Pillar Axiom MaxRep Replication

User's Guide

for SAN

ORACLE

PILLAR AXIOM

Part number: E28247-01
Pillar Axiom MaxRep Replication for SAN v2.0
2012 March

Table of Contents

Chapter 4 Configure Data Protection

Chapter 5 Monitor Data Protection

Chapter 6 Recover Protected Data

List of Figures

List of Tables

Preface

Related Documentation

Familiarize yourself with the following related documentation:

- *Pillar Axiom Customer Release Notes*: Includes late-breaking important information about the installation and operation of the Pillar Axiom system.
- *Pillar Axiom Administrator's Guide*: Provides detailed information on creating and managing storage resources.
- *Pillar Axiom MaxRep Replication for SAN Hardware Guide*: Describes hardware installation and initial software installation for Pillar Axiom MaxRep Replication for SAN.

Typographical Conventions

Table 1 Typography to mark certain content

Convention	Meaning
italics	Within normal text, words in italics indicate: • A reference to a book title. • New terms and emphasized words. • Command variables.
`monospace`	Indicates one of the following, depending on the context: • The name of a file or the path to the file. • *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 a graphical user interface (GUI). For example, "Click Storage > Clone

Table 1 Typography to mark certain content (continued)

Convention	Meaning
	LUNs" means to click the Clone LUNs link on the Storage page in the graphical user interface (GUI).
...	Used within an expression of a navigation path or within a cascading menu structure. The ellipsis indicates that one or more steps have been omitted from the path or menu structure. For example, in the Groups > Volume Groups > Actions > ... > Data Protection > Create menu structure, the ... implies that one or more menu items have been omitted.

Oracle Contacts

Table 2 Oracle resources

For help with...	Contact...
Support	https://support.oracle.com
Training	https://education.oracle.com
Documentation	• Oracle Technical Network: http://www.oracle.com/technetwork/indexes/documentation/index.html#storage • From the Pillar Axiom Storage Services Manager (GUI): Support > Documentation • From Pillar Axiom HTTP access: http://*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
Contact Oracle	http://www.oracle.com/us/corporate/contact/index.html

CHAPTER 1

Introduction to Pillar Axiom MaxRep Replication for SAN

About Pillar Axiom MaxRep Replication for SAN

Pillar Axiom MaxRep Replication for SAN enables you to replicate and restore Pillar Axiom system data in a storage area network (SAN) environment.

In SAN replication, pairs of parallel LUNs, made up of source and target LUNs, are called replication pairs. The LUNs can reside on two Pillar Axiom systems in a single location or on separate remotely distributed Pillar Axiom systems, designated primary and secondary.

One or more Pillar Axiom Replication Engines manage and monitor the 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.

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

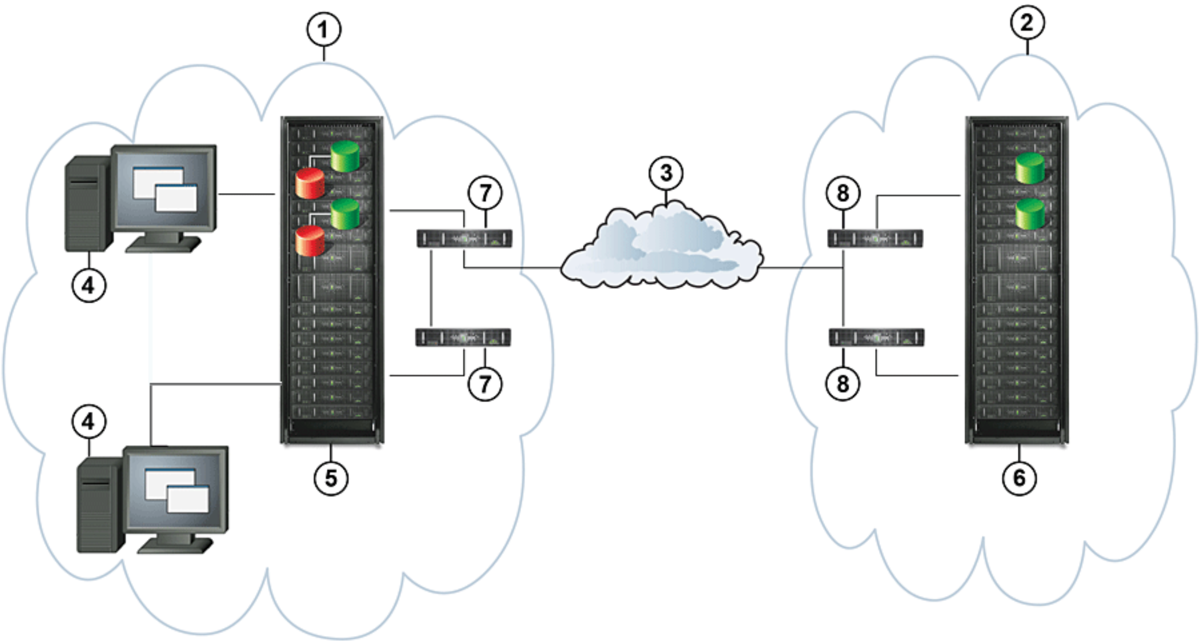
Pillar Axiom MaxRep Replication for SAN supports synchronous and asynchronous LUN replication or application consistent volume sets.

- Synchronous replication requires at least one Pillar Axiom Replication Engine and is supported when the source and target LUNs are attached to the same SAN network. Replication may also be synchronous when the source and target LUNs are located in two data centers connected by an extended SAN fabric that uses dense wavelength division multiplexing (DWDM) over dark fibre, which is the network system that consists of fibre optic cables between the primary and secondary locations.

- Asynchronous replication requires at least two Pillar AxiomReplication Engines and is supported in most cases 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.

To ensure high availability, deploy two Replication Engines. 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 1 Asynchronous Pillar Axiom MaxRep Replication for SAN configuration



Legend

1 Primary site	5 Primary Pillar Axiom system
2 Secondary site	6 Secondary Pillar Axiom system
3 WAN connection	7 Replication Engines on the primary site clustered for high availability
4 Application servers	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 Pillar Axiom MaxRep Replication for SAN.

Related concepts

- *About Pillar Axiom MaxRep Replication for SAN Components*
- *About How Pillar Axiom MaxRep Replication for SAN Works*
- *Replication Concepts*
- *About Replication Configurations*

About Pillar Axiom MaxRep Replication for SAN Components

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

The Pillar Axiom MaxRep Replication for SAN includes the following components:

Pillar Axiom system

The Pillar Axiom system is an application aware storage solution using policy based Quality of Service technology to serve application storage over Fibre Channel (FC) or iSCSI storage area networks. The replication process begins with the Pillar Axiom system that accepts a write operation to the protected LUNs and forwards the write operation to the Pillar Axiom Replication Engine for replication.

Pillar Axiom 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 interface of the Replication Engine, you can create, monitor, and recover protection plans. Utilization and trending reports and alerts are also managed by the Replication Engine.

