication pair.

   **Note:** Select a pair or click **Search** to list only those pairs on a specified source host, target host, or volume.

3 Click **View Recovery Range** to view the Recovery Point Accuracy graphs for the selected pair or group of pairs.

Select the option **Recovery Point Accuracy** to display a graphical image of the recovery period. Use the slide bars that are located under the graph to narrow down the recovery dates. To update the graphic with your changes, click **Generate Graphs**. Continue to adjust the Recovery Point until the graphic displays the time frame that you want.

**Note:** Select a recovery time that is represented as green on the graph. Data integrity is not guaranteed when you select a recovery time that is represented by any other color, such as yellow or red.

4 Click **Rollback**.

5 To approve deletion of the replication pair, click **OK**.

6 To approve deletion of the retention logs, click **OK**.

7 Select an option from the Recovery Options table.

**Using Time**

Provide the required date and time, or click **Recovery Point Accuracy** to use the Recovery Point Accuracy graphs to choose the accurate time to create the recovery snapshot.

**Using Application Consistency Event Based**

Select a recovery tag or search for a particular tag for any of the following options:

- Particular date or a range of dates
- Particular application
- User defined event
- Tag name
- Accuracy
- Display the recent consistency point

8 To start the secondary LUN rollback, click **Save**.

## Related Links

*Drive and Volume Recovery*
*Recovery Point Accuracy Page*
*Create a Rollback Scenario*
*Run a Backup or Rollback Scenario*

APPENDIX A

# Oracle MaxRep Support User Interface

## About the Support User Interface

Oracle MaxRep for SAN provides an Oracle MaxRep Support User Interface (Support UI) that allows you to configure all of the Oracle MaxRep Replication Engines that are accessible in your network environment.

The Support UI issues commands to the Oracle MaxRep Support Agent. When using this interface, you do not need log into the Replication Engine server as **`root`** at the OS level: all changes are managed by the Support Agent.

The Support UI runs from a web page that is separate from the Oracle MaxRep for SAN software. The interface is divided into two groups: Task Status and Audit Logs, and Management Tasks.

The Task Status and Audit Logs group includes the following items:

| | |
|---|---|
| **Dashboard** | Provides an overview of the Oracle MaxRep Replication Engine network configuration and health. You can access many of the management tasks from this page by clicking the edit icon (  ) next to the status item. |
| **Task Status** | Provides a summary of the pending, in progress, and completed tasks. |
| **Audit Logs** | Provides a summary of the completed tasks and activity by the Support UI. |

The Management Tasks group includes the following items:

| | |
|---|---|
| **Shutdown/Restart Services** | Allows you to manage the replication services that are running on the Replication Engine as well as shutdown or reboot the entire Replication Engine. |
| **Configure Host Name** | Allows you to assign your Replication Engine host IP address to a user-friendly name. |
| **Configure Networking** | Allows you to assign IP addresses in your network to Ethernet ports on the Replication Engine. |
| **Configure DNS** | Allows you to assign the Replication Engine to a domain and set the available Domain Name Servers (DNS) on the network. |
| **Set Time Zone** | Allows you to set the Replication Engine to a specific time zone. |

| | |
|---|---|
| **Set NTP Server** | Allows you to specify the servers on the network that run Network Time Protocol (NTP) to synchronizes the Replication Engine clocks with a standard time. |
| **Modify HTTP Server Document Root** | Allows you to move the HTTP server document root from the Replication Engine to a LUN on the Oracle FS System. |
| **Move Cache Directory** | Allows you to move the process server cache to a LUN on the Oracle FS System. |
| **Change Configuration Server** | Allows you to specify an alternate Replication Engine as the configuration server. |
| **Configure MaxRep HA** | Allows you to configure two Replication Engines as high availability pair. |
| **Software Updates** | Allows you to update the Oracle MaxRep software. |
| **ILOM Configuration** | Allows you to configure the integrated lights out manager (ILOM) network configuration and configure the Call-Home trap receiver with the Oracle FS System. |

### Related Links

*Log In to the Support Interface*
*View the MaxRep Support Dashboard*
*View the Replication Engine Audit Logs*
*View the Replication Engine Task Status*

## Log In to the Support Interface

Log in to the Oracle MaxRep Support User Interface to perform maintenance tasks on the Oracle MaxRep Replication Engine, monitor support activities on the Replication Engine, and review the task logs.

When logging into the Support UI use the configuration Replication Engine.

1. Start a web browser from your workstation.
2. Enter the URL to the Support UI page.

   **`http://system-name-ip/support`**

   Where *system-name-ip* is the name or the public IP address for the control service Replication Engine.
3. Enter the user name and password.
   The Oracle MaxRep Support User Interface dashboard displays.

### Related Links

*View the MaxRep Support Dashboard*

## View the MaxRep Support Dashboard

The Oracle MaxRep Support User Interface (Support UI) Dashboard provides an overview of the Replication Engine network settings and system health.

The dashboard is the first page that displays when you log in to the Support UI.

1. Log in to the Support UI page from the control service Replication Engine. The Dashboard page displays.
2. Review the displayed information to ensure that the Replication Engine details are what you expect.

You can access many of the management tasks from this page by clicking the edit icon ( ) next to the status item.

### Related Links

*Dashboard Page*
*Log In to the Support Interface*

## Dashboard Page

Displays the network status and heath of the registered Oracle MaxRep Replication Engines.

To display details of a specific Replication Engine host, select the name from the tab or the **Host** list.

### Server Details

You can access many of the management tasks from this page by clicking the edit icon ( ) next to the status item.

**Host Name**

Identifies the host name of the registered Replication Engine.

**Domain Name**

Identifies the name of the domain name of the registered Replication Engine.

**Domain Name Server**

Identifies the IP addresses of the primary and secondary Domain Name Severs (DNS) that are used to resolve the fully qualified host name.

**Time Zone**

Identifies the time zone of the registered Replication Engine.

**NTP Server**

Identifies the IP addresses of the Network Time Protocol (NTP) servers.

**Note:** The servers should be the same as that used by the Oracle FS System.

**HTTP Document Root is mounted on**

Indicates the path name and storage capacity for the HTTP documentation root volume. This entry is one of the following items:

- The path name of the `/home` directory.
- The LUN identifier (LUID) when the document root is moved to an Oracle FS System LUN that is mapped to the Replication Engine.

**Cache Directory is mounted on**

Indicates the path name and storage capacity for the cache directory volume. This entry is one of the following items:

- The path name of the `/home` directory.
- The LUN identifier (LUID) when the cache directory is moved to an Oracle FS System LUN that is mapped to the Replication Engine.

**Versions and Updates**

Indicates the version number Replication Engine software. Selecting the version number link displays a history of the software updates.

**Replication Services**

Indicates the health of the replication services. Selecting the health status link displays a summary of the replication services.

**Role**

*(HA configurations only)* Indicates the status of the HA Replication Engine mode.

Possible states:

**Active**

The Replication Engine is actively replicating data.

**Passive**

The Replication Engine is in standby mode in the event of a failure of the primary Replication Engine.

## Network Details

Displays the overview of the Replication Engine network connections.

**Interface**

Indicates the name of the bonded port interface. The names of the interface coincides with the connection port type that are used on the Replication Engine.

**Slaves**

Indicates the port identifier that is located on the back of the Replication Engine of any ports that are included in the bonded interface.

**IP Address**

Indicates the port IP address.

**Network Mask**

Indicates the port network mask for the port IP address.

**Gateway**

Indicates the IP address of the port gateway router.

**DNS**

Indicates the domain name server (DNS) for the port, if configured.

### Related Links

*View the MaxRep Support Dashboard*

## View the Replication Engine Audit Logs

Access the audit logs when you need to review a summary of the completed tasks and activity by the Oracle MaxRep Support User Interface.

1. Log in to the Support UI page from the control service Replication Engine. The Dashboard page displays.
2. To view the audit logs, choose **Task Status/Audit Logs** > **Audit Logs**.
3. Review the displayed information to ensure that the Replication Engine details are what you expect.

### Related Links

*Audit Logs Page*
*Log In to the Support Interface*

## Audit Logs Page

Displays a list of completed and failed tasks by the Oracle MaxRep Support Agent.

Oracle Customer Support might ask you to access information on this page to assist with troubleshooting your system.

**User**

Identifies the user name that performed the task.

**IP Address**

Identifies the IP address of the host from which the task was performed.

**Log Details**

Identifies the detailed record of the performed task.

**Time**

Identifies the time stamp that the task occurred.

### Related Links

*View the Replication Engine Audit Logs*

## View the Replication Engine Task Status

Access the audit logs when you need to review a summary of the pending, current, and completed tasks and activity by the Oracle MaxRep Support User Interface.

1. Log in to the Support UI page from the control service Replication Engine. The Dashboard page displays.
2. To view the task status, navigate to **Task Status/Audit Logs** > **Task Status**.
3. Review the displayed information to ensure that the Replication Engine details are what you expect.

### Related Links

*Task Status Page*

*Log In to the Support Interface*

## Task Status Page

Displays a list of pending, current, and completed tasks by the Oracle MaxRep Support Agent.

The Task Status page allows you to view details about the tasks performed by the Support Agent.

**Sl No**

Identifies the task number.

**Task title**

Identifies the name of the requested task from the Support User Interface.

**Host**

Identifies the name of the Oracle MaxRep Replication Engine host from which the administrator issued the task.

**Last Update time**

Identifies the time stamp that the task occurred.

**Status**

Identifies the state of the requested task.

Possible states:

**Completed**

Indicates that the task finished without errors.

**In Progress**

Indicates that the Support Agent is currently performing the requested task.

**Pending**

Indicates that the requested task is in queue.

**Failed**

Indicates that the requested task did not finish. Click **View** to display the task details.

**Action**

Identifies the possible commands that you can perform for the specific task.

Possible actions:

**View**

Allows you to display the task details.

**Delete**

The **Delete** action has a different meaning depending on the state of the task.

- If the task state is **In Progress** or **Pending**, **Delete** allows you to cancel the requested task.

  **Note:** During the progress of performing your task, the Support Agent cannot abandon the progress. If this is the case, the **Delete** link is not available.

- If the task state is **Completed** or **Failed**, **Delete** allows you to remove the item from the list.

  **Note:** Delete does not reverse the action of the task. The audit log displays a record of the completed task.

### Related Links

*View the Replication Engine Task Status*

## Replication Engine Management

You can perform various tasks on the Oracle MaxRep Replication Engine using the Oracle MaxRep Support Agent that runs the commands that select from the Support User Interface.

The tasks that you can perform on the Replication Engine host include the following:

- Stop and start the replication services
- Shutdown and restart the Replication Engine
- Reboot the Replication Engine

- Configure a host name for the Replication Engine
- Configure the Replication Engine network
- Configure the Domain Name Server (DNS)
- Set the Replication Engine time zone
- Set the Replication Engine Network Time Protocol (NTP) server
- Modify the Replication Engine HTTP documentation root path
- Modify the Replication Engine cache path
- Change the Replication Engine configuration server
- Configure Oracle MaxRep High Availability (HA)
- Update the Replication Engine software
- Configure the Integrated Lights Out Manager (ILOM) for Oracle MaxRep for SAN

### Related Links

*About the Support User Interface*

## Stop Replication Services

You might want to stop the replication services for all protection plans on the Oracle MaxRep Support User Interface.

Use the Oracle MaxRep Support User Interface to stop the replication services. Run the Support UI from a separate web page than the Oracle MaxRep for SAN software.

**Caution:** Stopping the replication services stops all data replication services. In some circumstances, a resynchronization might be required when the services are restarted. To avoid the resynchronization, use the stop command when the Replication Engine is not backing up data.

1. Log in to the Support User Interface page on the control service Replication Engine.
   The Dashboard page displays.
2. Click the **Management Tasks** > **Shutdown/Restart Services** link.
3. From the **Host** list, select the Replication Engine that is running the Oracle MaxRep replication services.
4. Select **Stop Replication Services**.
5. To stop the replication services, click **Save Task**.

When the replication services stop, all replication to and from the Replication Engine halts. To resume replication services, use the **Start Replication Services** option.

### Related Links

*Log In to the Support Interface*
*Start Replication Services*
*Resync a Protection Plan*

## Start Replication Services

Start the replication services if these services have been stopped for some reason.

Use the Oracle MaxRep Support User Interface to start the replication services. Run the Support UI from a separate web page than the Oracle MaxRep for SAN software.

1. Log in to the Support User Interface page on the control service Replication Engine.
   The Dashboard page displays.
2. Click the **Management Tasks** > **Shutdown/Restart Services** link.
3. From the **Host** list, select the Replication Engine that is running the Oracle MaxRep replication services.
4. Select **Start Replication Services**.
5. To start the replication services, click **Save Task**.

When the replication services start, all replication resumes.

### Related Links

*Log In to the Support Interface*

## Restart the Replication Engine

Restart the Oracle MaxRep Replication Engine when you need to restart the operating system of the Replication Engine.

Restart the Replication Engine, which is running the replication services, using the Oracle MaxRep Support User Interface. Run the Support UI from a separate web page than the Oracle MaxRep for SAN software.

**Caution:** Restarting the replication services stops all data replication services. In some circumstances, a resynchronization might be required when the services are restarted. To avoid the resynchronization, use the stop command when the Replication Engine is not backing up data.