MaxRep Agents

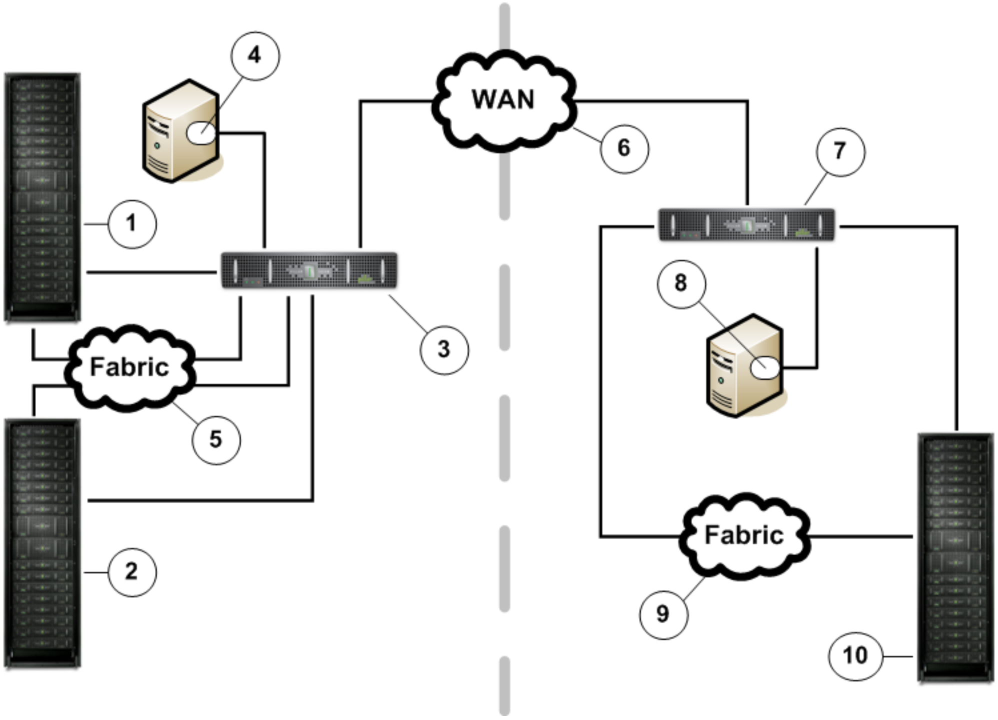
Optional MaxRep Agents are installed on application hosts and can issue application consistency bookmarks on a scheduled basis.

Replication Engine Cluster

Replication Engine Cluster is an optional component of the Pillar Axiom MaxRep solution. This component is a high availability feature that includes a passive Replication Engine, which is ready to take over when the active Replication Engine is down.

The following figure shows the relationship of each Pillar Axiom MaxRep Replication for SAN component in a remotely distributed Pillar Axiom system.

Figure 2 Pillar Axiom MaxRep components



Legend

1 Primary Pillar Axiom system	6 Wide area network (WAN)
2 Local secondary Pillar Axiom system	7 Remote Replication Engine
3 Replication Engine	8 Remote host with MaxRep agent
4 Host with MaxRep agent	9 Fabric (FC) or LAN (iSCSI)
5 Fabric (FC) or LAN (iSCSI)	10 Remote secondary Pillar Axiom system

Related concepts

- *About Pillar Axiom MaxRep Replication for SAN*
- *Replication Concepts*

About How Pillar Axiom MaxRep Replication for SAN Works

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

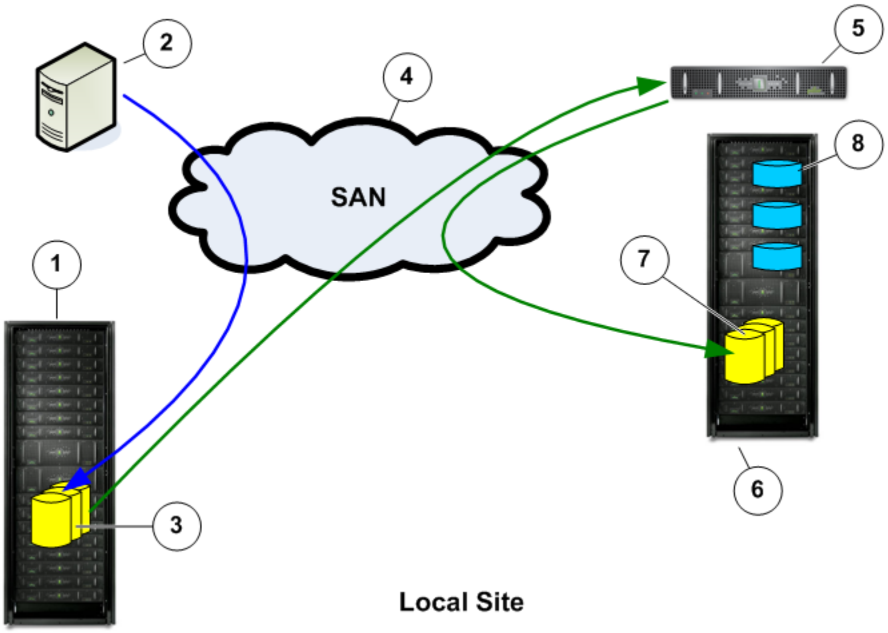
Pillar Axiom MaxRep Replication for SAN replicates your mission-critical Axiom LUNs to one or more secondary LUNs that can be either local or remote.

In the figure below, source LUNs are configured in a way so the LUNs can be replicated to an alternate Pillar Axiom system. After the initial synchronization, as new data is written to the protected source LUNs, the Axiom system sends a copy of the data to the Pillar Axiom Replication Engine along with additional metadata that describes the location of the data on 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 as well as the retention LUN, or journal, of the protection plan LUNs.

Retention LUNs are LUNs on the Pillar Axiom 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 How replication works



Legend

1 Primary Pillar Axiom system	5 Replication Engine
2 Application server	6 Local secondary Pillar Axiom system
3 Source LUNs	7 Target LUNs
4 Storage area network (SAN) fabric	8 Pillar Axiom MaxRep LUNs ○ Home LUN: Software and cache ○ Backup LUN: Configuration backup ○ Retention LUN: Replication journal

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 in the event of a failure or replacement of the Replication Engine. The benefit of such a configuration is that Pillar Axiom MaxRep Replication for SAN can be deployed into your existing environments without disrupting your business continuity.

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 Pillar Axiom MaxRep Replication for SAN graphical user interface (GUI) uses the terms *sync* and *resync* to refer to synchronization and resynchronization, respectively.

Resync Step 1

This is 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, this copy transfers only unmatched blocks of data between the source and target LUNs are transferred between two Pillar Axiom 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 Synchronization Step 1 process is journaled for processing in Synchronization Step 2. The Replication Engine replicates the captured changes to the target LUN.

Differential Sync	In the Differential Sync step Pillar Axiom MaxRep Replication 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 uses a similar synchronization process. Pillar Axiom MaxRep Replication for SAN supports Fast Resync, which replicates only unmatched blocks to the target LUN during the initial synchronization step.

During maintenance activities on a source LUN or during an actual failure of a source LUN, Pillar Axiom MaxRep Replication for SAN can switch direction in order to restore the source LUN from the target LUN. Because Pillar Axiom MaxRep Replication 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 MaxRep agents are in use, the target LUN can also be rolled back to a consistency bookmark to ensure consistency of data.

Pillar Axiom 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 concepts

- *Replication Concepts*

Related references

- *Pillar Axiom MaxRep Replication for SAN Requirements*

Replication Concepts

Replicating data using Pillar Axiom MaxRep Replication 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 location. 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.

Pillar Axiom MaxRep Replication 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 Pillar Axiom 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 company’s critical technology infrastructure. A Disaster Recovery solution using CDP technology replicates your data to a secondary site. In case of disaster you can get immediate access to the data that had been on the primary site up to the moment of the disaster.

Replication Stages

Pillar Axiom MaxRep Replication for SAN replicates drive level data in three stages:

Resyncing (Step 1)	The 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 and 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.
- Filesystem consistency through host-based 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. Pillar Axiom MaxRep Replication for SAN also provides application consistency through host-based MaxRep Agents.

Bookmarks can only be created by MaxRep agents that work with an application or filesystem.

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 data can be rolled back to any of the application-consistent bookmarks in this retention window. Alternatively, the data 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 will only be *Consistent*.

There are three 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 will be overwritten once 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. This 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 discarding older data changes within the retention log files to make room for new data changes.

Snapshot
A snapshot is an accessible replica of data from the primary Pillar Axiom system as it existed at a single point in time in the retention window. There are two types of snapshots: physical replication copies and virtual snapshots.

- A physical replication copy 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).

  - 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.

These copies and snapshots can be accessed in one of following modes:

Read-Only

Read-only snapshots are for informational purposes and cannot accept or retain writes.

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 Tracking

Read-write tracking virtual snapshots go a step further than read-write snapshots. This mode is especially useful if a new virtual snapshot has to be updated with the writes of an un-mounted virtual snapshot.

Related concepts

- *About How Pillar Axiom MaxRep Replication for SAN Works*
- *About Application Consistency Protection Plans*

Related references

- *Pillar Axiom MaxRep Replication for SAN Requirements*

Pillar Axiom MaxRep Replication for SAN Requirements

Pillar Axiom MaxRep Replication for SAN has a number of requirements that must be met for replication to work properly.

Table 3 Pillar Axiom MaxRep requirements

Item	Requirement
Pillar Axiom system	All source and target Pillar Axiom systems must be Pillar Axiom 500 or Pillar Axiom 600 and running Pillar Axiom Storage Services Manager release 5.3.0, or higher. • For Fibre Channel (FC) only: The Pillar Axiom system must have FC SAN fabric connectivity. • For iSCSI only: The Pillar Axiom system must have Ethernet LAN connectivity. Brick capacity must be sized properly to account for the additional capacity required for the replication solution. The Brick spindle count must be sized properly to account for the performance requirements for the replication solution.
Pillar Axiom Replication Engines	The number of Pillar Axiom Replication Engines required varies based upon the specific solution. Synchronous replication between two Pillar Axiom systems connected to the same SAN fabric may only require a single Replication Engine. Complex implementations that include 1-to-n or n-to-1 synchronous and asynchronous replication with Replication Engine high availability (HA) clustering can include up to eight Replication Engines. Refer to your account representative to ensure the number of Replication Engines in your environment is sufficient for your replication needs.
SAN ports	Each Replication Engine that uses FC connectivity to a primary or secondary Pillar Axiom system requires eight connections. These connections are rated up to 1 Gb/s (iSCSI) or 4 Gb/s (FC) and are provided through little (LC) connectors on the back of the Replication Engine.
Ethernet ports	Each Replication Engine that uses FC or iSCSI connectivity to a primary or secondary Pillar Axiom system requires two Ethernet connections: One Gigabit

Table 3 Pillar Axiom MaxRep requirements (continued)

Item	Requirement
	Ethernet (1 GbE) RJ45 connection for management, and one 100BT RJ45 connection for console access by technical support. To support IP bonding for the management interface, one additional 1 GbE RJ45 Ethernet port is required. Each Replication Engine that uses iSCSI connectivity to a primary or secondary Pillar Axiom system requires five Ethernet connections: Four 1 GbE RJ45 connections for management and replication data flow, and one 100BT RJ45 connection for console access by Customer Support. IP bonding is not available for iSCSI-connected Replication Engines.
Power	Each Replication Engine requires two IEC320 C13 or IEC 60320 C13 power connectors with C14 receptacles. Refer to the *Pillar Axiom MaxRep Replication for SAN Hardware Guide* for specific power requirements.
Rack space	Each Replication Engine has a standard 2U form factor.
Browser	Access to the management interface of the Replication Engine is provided through a standard Internet browser. Browser requirements include: • Microsoft Internet Explorer 5.5 or later • Mozilla Firefox 1.5 or later • Screen resolution of 1024 x 768 pixels • Adobe Flash Player 10 or later
Environment	Connectivity between sites for synchronous replication must include an extension of the local SAN fabric to the remote site using dense wavelength division multiplexing (DWDM) over dark fibre, which is the network system that consists of fibre optic cables between the primary and secondary locations. Sufficient bandwidth must be available to accommodate the change rate of the source data as well as the target Pillar Axiom system writes and journaling. Connectivity between sites for remote asynchronous replication must include sufficient WAN bandwidth to accommodate the change rate of the source data.

About Replication Configurations

Pillar Axiom MaxRep Replication for SAN supports three basic types of replication configurations: synchronous, asynchronous, and multi-hop.

Separate licenses are available for synchronous and asynchronous replication. Because multi-hop replication combines synchronous and asynchronous replication, both synchronous and asynchronous licenses are required for multi-hop configurations.

Related concepts

- *About Synchronous Replication*
- *About Asynchronous Replication*
- *About Multi-Hop Replication*
- *About Capacity Based Licenses*
- *About Licensing Optional Premium Features*

About Synchronous Replication

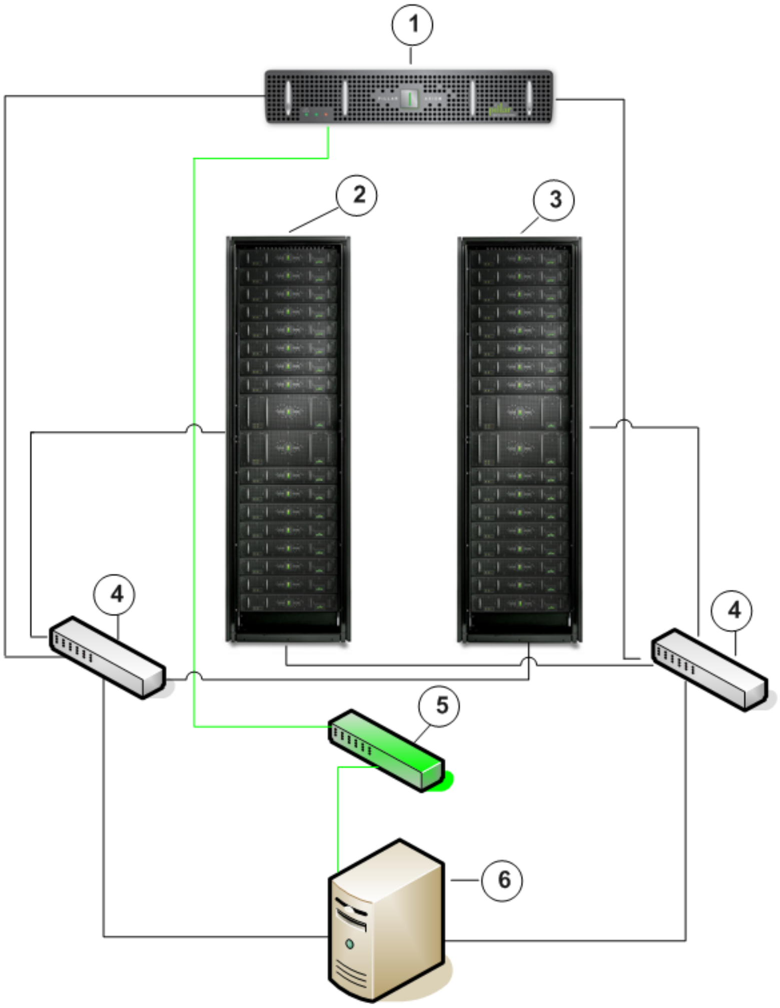
Synchronous replication involves saving data simultaneously in primary storage and in secondary storage, usually at the same location, within a 100 kilometer radius in the same metropolitan area, or within a limited radius. Synchronous replication can be configured for standard or high availability requirements.