**Note:** If you are restarting the control service Replication Engine, the web services that run the Oracle MaxRep for SAN GUI and the Support UI also restart. These interfaces are not accessible until the control service Replication Engine restart has completed.

1. Log in to the Support User Interface page on the control service Replication Engine.

The Dashboard page displays.

2 Click the **Management Tasks** > **Shutdown/Restart Services** link.

3 From the **Host** list, select the Replication Engine that is running the Oracle MaxRep replication services.

4 Select **Restart Replication Services**.

5 To restart the replication services, click **Save Task**.

If you restarted the control service Replication Engine, the web services that run the Oracle MaxRep for SAN GUI and the Support UI also restart. These interfaces are not accessible until the control service Replication Engine restart has completed.

In some circumstances you might also need to perform a resychronization of your protection plans after the Replication Engine has restarted.

### Related Links

*Log In to the Support Interface*
*Resync a Protection Plan*

## Shutdown the Replication Engine

You might need to shutdown the Oracle MaxRep Replication Engine for maintenance.

Shutdown the Replication Engine, which is running the replication services, using the Oracle MaxRep Support User Interface. Run the Support UI from a separate web page than the Oracle MaxRep for SAN GUI.

**Caution:** Shutting down the Replication Engine stops all data replication services. In some circumstances, a resynchronization might be required when the services are restarted. To avoid the resynchronization, use the stop command when the Replication Engine is not backing up data.

**Note:** If you are shutting down the control service Replication Engine, the web services that run the Oracle MaxRep for SAN GUI and the Support UI also shut down. These interfaces are not accessible until the control service Replication Engine restart has completed.

1 Log in to the Support User Interface page on the control service Replication Engine.
The Dashboard page displays.

2 Click the **Management Tasks** > **Shutdown/Restart Services** link.

3 From the **Host** list, select the Replication Engine that is running the Oracle MaxRep replication services.

4 Select **Shutdown**.

5 To shutdown the replication services, click **Save Task**.

If you shut down the control service Replication Engine, the web services that run the Oracle MaxRep for SAN GUI and the Support UI also shut down. These

interfaces are not accessible until the control service Replication Engine restart has completed. Restart the Replication Engine manually, or by using the ILOM facility to power-on the Replication Engine.

### Related Links

*Log In to the Support Interface*
*Resync a Protection Plan*

## Reboot the Replication Engine

You might be requested by Oracle Customer Support to reboot the Replication Engine, which power-cycles the Replication Engine and then restarts all services.

Reboot the Replication Engine, which is running the replication services, using the Oracle MaxRep Support User Interface. Run the Support UI from a separate web page than the Oracle MaxRep for SAN software.

**Note:** If you are restarting the control service Replication Engine, the web services that run the Oracle MaxRep for SAN GUI and the Support UI also restart. These interfaces are not accessible until the control service Replication Engine restart has completed.

In some circumstances, when the reboot completes, you might need to resynchronize some of the protection plans.

1. Log in to the Support User Interface page on the control service Replication Engine.
   The Dashboard page displays.
2. Click the **Management Tasks** > **Shutdown/Restart Services** link.
3. From the **Host** list, select the Replication Engine that is running the Oracle MaxRep replication services.
4. Select **Reboot**.
5. To reboot the replication services, click **Save Task**.

If you rebooted the control service Replication Engine, the web services that run the Oracle MaxRep for SAN GUI and the Support UI also restart. These interfaces are not accessible until the control service Replication Engine restart has completed.

Access the Oracle MaxRep GUI and resynchronize your protection plans, as needed.

### Related Links

*Log In to the Support Interface*
*Resync a Protection Plan*

## Configure Replication Engine Host Name

Renaming the Oracle MaxRep Replication Engine makes the Replication Engine easier to identify.

When the Replication Engine is first installed, the default host name is `MaxRepOS 10.0.0.11`. Renaming allows you to specify a meaningful host name that makes the host easy to identify. Oracle recommends that you rename the host before performing other configuration tasks on the Replication Engine. The new name takes a few minutes to process through the network.

1. Start a web browser from your workstation.
2. Enter the URL to the Support UI page.
   **`http://10.0.0.11/support`**
3. Enter the user name and password.
   The Oracle MaxRep Support User Interface dashboard displays.
4. Click the **Management Tasks** > **Configure Hostname** link.
5. From the **Host** list, select the Replication Engine that is running the Oracle MaxRep replication services.
6. Enter a new name for the Oracle MaxRep Replication Engine in the **Hostname** field.
7. To rename the Replication Engine host, click **Save Hostname**.

Allow a few minutes for the new host name to process through the system and the Support UI screens.

You can monitor this task from the Task Status page. It might take a few minutes for the hostname to display in the Dashboard after the task has successfully completed.

### Related Links

*Log In to the Support Interface*
*View the Replication Engine Task Status*
*View the MaxRep Support Dashboard*

## Configure Replication Engine Networking

Configure the network settings on the Oracle MaxRep Replication Engine when you need to update the port information that was configured during the initial installation.

Update the network settings if any of the port IP addresses, subnet mask, or default gateway information has changed.

1. Log in to the Support User Interface page on the control service Replication Engine.
   The Dashboard page displays.
2. Select **Management Tasks** > **Configure Networking**.

3 From the **Host** list, select the host that is running the Oracle MaxRep replication services.
The screen updates with an image of the Replication Engine network connections. The system also displays a table of the current network settings.

4 To edit the port network settings, click the link for that port.
Available settings includes:

- **IP Address**
- **Network Mask**
- **Gateway**
- **DNS** (Optional)

5 To save the network settings, click **Save**.

6 (Optional) Edit more port settings by clicking the link that is next to the port.

**Note:** Configure all of the interfaces before saving the task.

7 To save all of your network changes, click **Save Task**.

When you save your changes, the system displays the **Task Status** page. You can monitor the task progress and, in some cases, cancel the change from this page.

### Related Links

*Log In to the Support Interface*
*View the Replication Engine Task Status*

## Configure Replication Engine DNS Server

You can configure the Domain Name Server (DNS) domain name and servers for the Oracle MaxRep Replication Engine. DNS is the TCP/IP protocol that allows you use names rather than IP address numbers to refer to the Support UI host computer.

You can define a primary DNS server and a secondary DNS server. The system uses the primary DNS server to resolve host names into IP addresses. If the primary server cannot be reached, the system uses the secondary DNS server.

1 Log in to the Support User Interface page on the control service Replication Engine.
The Dashboard page displays.

2 Select **Management Tasks** > **Configure DNS**.

3 From the **Host** list, select either a single host, or select **All Servers** to select the Replication Engines that are available in the replication configuration.

4 Enter the **Domain Name**.

5 Enter the **DNS Name Server**.

**Note:** Separate multiple DNS name server entries with commas.

6 To set the DNS server names, click **Save DNS Details**.

When you save your changes, the system displays the **Task Status** page. You can monitor the task progress and, in some cases, cancel the change from this page.

### Related Links

*Log In to the Support Interface*
*View the Replication Engine Task Status*

## Set the Replication Engine Time Zone

You can set the time zone offset for the Oracle MaxRep Replication Engine. You might need to set the time zone if your remote and local Replication Engines are located in different time zones.

1 Log in to the Support User Interface page on the control service Replication Engine.
The Dashboard page displays.

2 Select **Management Tasks** > **Set Timezone**.

3 From the **Host** list, select either a single host, or select **All Servers** to select the Replication Engines that are available in the replication configuration.

4 From the **Time Zone** list, select the time zone to apply to the selected Replication Engine.

5 To set the time zone setting, click **Save Time Zone**.

When you save your changes, the system displays the **Task Status** page. You can monitor the task progress and, in some cases, cancel the change from this page.

### Related Links

*Log In to the Support Interface*
*View the Replication Engine Task Status*

## Configure Replication Engine NTP Server

You can synchronize the Oracle MaxRep Replication Engine time clock with the Oracle FS System by configuring the Network Time Protocol (NTP) server. Synchronizing the time clocks ensures that the timestamps from all of the log files are the same across the data network.

**Prerequisites**

The NTP server names or IP addresses that are used by the connected Oracle FS System.

1 Log in to the Support User Interface page on the control service Replication Engine.

The Dashboard page displays.

2 Select **Management Tasks** > **Configure NTP**.

3 From the **Host** list, select either a single host, or select **All Servers** to select the Replication Engines that are available in the replication configuration.

4 In the **NTP Server 1** field, enter the IP address or DNS names of the primary NTP server.

5 Add alternate IP addresses or DNS names to act as the secondary (**NTP Server 2)**) and tertiary (**NTP Server 3**) servers.
If the primary NTP server is unavailable, the system consults the alternate servers in round-robin fashion until the Replication Engine connects to an available NTP server. Enter IP addresses for up to two alternate NTP servers.

6 To set the NTP servers, click **Save Task**.

When you save your changes, the system displays the **Task Status** page. You can monitor the task progress and, in some cases, cancel the change from this page.

### Related Links

*Log In to the Support Interface*
*View the Replication Engine Task Status*

## Modify HTTP Server Document Root

You can move the default document root folder for the Oracle MaxRep Replication Engine web server to a LUN on the Oracle FS System.

**Prerequisites**

- An Oracle FS System LUN that is configured with the *Oracle MaxRep Home* storage profile.

  **Note:** Create the LUN on the an Oracle FS System that is on the same SAN fabric as the Replication Engine.

- The new LUN is mapped to the Replication Engine. Use the Map LUN action from the Toolkit for MaxRep of the Oracle MaxRep GUI.

At the time of installation, the home LUN is configured on the Replication Engine. The home LUN is the cache directory for the web server, configuration files, and replication data and as a result, can be IOP intensive. If your system configuration is very large or you need faster drive access to cache your data or web server, you can move the home LUN to the Oracle FS System. There are several factors that can affect home LUN performance such as the amount of replicated pairs and their associated change rates.

1 Log in to the Support User Interface page on the control service Replication Engine.

The Dashboard page displays.

2 Select **Management Tasks** > **Modify HTTP Server Document Root**.

3 From the **Host** list, select the Replication Engine that is running the Oracle MaxRep replication services.

4 From the **Path** field, select the available path name for the cache folder.

5 To set the new path, click **Save Task**.

When you save your changes, the system displays the **Task Status** page. You can monitor the task progress and, in some cases, cancel the change from this page.

### Related Links

*Log In to the Support Interface*
*View the Replication Engine Task Status*
*Map LUNs*

## Move Cache Directory

You can move the default cache directory from the Oracle MaxRep Replication Engine to the Oracle FS System.

**Prerequisites**

- An Oracle FS System LUN that is configured with the *Oracle MaxRep Home* storage profile.

  **Note:** Create the LUN on the an Oracle FS System that is on the same SAN fabric as the Replication Engine.

- The new LUN is mapped to the Replication Engine. Use the Map LUN action from the Toolkit for MaxRep of the Oracle MaxRep GUI.

At the time of installation, the home LUN is configured on the Replication Engine. The home LUN is the cache directory for the web server, configuration files, and replication data and as a result, can be IOP intensive. If your system configuration is very large or you need faster drive access to cache your data or web server, you can move the home LUN to the Oracle FS System. There are several factors that can affect home LUN performance such as the amount of replicated pairs and their associated change rates.

As a general guideline, when the number of replicated pairs for a home LUN reaches 50, Oracle recommends moving the home LUN to external storage. When you create the new LUN use the Storage Profile, *Oracle MaxRep Home*.

1 Log in to the Support User Interface page on the control service Replication Engine.
The Dashboard page displays.

2 Select **Management Tasks** > **Move Cache Directory**.

3 From the **Host** list, select the Replication Engine that is running the Oracle MaxRep replication services.

4 From the **Path** field, select the available path name for the cache folder.

5 To set the new path, click **Save Task**.

When you save your changes, the system displays the **Task Status** page. You can monitor the task progress and, in some cases, cancel the change from this page.

### Related Links

*Log In to the Support Interface*
*View the Replication Engine Task Status*
*Map LUNs*

## Change Configuration Server

You can change the location of the Oracle MaxRep Replication Engine configuration server.

At the time of installation, each Replication Engine is configured as a control service Replication Engine. Each Oracle MaxRep configuration that is replicating data includes only one Replication Engine that acts as the control service Replication Engine. During installation, direct any additional Replication Engines to this control service Replication Engine. After initial installation, changing the control service is uncommon. Oracle recommends that you contact Oracle Customer Support before moving the configuration server in these circumstances.

1 Log in to the Support User Interface page on the control service Replication Engine.
The Dashboard page displays.

2 Select **Management Tasks** > **Change Configuration Server**.

3 From the **Host** list, select the Replication Engine that is running the Oracle MaxRep replication services.

4 Enter the IP address or DNS name of the desired Replication Engine host in the **Primary Configuration Server IP** field.

5 To save your changes, click **Save Details**.

When you save your changes, the system displays the **Task Status** page. You can monitor the task progress and, in some cases, cancel the change from this page.

### Related Links

*Log In to the Support Interface*
*View the Replication Engine Task Status*

## Configure Oracle MaxRep High Availability

You can configure two Oracle MaxRep Replication Engines as a clustered high availability (HA) pair.

**Prerequisites**

HA Cluster information includes:

- IP address or host name
- Multicast Group IP address
- Ping node IP address

Primary and secondary node information includes:

- IP address or host name
- Fully qualified domain name

Two Replication Engines make up an HA cluster. One Replication Engine is in Active mode, while the other Replication Engines is in Standby, or Passive mode. Both of the Replication Engines in the cluster use the same multicast group IP address.