Synchronous replication requires at least one Pillar Axiom Replication Engine and is supported when the source and target LUNs are attached to the same SAN network. Replication may also be synchronous when the source and target LUNs are located in two data centers connected by an extended SAN fabric that uses dense wavelength division multiplexing (DWDM) over dark fibre, which is the network system that consists of fibre optic cables between the primary and secondary locations. Whenever you write data to primary storage, the data is simultaneously replicated to secondary storage.

For example, a typical synchronous replication configuration consists of a single Pillar Axiom Replication Engine and two Pillar Axiom systems located in the same SAN fabric.

When data from the application host is stored on the primary Pillar Axiom system, a copy of the data is synchronously replicated on the secondary Pillar Axiom system.

Figure 4 Basic configuration for synchronous replication



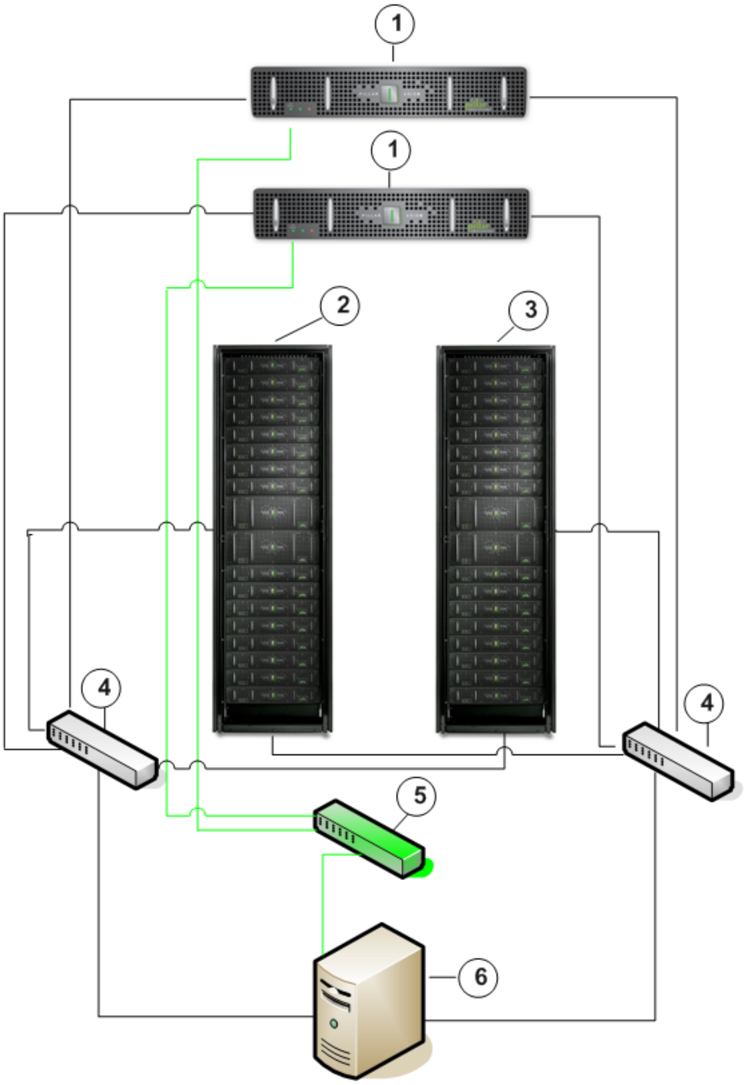
Legend

1 Replication Engine	5 Ethernet switch
2 Primary Pillar Axiom system	6 Application host
3 Secondary Pillar Axiom system	— Ethernet
4 Fibre Channel switch	— SAN fabric

Another example of a synchronous replication configuration includes adding a Replication Engine for high availability requirements. The two Replication Engines are clustered together to provide high availability. 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.

A High availability configuration for synchronous replication consists of a cluster of two Replication Engines and two Pillar Axiom systems, both on the same SAN fabric.

Figure 5 High availability configuration for synchronous replication



Legend

1 Replication Engine	5 Ethernet switch
2 Primary Pillar Axiom system	6 Application host
3 Secondary Pillar Axiom system	— Ethernet
4 Fibre Channel switch	— SAN fabric

Related concepts

- *About Replication Configurations*
- *About Pillar Axiom MaxRep Replication for SAN Components*

About Asynchronous Replication

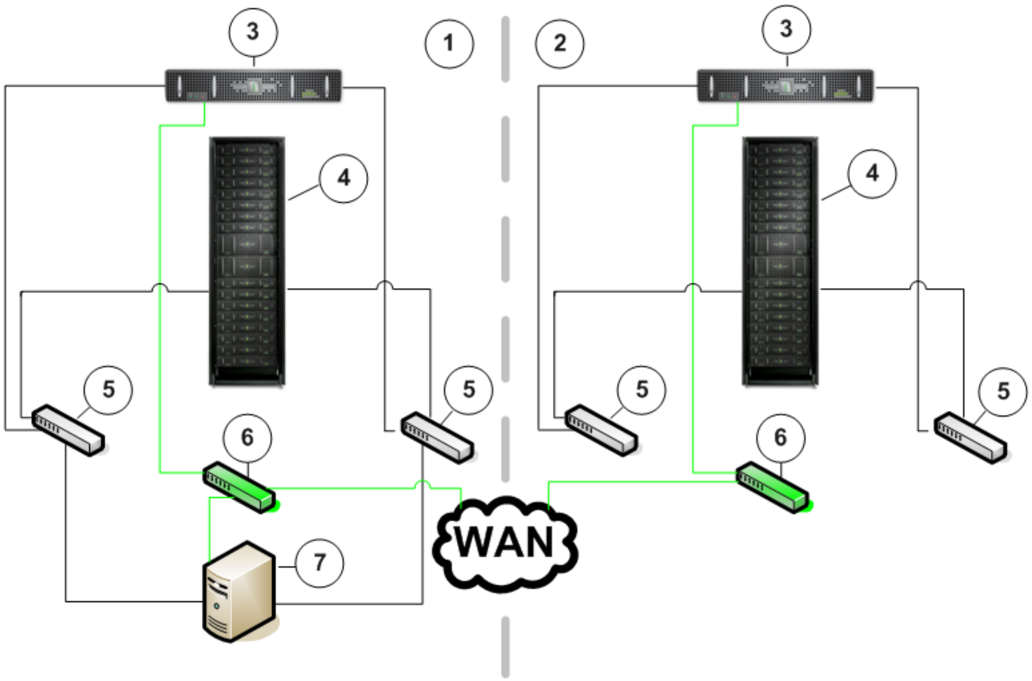
Asynchronous replication provides a time-lagged copy of data that is written to a secondary storage site, usually located remotely from the primary storage site.

Asynchronous replication requires at least two Pillar Axiom Replication Engines and is supported in most cases 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. Whenever you write data 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 a Pillar Axiom Replication Engine and a Pillar Axiom system.

When data from the application host is stored on the primary Pillar Axiom system, a copy of the data, along with any necessary journal information, is prepared for transfer to the Pillar Axiom system on the secondary site. The two Replication Engines manage the flow of data between the two Pillar Axiom systems.

Figure 6 Basic configuration for asynchronous replication



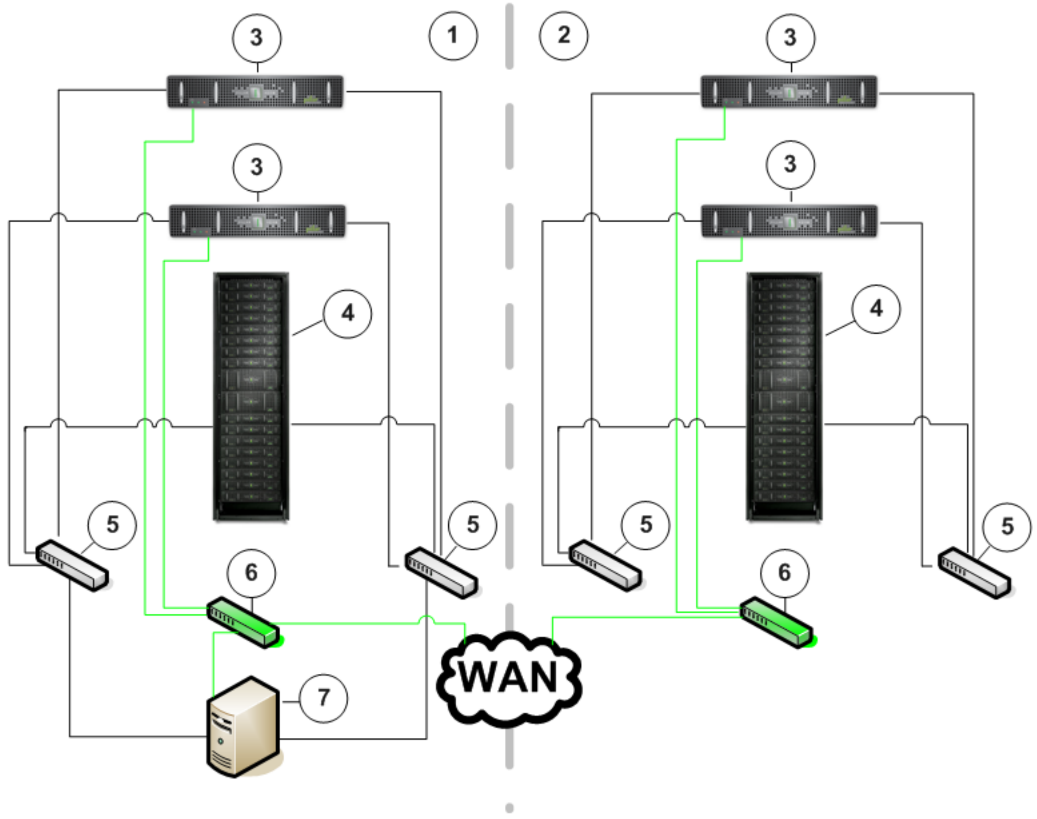
Legend

1 Primary site	6 Ethernet switch
2 Secondary site	7 Application host
3 Replication Engine	— Ethernet
4 Pillar Axiom system	— SAN fabric
5 Fibre Channel switch	

Another example of an asynchronous replication includes adding a Replication Engine to the primary and secondary sites for high availability requirements. The two Replication Engines are clustered together to provide high availability. One of the Replication Engines in each clustered pair is in active mode. The other Replication Engine is in passive mode, ready to take over if the active Replication Engine should fail.

A high availability configuration for asynchronous replication consists of a cluster of two Replication Engines and the primary Pillar Axiom system on the primary site. The secondary site contains a cluster of two Replication Engines and the secondary Pillar Axiom system.

Figure 7 High availability configuration for asynchronous replication



Legend

1 Primary site	6 Ethernet switch
2 Secondary site	7 Application host
3 Replication Engine	— Ethernet
4 Pillar Axiom system	— SAN fabric
5 Fibre Channel switch	

Related concepts

- *About Replication Configurations*
- *About Pillar Axiom MaxRep Replication for SAN Components*

About 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.

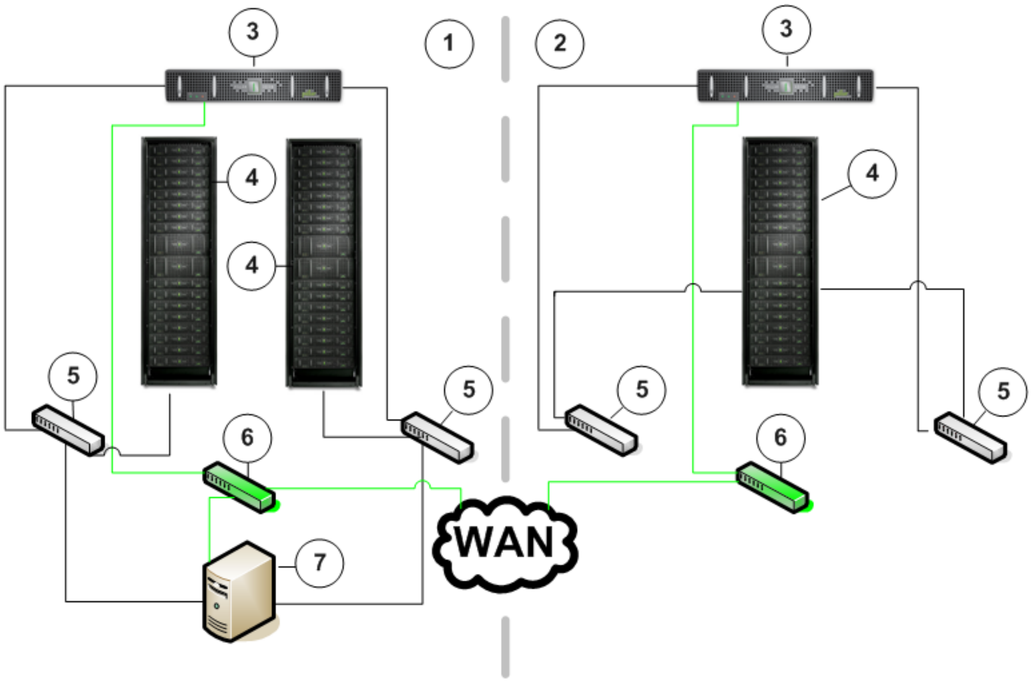
Multi-hop replication requires both a synchronous and an asynchronous capacity-based license. The first synchronous hop of replication occurs between two Pillar Axiom systems that are connected to the same SAN fabrics either at the same physical location, or between sites where the SAN fabrics are extended using DWDM over dark fibre. The second hop of replication is asynchronous from the target Pillar Axiom system of the first synchronous hop to a remote location connected via WAN.

For example, a typical multi-hop replication configuration consists of a Pillar Axiom Replication Engine and two Pillar Axiom systems set up in a synchronous replication relationship at the primary site. In addition, another Replication Engine and Pillar Axiom system at the secondary site are set up in an asynchronous replication relationship with the secondary Pillar Axiom system on the primary site.