After you configure the HA environment, you cannot access the Oracle MaxRep Support User Interface from the cluster IP address or host name. Instead, update the individual Replication Engine host name.

Important: Configuring HA in the Oracle MaxRep for SAN environment is a one-way process. If you change your mind and want to configure your system as non-high availability, then you must start the configuration process from the beginning, which might also include reinstalling the Replication Engine image.

1. Log in to the Support User Interface page on the control service Replication Engine.
   The Dashboard page displays.
2. Select **Management Tasks** > **Configure MaxRep HA**.
3. Select the **Primary Node** Replication Engine.
4. Enter the **Domain Name of Primary Node**.
5. Select the **Seondary Node** Replication Engine.
6. Enter the **Domain Name of Secondary Node**.
7. Enter the remaining HA configuration information:
   - **Multicast Group IP Address**
   - **Ping Node**
   - **Cluster IP Address**
   - **Appliance HA Cluster Name**
8. To save your changes, click **Save HA Details**.

When you save your changes, the system displays the **Task Status** page. You can monitor the task progress and, in some cases, cancel the change from this page.

### Related Links

*Configure MaxRep HA Page*
*Log In to the Support Interface*
*View the Replication Engine Task Status*

## Configure MaxRep HA Page

Displays the details for configuring high availability (HA) environment for the Oracle MaxRep for SAN.

| | |
|---|---|
| **Primary Node** | Identifies the IP address or host name of the primary (active) Replication Engine. |
| **Domain Name of Primary Node** | Identifies the fully qualified domain name of the primary node. |
| **Secondary Node** | Identifies the IP address or host name of the secondary (passive) Replication Engine. |
| **Domain Name of Secondary Node** | Identifies the fully qualified domain name of the secondary node. |
| **Multicast Group IP Address** | Identifies the unique IP address of the multicast group, which is used by the two Replication Engines in the HA cluster. Other Replication Engine cluster servers must use a different multicast IP address. Multicast IP addresses range is from 224.0.0.0 to 239.255.255.255. |
| **Ping Node** | Identifies the node by which both Replication Engines in the HA cluster ping a common IP address. If the active node cannot ping this ping node, then the passive Replication Engine pings the node and initiates fail over.<br><br>**Important:** To reduce the likelihood of failover, choose a reliable system. |
| **Cluster IP Address** | Identifies the IP address of the HA cluster. |
| **Appliance HA Cluster Name** | Identifies the host name of the HA cluster. |

**Note:** The customer network must be configured to allow ICMP network traffic for both MaxRep Replication Engines in the cluster to ping the Ping Node. The customer network must be configured to allow UDP port 694 network traffic for both Replication Engines in the cluster to communicate with each other using a multicast group IP address.

### Related Links

*Configure Oracle MaxRep High Availability*

## Update the Replication Engine Firmware

You might need to update the Oracle MaxRep Replication Engine firmware when a new version becomes available.

**Prerequisites**

- Updated software package from My Oracle Support
- Checksum file from My Oracle Support

**Important:** Ensure that all of the Replication Engines have the same software version. Oracle does not support Replication Engines that have different software versions in the same configuration.

**Important:** The software update can be a disruptive process. Replication will be interrupted, and, in some cses, you will be required to restart the replication process for your protection plans. Consult the software update release notes to determine if the update is disruptive, and whether a restart is required to fully apply the update.

During the update process, the Oracle MaxRep Support Agent stops the replication services, applies the software update, and then restarts the replication services.

### Related Links

*Log In to the Support Interface*
*View the Replication Engine Task Status*

### Review Your Current Firmware Version

In order to determine the correct upgrade path, review the current firmware release running on your environment, and perform the following:

1. From your Internet browser, log in to the Oracle MaxRep for SAN GUI.
2. Navigate to **Monitor > Protection Status > Versions and Updates**.
3. View the Update History for the control service Replication Engine and any process service Replication Engines that are listed.

### Determine Which Engine to Update First

To reduce downtime and ensure a successful upgrade, Replication Engines should be updated in a specific order. Follow the update sequence below for either non-high availability (NHA) or high availability (HA) environments.

#### Update Engines in a Non-HA Environment

1. Install the updates on the control service Replication Engine.
2. Reboot the control service Replication Engine, if required.
3. Install the updates on any process service Replication Engines.
4. Reboot the process service Replication Engines, if required.

### Update Engines in an HA Environment

1. Install the updates on the standby control service Replication Engine.
2. Reboot the standby control service Replication Engine, if required.
3. Install the updates on the active control service Replication Engine.
4. Reboot the active control service Replication Engine, if required.
5. Install the updates on any standby process service Replication Engines.
6. Reboot the standby process service Replication Engines, if required.
7. Install the updates on any active process service Replication Engines.
8. Reboot the active process service Replication Engines, if required.

## Download the Oracle MaxRep Software

Before you install the Oracle MaxRep Replication Engine software update, you need to download the file and any necessary checksum files from My Oracle Support (MOS).

**Prerequisites**

You must have access to a Customer Support portal account.

1. Point your web browser to *My Oracle Support* (http://support.oracle.com) and log in.
2. On the top menu bar, click **Patches & Updates**.
3. From the Patch Search pane Search tab, click **Product or Family (Advanced)**.
4. In the **Product is** field, enter your system model.

   **Tip:** As you begin entering characters, appropriate items appear in the drop-down list. Choose the model that corresponds to your system.
5. From the **Release** drop-down list, select the appropriate product release.
6. (Optional) From the **Platform** drop-down list, select the desired platform operating system.
7. Click **Search**.
   The system displays the Patch Search page with your search results.
8. (Optional) Click **Edit Search** to refine your search criteria.
9. To display detailed information about the software version, click the link under the **Patch Name** field.
   The Patch Search page displays details about the released software version and provides a download link.
10. To download the software package, click **Download**.

11 Save the software to your workstation.

12 (Optional) To read information about the download or the Release Notes (if available), click **Read Me**.

### Related Links

*Update the Replication Engine Firmware*

## Update the Firmware

**Prerequisites**

- Updated software package from My Oracle Support
- Checksum file from My Oracle Support

**Important:** Ensure that all of the Replication Engines have the same software version. Oracle does not support Replication Engines that have different software versions in the same configuration.

**Important:** The software update can be a disruptive process. Replication will be interrupted, and, in some cases, you will be required to restart the replication process for your protection plans. Consult the software update release to determine if the update is disruptive, and whether a restart is required to fully apply the update.

During the update process, the Oracle MaxRep Support Agent stops the replication services, applies the software update, and then restarts the replication services.

1 Log in to the Support User Interface page on the control service Replication Engine.
The Dashboard page displays.

2 Select **Management Tasks** > **Software Updates**.

3 From the **Host** list, select either a single host, or select **All Servers** to select the Replication Engines that are available in the replication configuration.

4 Click **Browse** and locate the Oracle MaxRep Replication Engine software package.

5 Enter the **Build Checksum** value.

The build checksum is included in a file named `md5sum.txt` that is included with the update bundle from My Oracle Support.

6 To upload the software update to the Replication Engine, click **Upload**.

When you click **Upload**, the system displays the Task Status page. You can monitor the update progress and, in some cases, cancel the change from this page.

**Note:** If the replication software does not restart after 10 minutes, contact Oracle Customer Support.

When the update completes, the services restart and the new software version displays in the Versions and Updates field in the Dashboard.

## Configure ILOM Network

Configure the Integrated Lights Out Manager (ILOM) for the Oracle MaxRep Replication Engine to send hardware fault notices to the Call-Home server.

**Prerequisites**

- Default ILOM password is reset.

  See the *Oracle MaxRep for SAN Hardware Guide*.
- IP address to the Oracle FS System Pilot management interface.

  **Note:** Use the Pilot that is registered to the Replication Engine so that Call-Home notifications and replication logs originate from the same Replication Engine.

Oracle Customer Support receives critical Oracle MaxRep Replication Engine activity notices by way of the Call-Home feature of the Oracle FS System. When you configure the Replication Engine network with the ILOM system, you are establishing the connection to the Call-Home server.

1. Log in to the Support User Interface page on the control service Replication Engine.
   The Dashboard page displays.
2. Select **Management Tasks** > **ILOM Configuration**.
3. From the **Host** list, select the Replication Engine that is running the Oracle MaxRep replication services.
4. Enter the ILOM network information.
   - **ILOM IP Address**
   - **ILOM Subnet Mask**
   - **ILOM Default Gateway**
5. Enter the **Trap Receiver Details**.

   **Note:** Use the IP address to the Oracle FS System Pilot management interface.

When you save your changes, the system displays the **Task Status** page. You can monitor the task progress and, in some cases, cancel the change from this page.

### Related Links

*Log In to the Support Interface*
*View the Replication Engine Task Status*

APPENDIX B

# Oracle MaxRep Command Line Reference

## The Oracle MaxRep Command Line Interface

For release 3.0.4 and higher, Oracle MaxRep for SAN provides a Command Line Interface (CLI). The CLI allows you to manage operations for Oracle MaxRep Replication Engines that are configured in your SAN replication environment.

The Oracle MaxRep Command Line Interface (MRCLI) supports the management of Oracle MaxRep Replication Engines through a specified list of commands. The MRCLI commands are presented in categories known as namespaces. Namespaces separate the commands by function. The MRCLI has built-in namespace `utility`.

The `utility` namespace has a corresponding `help` command, and a help page associated with its namespace `help` command. The namespace syntax is the namespace name, followed by a colon, followed by the command.

For example: `utility:getEngineIpFromId`

An administrative account username is required to run all commands, and the MRCLI prompts for a password.

Commands used in the MRCLI are not case-sensitive. Arguments are case-sensitive.

To resolve both forward and reverse lookups on a MaxRep Replication Engine, DNS must be configured on the host that is running the MRCLI.

## Install the Oracle MaxRep CLI Software

The Oracle MaxRep Command Line Interface (CLI) is a software application that must be downloaded and installed before use. The Oracle MaxRep CLI software is available to download through the Oracle MaxRep GUI for Windows, Solaris, and Linux operating systems (OS).

**Prerequisites**

For Windows operating systems, some prerequisites are required before installing and using the CLI software.

- The Oracle MaxRep CLI is installed in the same drive as the user profile. To obtain the drive location, run the `set` command at the Windows command prompt, and review the drive location listed for `USERPROFILE=`.

- Visual C++ Redistributable for Visual Studio 2012 Update 4 is installed on the host computer. To verify the installation, navigate to **Control Panel > Programs and Features > Microsoft Visual C++ 2012 Redistributable.**. If Visual C++ Redistributable for Visual Studio 2012 is not listed under Programs and Features, download and install the application *here*.

1. Log in to your Oracle MaxRep for SAN GUI, then navigate to **Settings > Software Repository**.
2. Select the download icon that corresponds to the `mrcli` file (`tar` or `ZIP`) specific to your operating system.
3. Save the file to a specified folder on your desktop (an example for Windows, `C:\Program Files`).
4. From that folder, extract the file to run the CLI application.

# MRCLI Command Line Reference

**`createProtectionPlan`**

Creates a protection plan.

## SYNOPSIS

`mrcli` [`-c` *configfile*] `-u` *user* `-m` *maxrepname* [`-v`] `createProtectionPlan` [`-x` *stdout* | *filename.xml*] *planName filename.xml*

## DESCRIPTION

Protection plans specify the parameters for replication. Creating a protection plan is the same process for a synchronous or asynchronous Oracle MaxRep for SAN system. Run `createProtectionPlan` to create a protection plan in the current control service configuration.

## OPTIONS

| | |
|---|---|
| **`-m`** ***maxrepname*** | The IP address or DNS name of the MaxRep Replication Engine. |
| ***planName*** | Specifies the name of the protection plan. |
| **`-u`** ***user*** | Identifies the administrator account that runs the command. |
| **`-c`** ***configfile*** | Specifies the configuration file to modify logging. When used, the `-c` command must be the first option entered at the command line. |
| **`-x`** ***stdout*** \| ***filename.xml*** | Prints output in XML format. |

**-v** Prints MaxRep CLI version and exits. This option should be run on its own, separate from additional options.

```
$ mrcli -v
```

## EXAMPLE

**Task**

Create the protection plan `ReplicationPlan1` on the MaxRep Replication Engine `co-mrengine-22`. Use XML file `plan1creation.xml`.

**Parameters**

- planName:

  `ReplicationPlan1`
- maxrepname: `co-mrengine-22`
- filename.xml: `plan1creation.xml`

```
$ mrcli -u admin -m co-mrengine-22 createProtectionPlan
ReplicationPlan1 plan1creation.xml
```

### activateProtectionPlan

Activates the specified protection plan.

## SYNOPSIS

`mrcli` [`-c` *configfile*] `-u` *user* `-m` *maxrepname* `[-v] activateProtectionPlan` *planName*

## DESCRIPTION

You can create multiple protection plans to configure protection for one or more replication pairs. Protection plans make it possible to apply different protection policies to different groups of replication pairs and to apply policy changes to the entire group at one time. Run `activateProtectionPlan` when you are ready to activate a specified protection plan. Activation of a protection plan begins replication of the data for the replication pairs that are included in the protection plan.

## OPTIONS

**-m** ***maxrepname*** The IP address or DNS name of the MaxRep Replication Engine.

***planName*** Specifies the name of the protection plan.

**-u** ***user*** Identifies the administrator account that runs the command.

**-c** *configfile* Specifies the configuration file to modify logging. When used, the `-c` command must be the first option entered at the command line.

**-v** Prints the current version of the MaxRep CLI then exits. This option should be run on its own, separate from additional options.

```
$ mrcli -v
```

## EXAMPLE

**Task**

Activate the protection plan `ReplicationPlan1` on the MaxRep Replication Engine `co-mrengine-22`.

**Parameters**

- planName: `ReplicationPlan1`
- maxrepname: `co-mrengine-22`

```
$ mrcli -u admin -m co-mrengine-22 activateProtectionPlan
ReplicationPlan1
```

### deactivateProtectionPlan

Deactivates a protection plan.

## SYNOPSIS

`mrcli` [`-c` *configfile*] `-u` *user* `-m` *maxrepname* [`-v`] `deactivateProtectionPlan` *planName*

## DESCRIPTION

The command `deactivateProtectionPlan` deactivates a specified protection plan from an active replication configuration.

## OPTIONS

**-m** *maxrepname* The IP address or DNS name of the MaxRep Replication Engine.

***planName*** Specifies the name of the protection plan.

**-u** *user* Identifies the administrator account that runs the command.

**-c** *configfile* Specifies the configuration file to modify logging. When used, the `-c` command must be the first option entered at the command line.

**-v** Prints MaxRep CLI version and exits. This option should be run on its own, separate from additional options.

```
$ mrcli -v
```

### EXAMPLE

**Task**

Run the command `deactivateProtectionPlan` to deactivate the plan `ReplicationPlan02` on MaxRep Replication Engine `co-mrengine-22`.

**Parameters**

- planName: `ReplicationPlan02`
- maxrepname: `co-mrengine-22`

```
$ mrcli -u admin -m co-mrengine-22 deactivateProtectionPlan
ReplicationPlan02
```

## resumeProtectionPlan

Resumes replication.

### SYNOPSIS

`mrcli` [`-c` *configfile*] `-u` *user* `-m` *maxrepname* [`-v`] `resumeProtectionPlan` *planName* [`-x` *stdout* | *filename.xml*]

### DESCRIPTION

The command `resumeProtectionPlan` resumes replication that has been either paused or flushed. Oracle recommends running the command `getProtectionPlanStatus` to obtain confirmation of the current state of the protection plan.

### OPTIONS

| | |
|---|---|
| **-m** *maxrepname* | The IP address or DNS name of the MaxRep Replication Engine. |
| *planName* | Specifies the name of the protection plan. |
| **-u** *user* | Identifies the administrator account that runs the command. |
| **-x** *stdout* \| *filename.xml* | Prints output in XML format. |
| **-c** *configfile* | Specifies the configuration file to modify logging. When used, the `-c` command must be the first option entered at the command line. |
| **-v** | Prints the current version of the MaxRep CLI then exits. This option should be run on its own, separate from additional options. |

```
$ mrcli -v
```

## EXAMPLE

**Task**

Use the `resumeProtectionPlan` command to resume replication for plan `ReplicationPlan01` on MaxRep Replication Engine `co-mrengine-02`.

**Parameters**

- planName: `ReplicationPlan01`
- maxrepname: `co-mrengine-02`

```
mrcli -u admin -m co-mrengine-02 resumeProtectionPlan
ReplicationPlan01
```

### pauseProtectionPlan

Pauses replication of a protection plan.

## SYNOPSIS

`mrcli` [`-c` *configfile*] `-u` *user* `-m` *maxrepname* [`-v`] `pauseProtectionPlan` *planName* [`-x` *stdout* | *filename.xml*]

## DESCRIPTION

In a synchronous replication environment, running the command `pauseProtectionPlan` pauses the replication of a protection plan by haulting the transfer of the differences of data between the source LUN and the target LUN. This command does not hault the logging of the differences of data on the source LUN. Oracle recommends running the command `getProtectionPlanStatus` to obtain confirmation of the current state of the protection plan.

## OPTIONS

| | |
|---|---|
| **-m** ***maxrepname*** | The IP address or DNS name of the MaxRep Replication Engine. |
| ***planName*** | Specifies the name of the protection plan. |
| **-u** ***user*** | Identifies the administrator account that runs the command. |
| **-x** ***stdout*** \| ***filename.xml*** | Prints output in XML format. |
| **-v** | Prints the current version of the MaxRep CLI then exits. This option should be run on its own, separate from additional options. |

```
$ mrcli -v
```

**-c** *configfile* — Specifies the configuration file to modify logging. When used, the `-c` command must be the first option entered at the command line.

## EXAMPLE

**Task**

Run the command `pauseProtectionPlan` to pause replication of protection plan `ReplicationPlan01` on MaxRep Replication Engine `co-mrengine-22`.

**Parameters**

- planName: `ReplicationPlan01`
- maxrepname: `co-mrengine-22`

```
$ mrcli -u admin -m co-mrengine-22 pauseProtectionPlan
ReplicationPlan01
```

### deleteProtectionPlan

Deletes a protection plan.

## SYNOPSIS

`mrcli -u` *user* `-m` *maxrepname* `[--f]` *force* `deleteProtectionPlan` *planName*

## DESCRIPTION

When the command `deleteProtectionPlan` is executed to the MaxRep Replication Engine that is hosting the control service, the command deletes the specified protection plan in that configuration.

## OPTIONS

**-m** *maxrepname* — The IP address or DNS name of the MaxRep Replication Engine.

*planName* — Specifies the name of the protection plan.

**-u** *user* — Identifies the administrator account that runs the command.

**--f** *force* — Forces cleanup.

## EXAMPLE

**Task**

Run the command `deleteProtectionPlan` to delete protection plan `ReplicationPlan02` on MaxRep Replication Engine `co-mrengine-22`.

**Parameters**

- planName: `ReplicationPlan02`
- maxrepname: `co-mrengine-22`

```
$ mrcli -u admin -m co-mrengine-22 deleteProtectionPlan --f
ReplicationPlan02
```

### `getProtectionPlans`

Returns a list of protection plans that are part of the current configuration.

## SYNOPSIS

`mrcli` [`-c` *configfile*] `-u` *user* `-m` *maxrepname* [`-v`] [`-x` *stdout* | *fileName.xml*] `getProtectionPlans`

## DESCRIPTION

When the command `getProtectionPlans` is executed to the MaxRep Replication Engine hosting the control service, the command provides a list of protection plans that are currently active in the control service configuration.

## OPTIONS

| | |
|---|---|
| **`-m`** ***maxrepname*** | The IP address or DNS name of the MaxRep Replication Engine. |
| **`-u`** ***user*** | Identifies the administrator account that runs the command. |
| **`-c`** ***configfile*** | Specifies the configuration file to modify logging. When used, the `-c` command must be the first option entered at the command line. |
| **`-v`** | Prints MaxRep CLI version and exits. This option should be run on its own, separate from additional options.<br>`$ mrcli -v` |
| **`-x`** ***stdout*** \| ***filename.xml*** | Prints output in XML format. |

## EXAMPLE

**Task**

Run the `getProtectionPlans` command to return a list of protection plans from MaxRep Replication Engine `co-maxrep-22`. The MaxRep CLI will prompt for a password.

**Parameters**

- maxrepname: `co-maxrep-22`
- plan.xml: `plandetails.xml`

```
$ mrcli -u admin -m co-maxrep-22 getProtectionPlans
```

```
$ mrcli -u admin -m co-maxrep-22 getProtectionPlans -x stdout
```

For XML output:

```
 $ mrcli -u admin -m co-maxrep-22 getProtectionPlans -x
plandetails.xml
```

### `getProtectionPlanStatus`

Returns the status summary of a protection plan.

## SYNOPSIS

`mrcli` [`-c` *configfile*] `-u` *user* `-m` *maxrepname* [`-v`] [`-x` *stdout* | *filename.xml*] `getProtectionPlanStatus` *planName*

## DESCRIPTION

When the `getProtectionPlanStatus` command is executed to the MaxRep Replication Engine that is hosting the active control service, the command returns details of the status of the specified protection plan.

## OPTIONS

| | |
|---|---|
| **-m** *maxrepname* | The IP address or DNS name of the MaxRep Replication Engine. |
| *planName* | Specifies the name of the protection plan. |
| **-u** *user* | Identifies the administrator account that runs the command. |
| **-v** | Prints MaxRep CLI version and exits. This option should be run on its own, separate from additional options.<br>`$ mrcli -v` |

| | |
|---|---|
| **-c** *configfile* | Specifies the configuration file to modify logging. When used, the `-c` command must be the first option entered at the command line. |
| **-x** *stdout* \| *filename.xml* | Prints output in XML format. |

## EXAMPLE

**Task**

Run the `getProtectionPlanStatus` command to return the status and details of protection plan `ReplicationPlan2` on MaxRep Replication Engine `co-mrengine-18`.

**Parameters**

- planName: `ReplicationPlan2`
- maxrepname: `co-mrengine-18`

```
$ mrcli -u admin -m co-mrengine-18 getProtectionPlanStatus
ReplicationPlan2
```

### `getProtectionPlanDetails`

Returns the details about a protection plan.

## SYNOPSIS

`mrcli` [`-c` *configFile*] `-u` *user* `-m` *maxrepname* [`-v`] [`-x` *stdout* | *filename.xml*] `getProtectionPlanDetails` *planName*

## DESCRIPTION

When you need to learn the details behind a protection plan, run the command `getProtectionPlanDetails` to return information about the plan's creation details in XML format.

## OPTIONS

| | |
|---|---|
| **-m** *maxrepname* | The IP address or DNS name of the MaxRep Replication Engine. |
| *planName* | Specifies the name of the protection plan. |
| **-u** *user* | Identifies the administrator account that runs the command. |
| **-c** *configfile* | Specifies the configuration file to modify logging. When used, the `-c` command must be the first option entered at the command line. |

**-v** Prints the current version of the MaxRep CLI then exits. This option should be run on its own, separate from additional options.

```
$ mrcli -v
```

**-x** ***stdout*** | ***filename.xml*** Prints output in XML format.

## EXAMPLE

**Task**

Run the `getProtetionPlanDetails` to obtain plan creation details for protetion plan `ProtectionPlan_22` on MaxRep Replication Engine `co-mrengine-02`. Use XML file plandetails.xml

**Parameters**

- planName: `ProtectionPlan_22`
- maxrepname: `co-mrengine-02`
- filename.xml: `plandetails.xml`

```
$ mrcli -u admin -m co-mrengine-02 getProtectionPlanDetails
ProtectionPlan_22
```

**For XML output:**

```
$ mrcli -u admin -m co-mrengine-02 getProtectionPlanDetails
ProtectionPlan_22 -x plandetails.xml
```

### createReverseReplicationParams

Creates reverse replication parameters.

## SYNOPSIS

`mrcli -u` *user* `-m` *maxrepname* `-r createReverseReplicationParams` *planName*

## DESCRIPTION

The `createReverseReplicationParams` command creates a reverse replication scenario. Upon successful execution of the command, two XML files are created: `mrclireversetest_forward.xml` and `mrclireversetest_reverse.xml`. Run the `-r` option on the source LUN and the target LUN.

**Note:** The XML files can contain fully qualified names.

## OPTIONS

**-m** ***maxrepname*** The IP address or DNS name of the MaxRep Replication Engine.

| | |
|---|---|
| *planName* | Specifies the name of the protection plan. |
| **-u** *user* | Identifies the administrator account that runs the command. |
| **-r** | Rediscovers a LUN. |

## EXAMPLE

**Task**

Run the command `createReverseReplicationParams` to reverse replication on plan `ReplicationPlan04` associated with MaxRep engine `co-mrengine-05`.

**Parameters**

- maxrepname: `co-mrengine-05`
- planName: `ReplicationPlan04`

```
$ mrcli -u admin -m co-mrengine-05 createReverseReplicationParams
ReplicationPlan04
```

### createVsnap

Creates a virtual snapshot, or Vsnap, of a specified LUN at the requested time.

## SYNOPSIS

`mrcli` [`-c` *configFile*] `-u` *user* `-m` *maxrepname* [`-v`] [`-x` *stdout* | *filename.xml*] `createVsnap` *planName SnapConfig.xml*

## DESCRIPTION

This command creates a Vsnap of the requested LUN at the requested time, and returns the name of the Vsnap and its internal ID.

## OPTIONS

| | |
|---|---|
| **-m** *maxrepname* | The IP address or DNS name of the MaxRep Replication Engine. |
| *planName* | Specifies the name of the protection plan. |
| **-u** *user* | Identifies the administrator account that runs the command. |
| **-c** *configfile* | Specifies the configuration file to modify logging. When used, the `-c` command must be the first option entered at the command line. |
| **-v** | Prints the current version of the MaxRep CLI then exits. This option should be run on its own, separate from additional options. |

```
$ mrcli -v
```

| | |
|---|---|
| **-x** *stdout* \| *filename.xml* | Prints output in XML format. |

## EXAMPLE

**Task**

Execute the commad `createVsnap` for `ReplicationPlan1` on the MaxRep Replication Engine `co-mrengine-02`. Alternatively, use the IP `10.123.456.789`. Use XML file `snapconfig.xml`.