When data from the application host is stored on the primary Pillar Axiom system on the primary site, the Replication Engine replicates any data changes to the secondary Pillar Axiom 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 the data and meta data is sent to the Pillar Axiom system located at the secondary site.

Figure 8 Typical multi-hop replication configuration



Legend

1 Primary site	6 Ethernet switch
2 Secondary site	7 Application host
3 Replication Engine	— Ethernet
4 Pillar Axiom system	— Fibre Channel (FC)
5 Fibre Channel switch	

Related concepts

- *About Replication Configurations*
- *About Pillar Axiom MaxRep Replication for SAN Components*

CHAPTER 2

Configure Pillar Axiom Systems and Servers

About Pillar Axiom System and Server Configuration

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

Initially, you need to configure the source and target LUNs for your replication pairs on your Pillar Axiom systems, and, if you are using application consistency, install the MaxRep agent on your application servers.

Create a Pillar Axiom Administrator Account

You can create new administrator accounts to allow users to perform various tasks on the Pillar Axiom system.

1 From the Pillar Axiom Storage Services Manager **Configure** tab, click **Global Settings** > **Administrator Accounts**.

2 Click **Actions** > **Create Account**.

3 Enter the name of the account in the **Login Name** field.

4 Choose a role from the **Role** drop-down 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.

   Required information:

   - **Full Name**
   - **Email Address**
   - **Phone Number**
   - **Password**

- Confirm Password

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

7 To save your changes, click OK.

Related concepts

- *About Pillar Axiom MaxRep Administrator Accounts*

Related tasks

- *Create a Source LUN*
- *Create a Target LUN*
- *Create a New MaxRep Account*

About the MaxRep Agents

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

Application consistent replication is available through the MaxRep agents. Pillar Axiom MaxRep ships with the MaxRep agent from the original equipment manufacturer (OEM). If you require additional information or a MaxRep agent software package for a specific operating system, please contact your account representative.

Pillar Axiom MaxRep systems 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 RHEL5-U5
Microsoft Exchange	Exchange 2007 Exchange 2007 SP1 Exchange 2007 SP2 Exchange 2007 SP3 Exchange 2010 Exchange 2010 SP1	Windows 2003 Windows 2003 SP2 Windows 2008 Windows 2008 R2 Windows 2008 R2 SP1
Microsoft SQL server	SQL 2005 SQL 2005 SP1	Windows 2003 Windows 2003 SP2

Table 4 Supported agents for standalone applications (continued)

Application consistency	Application	Operating system
	SQL 2005 SP2 SQL 2005 SP3 SQL 2005 SP4 SQL 2008 SQL 2008 SP1 SQL 2008 SP2 SQL 2008 SP3 SQL 2008 R2 SQL 2008 R2 SP1 SQL 2008 R2 SQ2	Windows 2008 Windows 2008 R2 Windows 2008 R2 SP1
Fileserver	not applicable	Windows 2003 Windows 2003 SP2 Windows 2008 Windows 2008 R2 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 RHEL5-U5
Microsoft Exchange	Exchange 2007 Exchange 2007 SP1 Exchange 2007 SP2 Exchange 2007 SP3 Exchange 2010 Exchange 2010 SP1	Windows 2008 Cluster Windows 2008 R2 Cluster Windows 2008 R2 Cluster SP1
SQL	SQL 2005 SQL 2005 SP1 SQL 2005 SP2 SQL 2005 SP3 SQL 2005 SP4 SQL 2008 SQL 2008 SP1 SQL 2008 SP2 SQL 2008 SP3 SQL 2008 R2	Windows 2008 Cluster Windows 2008 R2 Cluster Windows 2008 R2 Cluster SP1

Table 5 Supported agents for clustered applications (continued)

Application consistency	Application	Operating system
	SQL 2008 R2 SP1 SQL 2008 R2 SQ2	
Fileserver	not applicable	Windows 2008 Cluster Windows 2008 R2 Cluster Windows 2008 R2 Cluster SP1

Pillar Axiom MaxRep Replication for SAN also supports the InMage Unified Agent (for both Windows and Linux) and vContinuum for VMware. For vContinuum, the following table summarizes the platforms that are supported:

Table 6 Supported platforms for vContinuum

Component	Version
vSphere (ESX)	ESX3.5 ESXi 3.5 ESX 3.5 U2 ESXi 3.5 U2 ESX 4.0 ESXi 4.0 ESXi 4.1 ESX 4.1 Support between same versions only.
Guest VMs	Windows 2003 Windows 2008 Windows 2008 R2 SLES CentOS RHEL Debian (Etch 4) Ubuntu8
Management Console with vContinuum wizard	Windows XP, Vista, 7 (32 and 64 bit) Windows Server 2003 + SP (32 and 64 bit) Windows Server 2008 + SP (32 and 64 bit) Windows Server 2008 R2 (64 bit)
Master Target	Windows 2008 R2 (recommended) Windows 2003 Windows 2008,

Table 6 Supported platforms for vContinuum (continued)

Component	Version
VMware CLI	vSphere CLI 4.0 U1 vSphere CLI 4.0 vSphere CLI 3.5.2 Update 2

Related references

- *MaxRep Agent Settings*
- *Agent Heartbeat Monitoring*

Related tasks

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

MaxRep Agent Settings

Allows you to configure the Pillar Axiom Replication Engine agents.

To view the agent settings from the Pillar Axiom MaxRep Replication for SAN graphical user interface (GUI), navigate to Settings > Settings > Agent Settings.

Agent Settings

Server
Indicates the primary and secondary Pillar Axiom systems.

Agent Type
Indicates the type of agent installed on the Axiom 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 tasks

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

About 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 Pillar Axiom system.
- A new LUN set up as the source for a replication pair.

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

Note: As part of the replication pair creation, Pillar Axiom MaxRep Replication for SAN automatically creates the following items:

- All necessary host associations in the Pillar Axiom system.
- Mappings to the Pillar Axiom Replication Engines for the source and target LUNs.

During replication pair creation, Pillar Axiom MaxRep Replication 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.

Related concepts

- *About LUN Management*
- *About Protection Plans*

Related references

- *LUN Protection Monitoring*

Related tasks

- *Create a Pillar Axiom Administrator Account*
- *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 primary Pillar Axiom system.

1 Start the Pillar Axiom Storage Services Manager on the Pillar Axiom system that will be the primary system for the replication pair.

2 Follow the instructions for creating a LUN in the *Pillar Axiom Administrator's Guide*.

Related concepts

- *About Source and Target LUNs*

Related tasks

- *Create a Pillar Axiom Administrator Account*

Create a Target LUN

When creating a replication pair, create the target LUN if the LUN does not already exist on the secondary Pillar Axiom 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 LUN and increase the allocated and addressable logical capacities by 1 GB.

1 Start the Pillar Axiom Storage Services Manager on the Pillar Axiom system that will be the secondary system for the replication pair.

2 Follow the instructions for creating a LUN in the *Pillar Axiom Administrator's Guide*.

Related concepts

- *About Source and Target LUNs*

Related tasks

- *Create a Pillar Axiom Administrator Account*

About LUN Management

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

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

Map
Select this option to map retention and home LUNs of the registered Pillar Axiom system to the Replication Engine.