**Parameters**

- planName: `ReplicationPlan1`
- maxrepname: `co-mrengine-02` or IP address `10.123.456.789`
- filename.xml: `snapconfig.xml`

```
$ mrcli -u admin -m co-mrengine-02 createVsnap ReplicationPlan1
```

For XML output

```
$ mrcli -u admin -m 10.123.456.789 createVsnap ReplicationPlan1
snapconfig.xml
```

### createBookmark

Creates a bookmark.

## SYNOPSIS

`mrcli -u` *user* `-m` *maxrepname* `createBookmark` *planname bookmark*

## DESCRIPTION

Run the `createBookmark` command to create a bookmark for a specified protection plan in the current control service configuration.

## OPTIONS

| | |
|---|---|
| **bookmark** | Specifies the bookmark name. |
| **-m** *maxrepname* | The IP address or DNS name of the MaxRep Replication Engine. |
| *planName* | Specifies the name of the protection plan. |
| **-u** *user* | Identifies the administrator account that runs the command. |

## EXAMPLE

**Task**

Run the `createbookmark` command to create a bookmark on `RepPlan04`, associated with MaxRep engine `co-mrengine-02`. Name the bookmark `BookmarkPlan01`.

**Parameters**

- maxrepname: `co-mrengine-02`
- planName: `RepPlan04`
- bookmark: `BookmarkPlan01`

```
$ mrcli -u admin -m co-mrengine-02 createbookmark RepPlan04
BookmarkPlan01
```

### getBookmarkDetails

Returns details of a bookmark.

## SYNOPSIS

`mrcli -u` *user* `-m` *maxrepname* `getBookmarkDetails` *bookmark*

## DESCRIPTION

Use the command `getBookmarkDetails` to obtain details of a bookmark in the MaxRep Replication Engine that is hosting the active control service configuration.

## OPTIONS

| | |
|---|---|
| **bookmark** | Specifies the bookmark name. |
| **-m** *maxrepname* | The IP address or DNS name of the MaxRep Replication Engine. |
| **-u** *user* | Identifies the administrator account that runs the command. |

## EXAMPLE

**Task**

Run the command `getBookmarkDetails` to return the details of bookmark `tagcheck1` on MaxRep engine `co-mrengine-01`.

**Parameters**

- maxrepname: `co-mrengine-01`
- bookmark: `tagcheck1`

```
$ mrcli -u admin -m co-mrengine-01 getBookmarkDetails tagcheck1
```

### `listBookmarks`

Returns a list of bookmarks.

## SYNOPSIS

`mrcli -u` *user* `-m` *maxrepname* `listBookmarks` *planName*

## DESCRIPTION

The command `listBookmarks` displays a list of bookmarks present across all replication pairs in the current configuration. The command also provides a timestamp associated with the active control service configuration.

## OPTIONS

| | |
|---|---|
| **`bookmark`** | Specifies the bookmark name. |
| **`-m`** *maxrepname* | The IP address or DNS name of the MaxRep Replication Engine. |
| *planName* | Specifies the name of the protection plan. |
| **`-u`** *user* | Identifies the administrator account that runs the command. |

## EXAMPLE

**Task**

Run the command `listBookmarks` to return a list of bookmarks for `ReplicationPlan04` associated with MaxRep engine `co-mrengine-01`.

**Parameters**

- maxrepname: `co-mrengine-01`
- planName: `ReplicationPlan04`

```
$ mrcli -u admin -m co-mrengine-01 listBookmarks ReplicationPlan04
```

### destroyVsnap

Destroys a previously created virtual snapshot, or Vsnap.

## SYNOPSIS

`mrcli` [`-c` *configfile*] `-u` *user* `-m` *maxrepname* [`-v`] [`-x` *stdout* | *filename.xml*] `destroyVsnap` *scenarioID*

## DESCRIPTION

This command unmaps and destroys the Vsnap previously created by the `createVsnap` command. The Vsnap to be deleted is specified by the Vsnap ID or scenario ID. This command is synchronous and idempotent.

## OPTIONS

| | |
|---|---|
| **-m** *maxrepname* | The IP address or DNS name of the MaxRep Replication Engine. |
| **scenarioID** | The internal ID of the scenario associated with the planID. |
| **-u** *user* | Identifies the administrator account that runs the command. |
| **-x** *stdout* \| *filename.xml* | Prints output in XML format. |
| **-c** *configfile* | Specifies the configuration file to modify logging. When used, the `-c` command must be the first option entered at the command line. |

## EXAMPLE

**Task**

Destroy the Vsnap created on the MaxRep Replication Engine `co-mrengine-02` for scenario ID `29`.

**Parameters**

- scenarioID: `29`
- maxrepname: `co-mrengine-02`

```
$ mrcli -u admin -m co-mrengine-02 destroyVsnap 29
```

### getVsnapLunNumber

Returns the LUN number of an exported Vsnap of a specified protection plan.

## SYNOPSIS

`mrcli -u` *user* `-m` *maxrepname* `getVsnapLunNumber` *VsnapId* [`-x` *stdout* | *fileName.xml*]

## DESCRIPTION

The `getVsnapLunNumber` command returns the LUN number of an exported Vsnap of a specified protection plan with a Vsnap ID. The Vsnap ID is obtained through the MaxRep GUI.

## OPTIONS

| | |
|---|---|
| **-m** *maxrepname* | The IP address or DNS name of the MaxRep Replication Engine. |
| **-u** *user* | Identifies the administrator account that runs the command. |
| **-x** *stdout* \| *filename.xml* | Prints output in XML format. |
| **VsnapId** | The ID of the Vsnap that is being queried. |

## EXAMPLE

**Task**

Run the command `getVsnapLunNumber` to obtain the LUN number of the exported Vsnap `vsnap42` on MaxRep Replication Engine `co-mrengine-05` for protection plan `ReplicationPlan11`.

**Parameters**

- maxrepname: `co-mrengine-05`
- vsnapID: `vsnap42`

```
$ mrcli -u admin -m co-mrengine-05 getVsnapLunNumber vsnap42
ReplicationPlan11
```

### deregisterAxiom

Unregisters a Pillar Axiom system with a MaxRep Replication Engine.

## SYNOPSIS

`mrcli -u` *user* `-m` *maxrepname* `deregisterAxiom` *axiomname* `-p` *processServiceIP*

## DESCRIPTION

The command `deregisteraxiom` unregisters a specified Pillar Axiom system and its associated process service IP with a MaxRep Replication Engine.

## OPTIONS

| | |
|---|---|
| **-m** *maxrepname* | The IP address or DNS name of the MaxRep Replication Engine. |
| **-p** *processServiceIP* | The IP address of the MaxRep engine hosting the process service. |
| **-u** *user* | Identifies the administrator account that runs the command. |

## EXAMPLE

**Task**

Run the command `deregisterAxiom` to unregister the Pillar Axiom system `10.12.345.67` on MaxRep engine `co-mrengine-05` with the process service IP `10.23.456.789`.

**Parameters**

- maxrepname: `co-mrengine-05`
- axiomname: `10.12.345.67`
- processserviceIP: `10.23.456.789`

```
$ mrcli -u admin -m co-mrengine-05 deregisterAxiom 10.12.345.67 -
p 10.23.456.789
```

### getActivationStatus

Returns the activation status of a protection plan.

## SYNOPSIS

`mrcli` [`-c` *configfile*] `-u` *user* `-m` *maxrepname* [`-v`] `getActivationStatus` *planName*

## DESCRIPTION

The `getActivationStatus` command displays the current state of a specified protection plan.

## OPTIONS

**-m** *maxrepname* — The IP address or DNS name of the MaxRep Replication Engine.

*planName* — Specifies the name of the protection plan.

**-u** *user* — Identifies the administrator account that runs the command.

**-c** *configfile* — Specifies the configuration file to modify logging. When used, the `-c` command must be the first option entered at the command line.

**-v** — Prints the current version of the MaxRep CLI then exits. This option should be run on its own, separate from additional options.

```
$ mrcli -v
```

## EXAMPLE

**Task**

Run the `getactivationstatus` command to display the activation status of protection plan `ProtectionPlan07` on MaxRep Replication Engine `co-mrengine-05`.

**Parameters**

- planName: `ProtectionPlan07`
- maxrepname: `co-mrengine-05`

```
$ mrcli -u admin -m co-mrengine-05 getActivationStatus
ProtectionPlan07
```

### `getActiveControlService`

Returns the IP address of the active control service that runs on the MaxRep Replication Engine.

## SYNOPSIS

`mrcli` [`-c` *configfile*] `-u` *user* `-m` *maxrepname* [`-v`] `getActiveControlService`

## DESCRIPTION

This commands returns the IP address of the active control service on a specified MaxRep Replication Engine configuration.

## OPTIONS

**`-m` *maxrepname*** — The IP address or DNS name of the MaxRep Replication Engine.

**`-u` *user*** — Identifies the administrator account that runs the command.

**`-c` *configfile*** — Specifies the configuration file to modify logging. When used, the `-c` command must be the first option entered at the command line.

**`-v`** — Prints the current version of the MaxRep CLI then exits. This option should be run on its own, separate from additional options.

```
$ mrcli -v
```

### EXAMPLE

**Task**

Run the command `getActiveControlService` to return the IP address of the MaxRep Replication Engine running the control service associated with engine `co-mrengine-02`.

**Parameters**

maxrepname: `co-mrengine-02`

```
$ mrcli -u admin -m co-mrengine-02 getActiveControlService
```

## getAvailableRetentionLuns

Returns a list of retention LUNs.

### SYNOPSIS

`mrcli` [`-c` *configfile*] `-u` *user* `-m` *maxrepname* [`-v`] `getAvailableRetentionLuns` *planName*

### DESCRIPTION

The command `getAvailableRetentionLuns` displays a list of available retention LUNs on a MaxRep Replication Engine. Use `getAvailableRetentionLuns` to find available LUN capacity for a specified protection plan on a MaxRep Replication Engine. Commands are not case sensitive. Arguments are case sensitive.

### OPTIONS

| | |
|---|---|
| **-m** *maxrepname* | The IP address or DNS name of the MaxRep Replication Engine. |
| *planName* | Specifies the name of the protection plan. |
| **-u** *user* | Identifies the administrator account that runs the command. |
| **-c** *configfile* | Specifies the configuration file to modify logging. When used, the `-c` command must be the first option entered at the command line. |
| **-v** | Prints the current version of the MaxRep CLI then exits. This option should be run on its own, separate from additional options.<br>`$ mrcli -v` |

## EXAMPLE

**Task**

Run the `getAvailableRetentionLuns` command to return all available retention LUNs on MaxRep Replication Engine `co-mrengine-05` for protection plan `Plan08`.

**Parameters**

- planName: `Plan08`
- maxrepname: `co-mrengine-05`

```
$ mrcli -u admin -m co-mrengine-05 getAvailableRetentionLuns
Plan08
```

### getCommonConsistencyTime

Returns the most recent common consistency time for all replication pairs in a plan.

## SYNOPSIS

`mrcli` [`-c` *configfile*] `-u` *user* `-m` *maxrepname* `getCommonConsistencyTime` [`-a` *ATime*] [`-b` *BTime*] *planName* [`-x` *stdout* | *fileName.xml*] [`-v`]

## DESCRIPTION

Run the command `getCommonConsistencyTime` to obtain the most recent consistency time of all LUNs in a specified protection plan. If *ATime* is specified, the first common time occuring after *ATime* is displyed. If *BTime* is specified, the last common time occuring before *BTime* is displayed. Commands are not case sensitive. Arguments are case sensitive.

## OPTIONS

| | |
|---|---|
| **-a** *ATime* | Instructs the command to list the first common consistency event occuring after ATime. |
| **-b** *BTime* | Instructs the command to list the latest common consistency event occurring before BTime. |
| **-m** *maxrepname* | The IP address or DNS name of the MaxRep Replication Engine. |
| *planName* | Specifies the name of the protection plan. |
| **-u** *user* | Identifies the administrator account that runs the command. |
| **-c** *configfile* | Specifies the configuration file to modify logging. When used, the `-c` command must be the first option entered at the command line. |

| | |
|---|---|
| **-x** *stdout* \| *filename.xml* | Prints output in XML format. |
| **-v** | Prints the current version of the MaxRep CLI then exits. This option should be run on its own, separate from additional options.<br>`$ mrcli -v` |

## EXAMPLE

**Task**

Run the command `getCommonConsistencyTime` to display the most recent consistency time for all LUNs in protection plan `RepPlan02` on MaxRep Replication Engine `co-mrengine-04`. Use XML file `engine65.xml` for this plan.

**Parameters**

- planname: `RepPlan02`
- maxrepname: `co-mrengine-04`
- filename.xml: `engine65.xml`

```
$ mrcli -u admin -m co-mrengine-04 getCommonConsistencyTime
RepPlan02 -a
```

For XML output:

```
$ mrcli -u admin -m co-mrengine-04 getCommonConsistencyTime -x
engine65.xml
```

### getEngineDetails

Returns the details for a MaxRep Replication Engine.

## SYNOPSIS

`mrcli -u` *user* `-m` *maxrepname* [`-x` *stdout* | *filename.xml*] `getEngineDetails`

## DESCRIPTION

The command `getEngineDetails` returns the name, GUID, serial number, IP address, and software version of a specified MaxRep Replication Engine.

## OPTIONS

| | |
|---|---|
| **-m** *maxrepname* | The IP address or DNS name of the MaxRep Replication Engine. |
| **-u** *user* | Identifies the administrator account that runs the command. |
| **-x** *stdout* \| *filename.xml* | Prints output in XML format. |

## EXAMPLE

**Task**

Run the command `getEngineDetails` for MaxRep engine `co-mrengine-05`.

**Parameters**

maxrepname: `co-mrengine-05`

```
$ mrcli -u admin -m co-mrengine-05 getEngineDetails
```

**registerAxiom**

Registers a Pillar Axiom system with a MaxRep Replication Engine.

## SYNOPSIS

`mrcli -u` *user* `-m` *maxrepname* `registerAxiom` *axiomName* `-p` *processServiceIP*

## DESCRIPTION

The command `registerAxiom` registers a specified Pillar Axiom system and its associated process service IP with a MaxRep Replication Engine.

## OPTIONS

| | |
|---|---|
| **-m** *maxrepname* | The IP address or DNS name of the MaxRep Replication Engine. |
| **-p** *processServiceIP* | The IP address of the MaxRep engine hosting the process service. |
| **-u** *user* | Identifies the administrator account that runs the command. |

## EXAMPLE

**Task**

Run the command `registerAxiom` to register the Pillar Axiom system `coaxm001` on MaxRep engine `co-mrengine-04` with the process service IP `10.12.345.678`.

**Parameters**

- maxrepname: `co-mrengine-04`
- axiomName: `10.12.345.78`
- processServiceIP: `10.12.345.678`

```
$ mrcli -u admin -m co-mrengine-04 registerAxiom 10.12.345.78 -p
10.12.345.678
```

### rediscoverRegisteredAxiom

Forces the rediscovery of a registered Pillar Axiom system.

## SYNOPSIS

`mrcli -u` *user* `-m` *maxrepname* `rediscoverRegisteredAxiom` *axiomName* `-p` *processServiceIP*

## DESCRIPTION

Run the command `rediscoverRegisteredAxiom` to force the discovery of a specified, registered Pillar Axiom system on a specified MaxRep Replication Engine.

## OPTIONS

| | |
|---|---|
| **-m** *maxrepname* | The IP address or DNS name of the MaxRep Replication Engine. |
| **-p** *processServiceIP* | The IP address of the MaxRep engine hosting the process service. |
| **-u** *user* | Identifies the administrator account that runs the command. |

## EXAMPLE

**Task**

Run the command `rediscoverRegisteredAxiom` to return a discovery of Pillar Axiom system `coaxengine001` on MaxRep Replication Engine`co-mrengine-05` with the process service IP `10.23.456.789`.

**Parameters**

- maxrepname: `co-mrengine-05`
- axiomName: `coaxengine001`
- processServiceIP: `10.23.456.789`

```
$ mrcli -u admin -m co-mrengine-05 rediscoverRegisteredAxiom
coaxengine001 -p 10.23.456.789
```

### `getRegisteredAxiomDetails`

Returns the details of a specified Pillar Axiom system that is registered with a specified MaxRep Replication Engine.

## SYNOPSIS

`mrcli -u` *user* `-m` *maxrepname* `getRegisteredAxiomDetails` *AxiomName*

## DESCRIPTION

The command `getRegisteredAxiomDetails` returns the details of a specified Pillar Axiom system that is registered with a specified MaxRep Replication Engine.

## OPTIONS

| | |
|---|---|
| **-m** *maxrepname* | The IP address or DNS name of the MaxRep Replication Engine. |
| **-u** *user* | Identifies the administrator account that runs the command. |
| *axiomName* | The name of the Pillar Axiom system that is being queried. |

## EXAMPLE

**Task**

Run the command `getregisteredaxiomdetails` to obtain details about Pillar Axiom system `coaxiomengine009` that is registered on MaxRep Replication Engine `co-mrengine-02`.

**Parameters**

- maxrepname: `co-mrengine-02`
- axiomName: `coaxiomengine009`

```
$ mrcli -u admin -m co-mrengine-02 getRegisteredAxiomDetails
coaxiomengine009
```

### `getRegisteredAxiomDiscoveryHistory`

Returns the discovery history of a specified Pillar Axiom system.

## SYNOPSIS

`mrcli -u` *user* `-m` *maxrepname* `getRegisteredAxiomDiscoveryHistory` *axiomName* [`-p`] *processServiceIP*

## DESCRIPTION

The command `getRegisteredAxiomDiscoveryHistory` displays the discovery history of a specified Pillar Axiom system associated with a specified MaxRep Replication Engine running the process service.

## OPTIONS

| | |
|---|---|
| **-m** *maxrepname* | The IP address or DNS name of the MaxRep Replication Engine. |
| **-p** *processServiceIP* | The IP address of the MaxRep Replication Engine running the process service. |
| *axiomName* | The name of the Pillar Axiom system that is being queried. |
| **-u** *user* | Identifies the administrator account that runs the command. |

## EXAMPLE

**Task**

Run the command `getRegisteredAxiomDiscoveryHistory` to obtain the discovery history of Pillar Axiom system `coaxmengine01` associated with MaxRep Replication Engine `co-mrengine-22`, or IP `10.123.456.789`.

**Parameters**

- maxrepname: `co-mrengine-22`
- axiomName: `coaxmengine01`
- processServiceIP: `10.123.456.789`

```
$ mrcli -u admin -m co-mrengine-22
getRegisteredAxiomDiscoveryHistory coaxmengine01 -p 10.123.456.789
```

### getRetentionLunDetails

Returns the details of a specified retention LUN.

## SYNOPSIS

`mrcli` [`-c` *configfile*] `-u` *user* `-m` *maxrepname* [`-v`] [`-x` *stdout* | *filename.xml*] `getRetentionLunDetails` *LunId*

## DESCRIPTION

After retrieving the name of a retention LUN through the command `getRetentionLunDetails`, you can display the details of specified retention LUN with the command `getRetentionLunDetails`.

## OPTIONS

| | |
|---|---|
| **LunId** | The ID of the SAN LUN. |
| **-m** *maxrepname* | The IP address or DNS name of the MaxRep Replication Engine. |
| **-u** *user* | Identifies the administrator account that runs the command. |
| **-v** | Prints the current version of the MaxRep CLI then exits. This option should be run on its own, separate from additional options.<br>`$ mrcli -v` |
| **-c** *configfile* | Specifies the configuration file to modify logging. When used, the `-c` command must be the first option entered at the command line. |
| **-x** *stdout* \| *filename.xml* | Prints output in XML format. |

## EXAMPLE

**Task**

Run the command `getRetentionLunDetails` to obtain the details of active retention LUN `36000b08414b303032383334001fd` on MaxRep Replication Engine `co-mrengine-05`.

**Parameters**

- maxrepname: `co-mrengine-05`
- LUN ID: `36000b08414b303032383334001fd`

```
$ mrcli -u admin -m co-mrengine-05 getretentionlundetails
36000b08414b303032383334001fd
```

### getRollbackStatus

Returns the status of an in-progress rollback, or recovery, of a protection plan.

## SYNOPSIS

`mrcli` [`-c` *configfile*] `-u` *user* `-m` *maxrepname* [`-v`] [`-x` *stdout* | *filename.xml*] `getRollbackStatus` *planName*

## DESCRIPTION

When a rollback, or recovery, of a protection plan is in process, execute the command `getRollbackStatus` to obtain the status of the rollback that is currently running.

## OPTIONS

| | |
|---|---|
| **-m** *maxrepname* | The IP address or DNS name of the MaxRep Replication Engine. |
| *planName* | Specifies the name of the protection plan. |
| **-u** *user* | Identifies the administrator account that runs the command. |
| **-c** *configfile* | Specifies the configuration file to modify logging. When used, the `-c` command must be the first option entered at the command line. |
| **-x** *stdout* \| *filename.xml* | Prints output in XML format. |
| **-v** | Prints the current version of the MaxRep CLI then exits. This option should be run on its own, separate from additional options.<br>`$ mrcli -v` |

## EXAMPLE

**Task**

Run the command `getRollbackStatus` for obtain the rollback, or recovery, status of protection plan `ReplicationPlan10` on MaxRep Replication Engine `co-mrengine-02`.

**Parameters**

- planName: `ReplicationPlan10`
- maxrepname: `co-mrengine-02`

```
$ mrcli -u admin -m co-mrengine-02 getRollbackStatus
ReplicationPlan10
```

### getSourceArrays

Returns a list of names of the storage arrays that host a source LUN in a specified protection plan.

## SYNOPSIS

`mrcli` [`-c` *configfile*] `-u` *user* `-m` *maxrepname* [`-v`] `getSourceArrays` *planName*

## DESCRIPTION

The command `getSourceArrays` displays all the array names on Pillar Axiom or Oracle FS Systems that host a source LUN in a specified protection plan associated with a MaxRep Replication Engine.

## OPTIONS

| | |
|---|---|
| **-m** *maxrepname* | The IP address or DNS name of the MaxRep Replication Engine. |
| *planName* | Specifies the name of the protection plan. |
| **-u** *user* | Identifies the administrator account that runs the command. |
| **-c** *configfile* | Specifies the configuration file to modify logging. When used, the `-c` command must be the first option entered at the command line. |
| **-v** | Prints the current version of the MaxRep CLI then exits. This option should be run on its own, separate from additional options.<br>`$ mrcli -v` |

## EXAMPLE

**Task**

Run the command `getSourceArrays` to return a list of the names of the arrays on MaxRep Replication Engine `co-mrengine-05` for protection plan `ReplicationPlan10`.

**Parameters**

- planname: `ReplicationPlan10`
- maxrepname: `co-mrengine-05`

```
$ mrcli -u admin -m co-mrengine-05 getSourceArrays
ReplicationPlan10
```

### getSourceVolumes

Returns a comma-delimited list of source volume devices of a specified protection plan.

## SYNOPSIS

`mrcli` [`-c` *configfile*] `-u` *user* `-m` *maxrepname* [`-v`] `getSourceVolumes` *planID*

## DESCRIPTION

The command `getSourceVolumes` is run to obtain a comma-delimited list of source volumes associated with a specified protection plan ID. The protection plan ID is obtained through the command `getProtectionPlanId`.

## OPTIONS

| | |
|---|---|
| **-m** *maxrepname* | The IP address or DNS name of the MaxRep Replication Engine. |
| *planID* | The ID of the protection plan that is being queried. |
| **-u** *user* | Identifies the administrator account that runs the command. |
| **-c** *configfile* | Specifies the configuration file to modify logging. When used, the `-c` command must be the first option entered at the command line. |
| **-v** | Prints the current version of the MaxRep CLI then exits. This option should be run on its own, separate from additional options.<br>`$ mrcli -v` |

## EXAMPLE

**Task**

Run the command `getsourcevolumes` to obtain a comma-delimited list of source volumes names of protection plan ID `25` on MaxRep Replication Engine `co-mrengine-02`.

**Parameters**

- planID: `25`
- maxrepname: `co-mrengine-02`

```
$ mrcli -u admin -m co-mrengine-02 getSourceVolumes 25
```

### getTargetArrays

Returns a list of target arrays that host a target LUN in a specified protection plan.

## SYNOPSIS

`mrcli` [`-c` *configfile*] `-u` *user* `-m` *maxrepname* [`-v`] `getTargetArrays` *planName*

## DESCRIPTION

The command `getTargetArrays` displays all the array names on Pillar Axiom or Oracle FS Systems that host a target LUN in a specified protection plan associated with a MaxRep Replication Engine.

## OPTIONS

| | |
|---|---|
| **-m** *maxrepname* | The IP address or DNS name of the MaxRep Replication Engine. |
| *planName* | Specifies the name of the protection plan. |
| **-u** *user* | Identifies the administrator account that runs the command. |
| **-c** *configfile* | Specifies the configuration file to modify logging. When used, the `-c` command must be the first option entered at the command line. |
| **-v** | Prints the current version of the MaxRep CLI then exits. This option should be run on its own, separate from additional options.<br>`$ mrcli -v` |

## EXAMPLE

**Task**

Run the command `getTargetArrays` to return a list of the names of the target arrays on MaxRep Replication Engine `co-mrengine-05` for protection plan `ReplicationPlan10`.

**Parameters**

- planName: `ReplicationPlan10`
- maxrepname: `co-mrengine-05`

```
$ mrcli -u admin -m co-mrengine-05 getTargetArrays
ReplicationPlan10
```

### getTargetVolumes

Returns a comma-delimited list of target volume devices of a specified protection plan.

## SYNOPSIS

`mrcli` [`-c` *configfile*] `-u` *user* `-m` *maxrepname* [`-v`] `getTargetVolumes` *planID*

## DESCRIPTION

The command `getTargetVolumes` returns a comma-delimited list of target volumes associated with a specified protection plan ID. The protection plan ID is obtained through the command `getProtectionPlanId`.

## OPTIONS

| | |
|---|---|
| **-m** *maxrepname* | The IP address or DNS name of the MaxRep Replication Engine. |
| *planID* | The ID of the protection plan that is being queried. |
| **-u** *user* | Identifies the administrator account that runs the command. |
| **-c** *configfile* | Specifies the configuration file to modify logging. When used, the `-c` command must be the first option entered at the command line. |
| **-v** | Prints the current version of the MaxRep CLI then exits. This option should be run on its own, separate from additional options.<br>`$ mrcli -v` |

## EXAMPLE

**Task**

Run the command `getTargetVolumes` to obtain a comma-delimited list of source volumes names of protection plan ID `25` on MaxRep Replication Engine `co-mrengine-02`.