Unmap
Select this option to remove the mapping configuration between the registered Pillar Axiom 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
Select this option after you have resized a LUN associated with a replication pair. The following options are available to detect LUN resize:

- Detect Target LUN resize
- Detect Source LUN resize

iSCSI Login
Select this option to initiate an iSCSI session with the Pillar Axiom system target iSCSI ports.

Related concepts

- *About Source and Target LUNs*

Related references

- *LUN Protection Monitoring*

Related tasks

- *Detect Resizing of the Home and Retention LUNs*
- *Detect Resizing of a Source LUN*
- *Detect Resizing of a Target LUN*
- *Map LUNs*
- *Unmap LUNs*

Map LUNs

To make the replication LUNs on the registered Pillar Axiom system available, map the LUNs from the Pillar Axiom MaxRep Replication for SAN to the Pillar Axiom system. This option is used to map retention and home LUNs.

Before you map a LUN, you should consider the following points:

- When mapping a LUN, the Pillar Axiom system deletes any existing host mappings for that LUN.
- Mapped LUNs will not be automatically mounted across restarts of the Pillar Axiom system.
- Only *ext3 filesystem* formatting is permitted. The ext3 filesystem is a journaled file system commonly used by Linux kernels.
- A LUN is always mapped to an appliance initiator (AI) for the target port group. The AI port group is used to access the home, retention, and backup LUNs that are mounted on the Pillar Axiom Replication Engine.

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

1. Navigate to Settings > Axioms > Toolkit for MaxRep.
2. In the Select MaxRep Option page, select Map and click Next.
3. From the Select Axiom drop-down list, choose the Pillar Axiom system containing the LUN you want to map from the Select Axiom drop-down list.
4. Expand the entry for the Pillar Axiom system containing the LUN.
5. Select the LUNs to be mapped and click Next.
6. Review and make needed changes to the LUN scan options.

   In the LUN Scan Options table, you can change the names of the following objects:

   - LUN Name
   - Host Name
   - Mount Point
   - File System
7. Provide the Mount Point.
   - If the LUN is already formatted, deselect the option Format Required.
   - If the LUN requires formatting, select Format Required.
8. To initiate the mapping, click Submit.

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

Related concepts

- *About LUN Management*
- *About Source and Target LUNs*
- *About FC Initiator and Target Ports*

Related tasks

- *Unmap LUNs*

Unmap LUNs

When a LUN mapping between the Pillar Axiom system and the Pillar Axiom Replication Engine is no longer needed, use the Unmap LUNs option to remove it.

Any LUNs mapped to Pillar Axiom MaxRep Replication for SAN without using the Toolkit For MaxRep will not be listed by the Toolkit either for resize or for unmap. If those LUNs are used as part of a protection plan (as source, target, or retention), they will be listed in the page for the Detect Resize option, but not in the page for the Unmap option. Pillar Axiom MaxRep does not allow any LUN to be unmapped using the Toolkit if the LUN is used as part of a protection plan. An exception is for the Replication Engine cache home LUN; it will be listed for resize purposes only, and not for unmap purposes.

1. Navigate to Settings > Axioms > Toolkit for MaxRep.
2. In the Select MaxRep Option page, select Unmap and click Next.
3. From the Select Axiom drop-down list, choose the Pillar Axiom system containing the LUN you want to map.
4. Expand the entry for the Pillar Axiom system containing the LUN.
5. To initiate the unmapping operation, select the LUN or LUNs to be unmapped, and click Next.
6. Click Submit.

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

Related concepts

- *About LUN Management*
- *About Source and Target LUNs*

Related tasks

- *Map LUNs*

Detect Resizing of the Home and Retention LUNs

Pillar Axiom MaxRep Replication 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** > **Axioms** > **Toolkit for MaxRep**.
2. In the Select MaxRep Option page, select **Detect Resize** and click **Next**.
3. From the **Select Axiom** drop-down list, choose the Pillar Axiom system that contains the LUN that was resized.
4. Expand the entry for the Pillar Axiom system containing the LUN.
5. Select the LUNs to be detected and click **Next**.
6. In the Select LUN Scan Options table, review the LUNs to be scanned.

   Note: The Select LUN Scan Options table only lists the home and retention LUNs that are used in replication pairs.
7. To initiate the scanning for LUN capacity changes, click **Submit**.

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

Related concepts

- *About LUN Management*

Detect Resizing of a Source LUN

Pillar Axiom MaxRep Replication for SAN allows you to scan the source LUNs for capacity changes and reflect those changes in the protection plans.

1. Navigate to **Settings** > **Axioms** > **Toolkit for MaxRep**.
2. In the Select MaxRep Option page, select **Detect Resize** and click **Next**.

3. Choose the Pillar Axiom system containing the LUN for which you want to detect resizing from the Select Axiom drop-down list.
4. Expand the entry for the Pillar Axiom system containing the LUN.
5. Select the source LUNs to be detected and click Next.
6. In the Select LUN Scan Options table, review the source LUNs to be scanned.

   Note: The Select LUN Scan Options table only lists the source LUNs that are used in replication pairs.
7. To initiate the scanning for LUN capacity changes, click Submit.

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

Related concepts

- *About LUN Management*

Related tasks

- *Detect Resizing of a Target LUN*

Detect Resizing of a Target LUN

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

1. Navigate to Settings > Axioms > Toolkit for MaxRep.
2. In the Select MaxRep Option page, select Detect Resize and click Next.
3. Choose the Pillar Axiom system containing the LUN for which you want to detect resizing from the Select Axiom drop-down list.
4. Expand the entry for the Pillar Axiom system containing the LUN.
5. Select the target LUN to be detected and click Next.
6. In the Select LUN Scan Options table, review the target LUNs to be scanned.

   Note: The Select LUN Scan Options table only lists the target LUNs that are used in replication pairs.
7. To initiate the scanning for LUN capacity changes, click Submit.

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

Related concepts

- *About LUN Management*

Related tasks

- *Detect Resizing of a Source LUN*

Initiate a Pillar Axiom iSCSI Session

Use the iSCSI Login option when investigating iSCSI login problems to the Pillar Axiom system from the Pillar Axiom MaxRep Replication for SAN.

1. To perform the iSCSI Login operation, navigate to Settings > Axioms > Toolkit for MaxRep.
2. In the Select MaxRep Option page, select iSCSI Login and click Next.
3. In the Select an Axiom page, select a Pillar Axiom system from those listed.
4. Click Submit to initiate the login operation.
5. At the confirmation prompt, click OK.

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

Related concepts

- *About iSCSI Initiator and Target Ports*

CHAPTER 3

Configure Pillar Axiom MaxRep Replication for SAN

Pillar Axiom MaxRep Replication for SAN allows you to configure the Pillar Axiom Replication Engine and specific Pillar Axiom system settings that are relevant to replication.

The available Replication Engine settings that you can configure include:

- Register and manage the Pillar Axiom systems.
- Add and delete Replication Engine users.
- Configure settings.
- Manage and apply Replication Engine licenses.
- View data logs.
- Configure ports.
- Configure process service failover.

About Initial Configuration

Before you can use Pillar Axiom MaxRep Replication for SAN, you will need to configure the Pillar Axiom MaxRep software on your Pillar Axiom Replication Engines.

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

Note: Oracle consulting services installs the Pillar Axiom MaxRep Replication for SAN software.