**Parameters**

- planID: `25`
- maxrepname: `co-mrengine-02`

```
$ mrcli -u admin -m co-mrengine-02 getTargetVolumes 25
```

### getEngineTime

Returns engine time in UTC.

## SYNOPSIS

`mrcli -u` *user* `-m` *maxrepname* [`-v`] `getEngineTime` *arrayname*

## DESCRIPTION

The command `getEngineTime` returns the engine in UTC.

## OPTIONS

**-m** *maxrepname* — The IP address or DNS name of the MaxRep Replication Engine.

**-u** *user* — Identifies the administrator account that runs the command.

*arrayname* — Name of the array which is being queried.

**-v** — Prints the current version of the MaxRep CLI then exits. This option should be run on its own, separate from additional options.

```
$ mrcli -v
```

## EXAMPLE

**Task**

Run the command `getEngineTime` to obtain the UTC time of MaxRep engine `co-mrengine-02`.

**Parameters**

maxrepname: `co-mrengine-02`

```
$ mrcli -u admin -m co-mrengine-02 getEngineTime
```

### isActiveControlService

Indicates whether the given maxrepname is hosting the active control service.

## SYNOPSIS

`mrcli` [`-c` *configfile*] `-u` *user* `-m` *maxrepname* [`-v`] `isActiveControlService`

## DESCRIPTION

Run the command `isActiveControlService` to learn if a specified `maxrepname` is running the active control service in the current configuration. The command displays RETURN_CODE_OK (0) if the given `maxrepname` is the current host of the active control service.

## OPTIONS

**`-m` *maxrepname*** The IP address or DNS name of the MaxRep Replication Engine.

**`-u` *user*** Identifies the administrator account that runs the command.

**`-c` *configfile*** Specifies the configuration file to modify logging. When used, the `-c` command must be the first option entered at the command line.

**`-v`** Prints the current version of the MaxRep CLI then exits. This option should be run on its own, separate from additional options.

```
$ mrcli -v
```

## EXAMPLE

**Task**

Run the command `isActiveControlService` to learn if Replication Engine `co-mrengine-02` is running the active control service.

**Parameters**

maxrepname: `co-mrengine-02`

```
$ mrcli -u admin -m co-mrengine-02 isActiveControlService
```

### isPlanTargetByName

Indicates whether the given *maxrepname* is the target engine for the specified protection plan.

## SYNOPSIS

`mrcli` [`-c` *configfile*] `-u` *user* `-m` *maxrepname* [`-v`] `isPlanTargetByName` *planname*

## DESCRIPTION

Run the command `isPlanTargetByName` to learn if a specified *maxrepname* is the target engine for a specified protection plan. The command displays RETURN_CODE_OK (0) if the given *maxrepname* is the target engine for the protection plan.

## OPTIONS

**-m** *maxrepname* — The IP address or DNS name of the MaxRep Replication Engine.

**-u** *user* — Identifies the administrator account that runs the command.

**-c** *configfile* — Specifies the configuration file to modify logging. When used, the `-c` command must be the first option entered at the command line.

**-v** — Prints the current version of the MaxRep CLI then exits. This option should be run on its own, separate from additional options.

```
$ mrcli -v
```

*planname* — The name of the protection plan being queried.

## EXAMPLE

**Task**

Run the command `isPlanTargetByName` to learn if Replication Engine `co-mrengine-02` is the target engine for protection plan `ReplicationPlan02`.

**Parameters**

- maxrepname: `co-mrengine-02`
- planName: `ReplicationPlan02`

```
$ mrcli -u admin -m co-mrengine-02 isPlanTargetByName
ReplicationPlan02
```

### performRollback

Performs a rollback of a specified plan to the provided timestamp, or the most recent common time.

## SYNOPSIS

`mrcli` [`-c` *configfile*] `-u` *user* `-m` *maxrepname* `performRollback` [`-v`] *planName* [`-t` *timestamp/tag*]

## DESCRIPTION

The command `performRollback` performs a rollback of a specified protection plan on a target Replication Engine. The `performRollback` command does not deactivate the protection plan. Oracle recommends that you deactivate the protection plan after the rollback completes (see `getRollBackStatus`). Retention logs associated with the plan are automatically deleted after the rollback completes.

The `performRollback` command doest not provide the option to mount a rolled-back target LUN. To perform a rolled-back target, use the MaxRep GUI.

## OPTIONS

| | |
|---|---|
| **-m** *maxrepname* | The IP address or DNS name of the MaxRep Replication Engine. |
| *planName* | Specifies the name of the protection plan. |
| **-t** *timestamp/tag* | The timestamp for the rollback of the protection plan. |
| **-u** *user* | Identifies the administrator account that runs the command. |
| **-c** *configfile* | Specifies the configuration file to modify logging. When used, the `-c` command must be the first option entered at the command line. |

## EXAMPLE

**Task**

Run the command `performRollback` to roll back plan `RepPlan02` to the time `2015/4/18 0:37:38:244:747:8` on MaxRep Replication Engine `co-mrengine-01`. Perform a roll back also to `tag1`.

**Parameters**

- maxrepname: `co-mrengine-01`
- planName: `RepPlan02`
- timestamp/tag: `2015/4/18 0:37:38:244:747:8`

```
$ mrcli -u admin -m co-mrengine-01 performRollback RepPlan02 -t
"2015/4/18 0:37:38:244:747:8

$ mrcli -u admin -m co-mrengine-01 performRollback RepPlan02 -t
tag1
```

**help**

Prints help.

## SYNOPSIS

`mrcli help` [*command*]

## DESCRIPTION

The command `help` prints help for the MaxRep CLI, or a specified command name. Executing `mrcli` or `mrcli help` at the command line will display help, and print a summary of documented commands for which help is available. Executing `mrcli help` followed by a command name will display help about that specified command. The `mrcli help` command does not require a username or a MaxRep Replication Engine.

## OPTIONS

***command*** Specifies the command for which help is displayed.

## EXAMPLE

**Task**

First, run the `help` command to display the version number of the MaxRep CLI application, and a list of documented commands for which help is available. Second, run the `help` command to display help for the command `getProtectionPlans`.

**Parameters**

- command: `getProtectionPlans`

```
$ mrcli help

$ mrcli help getProtectionPlans
```

**utility:getArrayIpFromGuid**

Returns the IP address on record for a Pillar Axiom given its GUID.

## SYNOPSIS

`mrcli` [`-c` *configfile*]`-u` *user* `-m` *maxrepname* [`-v`] `utility:getArrayIpFromGuid` *arrayGuid*

## DESCRIPTION

The command `utility:getArrayIpFromGuid` is a utility namespace command that returns the IP address on record for a specified Pillar Axiom provided its GUID.

## OPTIONS

**`Guid`** The GUID of the array.

**`-m`** *maxrepname* The IP address or DNS name of the MaxRep Replication Engine.

**`-u`** *user* Identifies the administrator account that runs the command.

**`-c`** *configfile* Specifies the configuration file to modify logging. When used, the `-c` command must be the first option entered at the command line.

**`-v`** Prints the current version of the MaxRep CLI then exits. This option should be run on its own, separate from additional options.

```
$ mrcli -v
```

## EXAMPLE

**Task**

Run the command `utility:getArrayIpFromGuid` from Guid `998FEFF4-89F3-4CF6-A243` on MaxRep engine `co-mrengine-01`.

**Parameters**

- maxrepname: `co-mrengine-01`
- GUID: `998FEFF4-89F3-4CF6-A243`

```
$ mrcli -u admin -m co-mrengine-01 utility:getArrayIpFromGuid
998FEFF4-89F3-4CF6-A243
```

### `utility:getArrayNameFromGuid`

Returns the array name given the GUID.

## SYNOPSIS

`mrcli` [`-c` *configfile*] `-u` *user* `-m` *maxrepname* `utility:getArrayNameFromGuid` *arrayGuid*

## DESCRIPTION

The command `utility:getArrayNameFromGuid` is a utility-namespace command that returns the array name on record for the Pillar Axiom system given its GUID.

## OPTIONS

**`Guid`** The GUID of the array.

| | |
|---|---|
| **-m** *maxrepname* | The IP address or DNS name of the MaxRep Replication Engine. |
| **-u** *user* | Identifies the administrator account that runs the command. |
| **-c** *configfile* | Specifies the configuration file to modify logging. When used, the `-c` command must be the first option entered at the command line. |

## EXAMPLE

**Task**

Run the command `utility:getArrayNameFromGuid` to obtain the name of the array on Pillar Axiom system associated with GUID `998FEFF4-4CF6-A243-84FBCA055AE2`. The Pillar Axiom system is registered with MaxRep Replication Engine `co-mrengine-01`.

**Parameters**

- maxrepname: `co-mrengine-01`
- GUID: `998FEFF4-4CF6-A243-84FBCA055AE2`

```
$ mrcli -u admin -m co-mrengine-01 utility:getArrayNameFromGuid
998FEFF4-4CF6-A243-84FBCA055AE2
```

### `utility:getArrayNameFromLuid`

Returns the name on record for the array that hosts the LUN that is identified by its LUID.

## SYNOPSIS

`mrcli` [`-c` *configfile*] `-u` *user* `-m` *maxrepname* [`-x`] *stdout* | *filename.xml* [`-v`] `utility:getArrayNameFromLuid` *luid*

## DESCRIPTION

The command `utility:getArrayNameFromLuid` is a utility-namespace command that returns the name of a specified Pillar Axiom array that hosts a LUN with its LUID.

## OPTIONS

| | |
|---|---|
| **luid** | The LUN ID. |
| **-m** *maxrepname* | The IP address or DNS name of the MaxRep Replication Engine. |
| **-u** *user* | Identifies the administrator account that runs the command. |

| | |
|---|---|
| **-c** *configfile* | Specifies the configuration file to modify logging. When used, the `-c` command must be the first option entered at the command line. |
| **-v** | Prints the current version of the MaxRep CLI then exits. This option should be run on its own, separate from additional options.<br>`$ mrcli -v` |
| **-x** *stdout* \| *filename.xml* | Prints output in XML format. |

#### EXAMPLE

**Task**

Run the command `utility:getArrayNameFromLuid` using LUID `2000b080047001268` associated with MaxRep Replication Engine `co-mrengine-23`.

**Parameters**

- maxrepname: `co-mrengine-23`
- LUID: `2000b080047001268`

```
$ mrcli -u admin -m co-mrengine-23 utility:getArrayNameFromLuid
2000b080047001268
```

## utility:getProtectionPlanId

Presents the ID of the protection plan.

### SYNOPSIS

`mrcli` [`-c` *configfile*] `-u` *user* `-m` *maxrepname* [`-v`] `utility:getProtectionPlanId` *planName*

### DESCRIPTION

If you are unsure of the ID of the protection plan in which you are working in or that you are searching for, you can return the ID of the protection plan with the plan name. Run the command `utility:getProtectionPlanId` to obtain the ID of a specific protection plan.

### OPTIONS

| | |
|---|---|
| **-m** *maxrepname* | The IP address or DNS name of the MaxRep Replication Engine. |
| *planName* | Specifies the name of the protection plan. |
| **-u** *user* | Identifies the administrator account that runs the command. |

**-c** *configfile* Specifies the configuration file to modify logging. When used, the `-c` command must be the first option entered at the command line.

**-v** Prints the current version of the MaxRep CLI then exits. This option should be run on its own, separate from additional options.

```
$ mrcli -v
```

## EXAMPLE

**Task**

Run the command `utility:getProtectionPlanId` to obtain the internal ID of protection `replicationplan01` on MaxRep Replication Engine `co-mrengine-01`.

**Parameters**

- planName: `replicationplan01`
- maxrepname: `co-mrengine-01`

```
$ mrcli -u admin -m co-mrengine-01 utility:getProtectionPlanId
replicationplan01
```

### utility:getProtectionPlanName

Returns the name of the protection plan.

## SYNOPSIS

`mrcli -u` *user* `-m` *maxrepname* `utility:getProtectionPlanName` *planID*

## DESCRIPTION

If you are unsure of the name of the protection plan in which you are working in or that you are searching for, you can return the name of the protection plan with its internal ID. Run the `utility:getProtectionPlanName` to obtain the name of a specific protection plan.

## OPTIONS

**-m** *maxrepname* The IP address or DNS name of the MaxRep Replication Engine.

*planID* The ID of the protection plan that is being queried.

**-u** *user* Identifies the administrator account that runs the command.

## EXAMPLE

**Task**

Run the `utility:getProtectionPlanName` command to return the protection plan name associated with plan ID `44` on MaxRep Replication Engine `co-mrengine-05`.

**Parameters**

- planID: `44`
- maxrepname: `co-mrengine-05` or `10.123.456.789`
- filename.xml: `engine59.xml`

```
$ mrcli -u admin -m co-mrengine-05 utility:getProtectionPlanName
44
```

### utility:getFQNFromLuid

Returns the Fully Qualified Name (FQN) of a LUN given its LUID.

## SYNOPSIS

`mrcli` [`-c` *configfile*] `-u` *user* `-m` *maxrepname* [`-v`] `utility:getFQNFromLuid` *luid*

## DESCRIPTION

The command `utility:getFQNFromLuid` is a utility namespace command that returns the Fully Qualified Name (FQN) of a LUN given its LUID. At successful completion of the command, the command line returns the FQN and RETURN-CODE-OK (0).

## OPTIONS

**`luid`** The LUN ID.

**`-m` *maxrepname*** The IP address or DNS name of the MaxRep Replication Engine.

**`-u` *user*** Identifies the administrator account that runs the command.

**`-c` *configfile*** Specifies the configuration file to modify logging. When used, the `-c` command must be the first option entered at the command line.

**`-v`** Prints the current version of the MaxRep CLI then exits. This option should be run on its own, separate from additional options.

```
$ mrcli -v
```

## EXAMPLE

**Task**

Run the command `utility:getfqnfromluid` to return the FQN of the LUN identified by LUID `2000b080047001268`, and associated with MaxRep Replication Engine `co-mrengine-02`.

**Parameters**

- maxrepname: `co-mrengine-02`
- LUID: `2000b080047001268`

```
$ mrcli -u admin -m co-mrengine-02 utility:getfqnfromluid
2000b080047001268
```

### utility:getScenarioId

Returns the internal ID of the scenario associated with a protection plan ID.

## SYNOPSIS

`mrcli` [`-c` *configfile*] `-u` *user* `-m` *maxrepname* [`-v`] `utility:getScenarioId` *planID scenariotype*

## DESCRIPTION

The command `utility:getScenarioId` is a utility namespace command that returns the internl ID of the scenario associated with a protection plan ID.

## OPTIONS

**`-m` *maxrepname*** — The IP address or DNS name of the MaxRep Replication Engine.

***planID*** — The ID of the protection plan that is being queried.

**`-u` *user*** — Identifies the administrator account that runs the command.

**`-c` *configfile*** — Specifies the configuration file to modify logging. When used, the `-c` command must be the first option entered at the command line.

**`-v`** — Prints the current version of the MaxRep CLI then exits. This option should be run on its own, separate from additional options.

```
$ mrcli -v
```

## EXAMPLE

**Task**

Run the command `utility:getScenarioId` to learn the scenario ID of protection plan ID `42` on MaxRep Replication Engine `co-mrengine-02` . The scenario type of the plan is `backup protection`.

**Parameters**

- maxrepname: `co-mrengine-02`
- planID: `42`
- scenariotype: `backup protection`

```
$ mrcli -u admin -m co-mrengine-02 utility:getScenarioId 42
backup protection
```

### utility:getEngineIpFromGuid

Returns the IP address for a specified MaxRep Replication Engine.

## SYNOPSIS

`mrcli -u` *user* `-m` *maxrepname* `utility:getEngineIpFromGuid` *engineGuid*

## DESCRIPTION

The command `utility:getEngineIpFromGuid` is a utility-namespace commad that displays the IP address on record for a specified MaxRep Replication Engine, provided its GUID.

## OPTIONS

| | |
|---|---|
| **engineGuid** | The GUID of the MaxRep Replication Engine. |
| **-m** *maxrepname* | The IP address or DNS name of the MaxRep Replication Engine. |
| **-u** *user* | Identifies the administrator account that runs the command. |

## EXAMPLE

**Task**

Run the command `utility:getEngineIpFromGuid` to obtain the IP address from MaxRep Replication Engine `co-mrengine-02`, using its GUID `22e5d710-cbb7-4139-88cd-64bfbceec365`.

**Parameters**

- maxrepname: `co-mrengine-02`
- GUID: `22e5d710-cbb7-4139-88cd-64bfbceec365`

```
$ mrcli -u admin -m co-mrengine-02 utility:getengineipfromguid
22e5d710-cbb7-4139-88cd-64bfbceec365
```

### utility:getTargetEngineId

Returns a comma-delimited list of GUIDs for the target engines associated with a protection plan ID.

## SYNOPSIS

`mrcli` [`-c` *configfile*] `-u` *user* `-m` *maxrepname* [`-v`] `utility:getTargetEngineId` *planID*

## DESCRIPTION

The command `utility:getTargetEngineId` is a utility-namespace command that returns a comma-delimited list of target engine GUIDs associated with a specified protection plan, given the protection plan ID and the MaxRep Replication Engine. The protection plan ID is obtained through the command `utility:getProtectionPlanId`.

## OPTIONS

| | |
|---|---|
| **-m** *maxrepname* | The IP address or DNS name of the MaxRep Replication Engine. |
| *planID* | The ID of the protection plan that is being queried. |
| **-u** *user* | Identifies the administrator account that runs the command. |
| **-v** | Prints the current version of the MaxRep CLI then exits. This option should be run on its own, separate from additional options.<br>`$ mrcli -v` |
| **-c** *configfile* | Specifies the configuration file to modify logging. When used, the `-c` command must be the first option entered at the command line. |

## EXAMPLE

**Task**

Run the command `utility:getTargetEngineId` to obtain a list of source engine IDs associated with protection plan `22` on MaxRep Replication Engine `co-mrengine-01`.

**Parameters**

- maxrepname: `co-mrengine-01`
- planID: `22`

```
$ mrcli -u admin -m co-mrengine-01 utility:gettargetengineid 22
```

### utility:getSourceEngineId

Returns a comma-delimited list of GUIDs of the source engines associated with a protection plan.

## SYNOPSIS

`mrcli` [`-c` *configfile*] `-u` *user* `-m` *maxrepname* [`-x` *stdout* | *filename.xml*] [`-v`] `utility:getSourceEngineId` *planID*

## DESCRIPTION

The command `utility:getSourceEngineId` is a utility-namespace command that returns a comma-delimited list of source engine GUIDs associated with a specified protection plan, given the protection plan ID and the MaxRep Replication Engine. The protection plan ID is obtained through the command `utility:getProtectionPlanId`.

## OPTIONS

| | |
|---|---|
| **-m** *maxrepname* | The IP address or DNS name of the MaxRep Replication Engine. |
| *planID* | The ID of the protection plan that is being queried. |
| **-u** *user* | Identifies the administrator account that runs the command. |
| **-v** | Prints the current version of the MaxRep CLI then exits. This option should be run on its own, separate from additional options.<br>`$ mrcli -v` |
| **-x** *stdout* \| *filename.xml* | Prints output in XML format. |

**-c** ***configfile*** Specifies the configuration file to modify logging. When used, the `-c` command must be the first option entered at the command line.

## EXAMPLE

**Task**

Run the command `utility:getSourceEngineId` to obtain a list of source engine IDs associated with protection plan `22` on MaxRep Replication Engine `co-mrengine-01`.

**Parameters**

- maxrepname: `co-mrengine-01`
- planID: `22`

```
$ mrcli -u admin -m co-mrengine-01 utility:getSourceEngineId 22
```

APPENDIX C

# Glossary

## Glossary

The following terms are used with these meanings in the Oracle MaxRep documentation.

**access control group (ACG)**

A method that restricts the exported copy to a host or a group of hosts. Specifying an ACG is the equivalent of LUN host mapping on the Oracle FS System.

**application consistency**

Application data can be spread across multiple LUNs. Application consistency provides a synchronized copy of all LUNs that are associated with the application.

**asynchronous replication**

The process of providing time lagged copies of data. Asynchronous replication uses a combination of three protection schemes to ensure data integrity: a data change map, a write journal, and a drive cache on the Oracle FS System.

Application performance of asynchronous replication is better than that of synchronous replication because asynchronous replication I/O is blocked only until the primary storage acknowledges the write.

**bitmap mode**

The Oracle MaxRep Replication Engine cache switches to bitmap mode when, due to WAN connectivity issues or other replication performance bottlenecks, the DRAM cache is full, and the Replication Engine cache is close to becoming full. In bitmap mode the Replication Engine keeps track of the changed data blocks so that, when connectivity is restored, the changed block can be replicated.

**block-based replication**

Replicates raw blocks of data regardless of the file system or application.

**bookmarks**

Application consistency markers that are created within a LUN that are used in the retention log to create a synchronized copy.

**cache LUN**

See *home LUN*.

**Continuous Data Protection (CDP)**

Real-time data protection that provides the ability for a backup administrator to restore the data to any point in time.

**control service**

The service that is used to configure the replication process and policies.

**data cache**

Temporary storage of replication data in memory on the replication engine.

**differential sync**

Replicates only the data that has changed since the last successful full synchronization.

**FX agent**

A host-based file system splitter that enables application protection and data replication.

**home LUN**

A LUN on the Oracle FS System that stores the configuration data and cache for the Replication Engine. Also called *cache LUN*.

**initial sync**

The initial copy of the data sent from the source LUN to the target LUN.

**initiator ports**

The SAN ports that initiate I/O to a storage device. On a Replication Engine, at least one port must be an initiator port. The initiator port for the source LUN is designated as AIS, and the designator for the target LUN initiator is AIT.

**local replication**

Replication that occurs only on the primary site.

**MaxRep agent**

An application specific agent that provides time sequenced application consistency.

**multi-hop replication**

Two-stage replication that provides a synchronous replication, which is then asynchronously replicated to a third location. Multi-hop replication uses a synchronous and an asynchronous replication license.

**Node Port ID Virtualization (NPIV)**

A method to provide multiple virtual node ports (also called N_Ports) to be presented over a single, physical fiber channel port.

**Oracle FS System**

The Oracle FS System is a complete and integrated full-featured network storage system.

**Oracle MaxRep for SAN**

(1) A block-based replication solution that provides the following benefits:

- Disaster recovery
- Business continuity
- Application consistent recovery

(2) The graphical user interface (GUI) that provides the configuration, control, and monitoring operations for Oracle MaxRep for SAN.

**physical snapshot**

A point-in-time full volume snapshot, or copy, of a source LUN. The full replicated copy can be accessed directly from the Oracle FS System.

**primary LUN**

see *source LUN*.

**process service**

The utility that runs on the active Replication Engine and manages the replication of protection plans.

**profiler tool**

Provides an estimate for the size of the target copy and event journal, and for the amount of bandwidth that is required between the source and target Oracle FS Systems to meet requested retention windows and recovery point objectives (RPOs).

**protection plan**

The collection of specific policies and configurations that define the replication and retention policies for one or more replication pairs in the Oracle MaxRep software.

**recovery point objective (RPO)**

The maximum time period of acceptable data loss before a disaster has an adverse impact on data recovery.

The maximum desired time period prior to a failure or disaster during which changes to data might be lost as a consequence to attempts of data recovery. Data changes preceding the failure or disaster by at least this time period are preserved by recovery actions. The RPO default value is Zero and is equivalent to a "zero data loss" requirement.

**recovery snapshot**

A mechanism for recovering, or copying, data on a LUN. An administrator creates a recovery snapshot in a physical or virtual capacity.

**recovery time objective (RTO)**

The maximum acceptable amount of time to become fully operational after an interruption of service.

**remote replication**

The replication that takes place between a primary and secondary site.

**Replication Engine**

Oracle FS System hardware required for Oracle MaxRep.

**Replication Engine cache**

The memory available on the replication engine for staging the data that is associated with replication operations.

**Replication Engine target ports**

The ports on the Replication Engine that receive I/O commands from any initiator, usually from the Oracle FS System. Each Replication Engine must have at least one target port.

**replication pair**

The association of a source LUN and a target LUN for recovery purposes.

**resync**

The operation that re-synchronizes the replication data to achieve parity between the LUNs in a replication pair after an interruption occurs.

**retention journal**

The time indexed replication events that allows the data to be rolled back to any point in time.

**retention LUNs**

The LUNs on the Oracle FS System that hold the retention journal for a protection plan.

**retention period**

The configurable period of time for which the retention logs should attempt to keep all the changes for a given replication pair. Data recovery is limited to the time period defined in the retention logs.

**reverse replication**

Replicating data from the remote site back to the primary site during a service interruption. The primary site becomes the remote site until the original remote site comes back online after a service interruption.

**rollback**

The restoration of data to a specified earlier point in time.

**scheduled checkpoint**

The mechanism to automate the creation of periodic recovery points to roll back to.

**scheduled physical snapshot**

Mechanism to automate periodically creating recovery points to which data can be rolled back.

**secondary LUN**

see *target LUN*.

**source LUN**

The LUN designated for replication that is located on the primary Oracle FS System. The source LUN is also called a primary LUN.

**sparse retention**

Retains fewer bookmarks (recovery fall back points) for older data in specified retention period. The feature that backs up older data less frequently than new data.

**synchronous replication**

Ensures that a write operation to the primary Oracle FS System will not be acknowledged until it has been written to both the primary Oracle FS System and the Replication Engine.

**target LUN**

The LUN on the Oracle FS System that is identified as a destination for replication. The target LUN must be created on the Oracle FS System prior to configuring replication. A target LUN is also called a secondary LUN.

**virtual snapshot**

A virtual snapshot, also called a *Vsnap*, is a type of recovery mechanism that provides a point-in-time, virtual copy of a source LUN. Virtual snapshots are created on the Replication Engine, and require no disk space on the primary or secondary Oracle FS System. Creating a virtual snapshot does not interfere with the current replication.

**VX agent**

Host-based volume splitter that enables application protection and replication.

**write splitter**

The Oracle FS System feature that controls the data write operations by splitting the write data between the primary Oracle FS System and the Replication Engine. The write splitter runs on the Controller.

# Index

## A



## B



## C

## D



## E



## F

## G



## H



## I



## L



## M

## R

## S

## T



## U



## V



## W



## Z