Initial configuration of Pillar Axiom MaxRep Replication for SAN includes these tasks:

- Set up user accounts.
- Install the Pillar Axiom MaxRep Replication for SAN license on your control service Replication Engine.
- Configure the Replication Engine HBA ports.

- Register your Pillar Axiom systems.
- Configure the Replication Engine settings.
- Configure any remote Replication Engines, if installed.

Related concepts

- *About Pillar Axiom MaxRep Administrator Accounts*
- *About Capacity Based Licenses*
- *About FC Initiator and Target Ports*
- *About iSCSI Initiator and Target Ports*
- *About Pillar Axiom System Registration*
- *About Pillar Axiom Replication Engine Settings*
- *About Remote Replication Engine Configuration*

About Pillar Axiom MaxRep Administrator Accounts

The Pillar Axiom MaxRep Replication 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 Pillar Axiom MaxRep Replication 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 Pillar Axiom 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 tasks

- *Create a New MaxRep Account*
- *Create a Pillar Axiom Administrator Account*
- *Log In to a Pillar Axiom Replication Engine*

Create a New MaxRep Account

You can create new administrator or monitor user accounts for the Pillar Axiom MaxRep Replication for SAN system.

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

Note: For security reasons, we recommend that you create a separate account for each administrator of the Pillar Axiom MaxRep system. Then you can grant the appropriate administrator access rights to each user. We do not recommend the practice of sharing login credentials, or of having all administrators log in to the default admin user account.

1. Choose Settings > Manage Users.
2. Click Add User.
3. Add a full name and username for the administrator.

A UID (unique ID) is automatically generated for the user account.

4 (Optional) To allow this user administrator privileges, select Admin Access.

Note: The Administrator role provides the user full access to all Pillar Axiom MaxRep functions. Users with the Monitor roles have limited access.

5 To authenticate the user, select Local database.

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

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

7 Enter an email address for the user.

This is the email address that will be used to deliver email alerts to this user.

8 Click Save.

Related concepts

- *About Pillar Axiom MaxRep Administrator Accounts*

Related tasks

- *Edit a User Account*
- *Delete a User Account*

Log In to a Pillar Axiom Replication Engine

To use the Pillar Axiom MaxRep Replication for SAN software, you must first log in to a Pillar Axiom Replication Engine.

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

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 concepts

- *About Pillar Axiom MaxRep Administrator Accounts*

Related tasks

- *Edit a User Account*
- *Delete a User Account*
- *Log In to a Pillar Axiom Replication Engine*

Edit a User Account

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

The administrator role has the following restrictions:

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

The user account settings that were originally entered in the New User page when adding a new user can be changed in the User Configuration page. In addition, the Trap Listeners, Alert Notification, Email Subject, and Replication Engine Auto Timeout default settings are assigned automatically when adding a new user, and can only be changed on the User Configuration page.

1 Choose Settings > Manage Users.

   Result:
   All user accounts on this Replication Engine are listed in the Configured System Users table.

2 Click Edit in the Edit column next to the user account you want to edit.

   Result:
   Configuration details for the selected user account are listed on the User Configuration page.

3 To update user settings for this user account, enter new values in the New Values column of the Update User Settings table and click Save.

4 To delete an SNMP trap listener, select the listener in the Configured Trap Listeners table and click Delete.

5 To add the Pillar Axiom system as an SNMP trap listener, specify the Axiom system in the Add Trap Listener table and click Add.

6 (Administrator role only) To add the Pillar Axiom system as an SNMP trap listener, in the Add Trap Listener table, enter the IP address or host name

of the Axiom system where the trap is installed and its port number (the default is port 162), and click **Add**.

Required fields:

- IP address or network name of the system where the trap is defined.
- Port number to which the Replication Engine should connect. The default port number is 162.

Note: Setting up the Axiom system as the SNMP trap allows events to be transmitted to Oracle Pillar Customer Support.

7 Select the default method of notification.

Valid choices:

- **Email**: Make sure that you enter a valid email address when selecting this option.
- **Trap**: Make sure that you enter the valid SNMP information when selecting this option.

8 Select the alerts from the **Alert Notification** table and click **Save**.

9 To test the email address configured for alert notifications, click **Test Mail**.

10 To change the default subject of alert email messages, enter a new value in the **Email Subject** table and click **Save**.

11 To change the default period of inactivity after which this user will be automatically logged out of the Replication Engine, change the value in the **Replication Engine Auto Timeout** table and click **Save**.

Related tasks

- *Delete a User Account*
- *Create a New MaxRep 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 Choose **Settings** > **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 tasks

- *Edit a User Account*
- *Create a New MaxRep Account*

About Capacity Based Licenses

You need to license Pillar Axiom MaxRep Replication for SAN on your primary Pillar Axiom Replication Engine before you can configure and use the Pillar Axiom MaxRep software. The primary Replication Engine is the Replication Engine on which the control service runs. The control service Replication Engine becomes a License Server for other Replication Engines.

Synchronous and asynchronous replication licenses with or without application protection are available for Pillar Axiom MaxRep Replication for SAN. Licenses that do not include application protection are limited to 30 days of retention, but licenses that include application protection have unlimited retention. Available licenses include:

- Synchronous data protection (30-day retention limit)
- Asynchronous data protection (30-day retention limit)
- Synchronous data protection with application consistency
- Asynchronous data protection with application consistency

In addition to enabling the type of replication you will use, 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 Pillar Axiom MaxRep Replication for SAN comes pre-installed on your Replication Engine. In case you need to reinstall or upgrade, instructions for uploading and applying licenses are provided in the following sections.

Contact your account representative to obtain additional licenses.

Related tasks

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

About Licensing Optional Premium Features

All features on the Pillar Axiom 600 storage system are enabled out of the factory. Administrators should ensure they are in compliance with their End User License Agreements and have purchased the necessary licenses for Optional Premium features.

The following features are currently licensed on the Pillar Axiom Replication Engine:

- Pillar Axiom MaxRep Asynchronous Replication - Terabyte Perpetual
- Pillar Axiom MaxRep Asynchronous Replication with Application Protection - Terabyte Perpetual
- Pillar Axiom MaxRep Synchronous Replication - Terabyte Perpetual
- Pillar Axiom MaxRep Synchronous Replication with Application Protection - Terabyte Perpetual

Related concepts

- *About Capacity Based Licenses*

Upload Your Capacity-Based License

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

Note: The first time you log in to Pillar Axiom MaxRep Replication for SAN, the following message displays:

```
This Replication Engine Server is not yet licensed. Navigate
to the License Management page to upload a license.
```

When you receive your license file, copy it to your local workstation and start the Pillar Axiom MaxRep Replication for SAN software on your primary Replication Engine.

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

1. Choose **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 concepts

- *About Capacity Based Licenses*

Related tasks

- *Apply Your License*

Apply Your License

After you have uploaded your license, you can apply it to your primary Pillar Axiom Replication Engine, and to other process service Replication Engines or hosts.

Use the Pillar Axiom MaxRep Replication for SAN software to apply your license.

1 Choose Settings > Settings > License Management.

2 Click the Apply License tab.

3 In the Unlicensed Hosts table, select the server (Replication Engine or host) to which 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 type of license (Replication Engine or host-based agent) and click Apply.

   Result:
   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.

Related concepts

- *About Capacity Based Licenses*

Related tasks

- *Upload Your Capacity-Based License*

About FC Initiator and Target Ports

Before you can create replication pairs, you need to verify that all of the Fibre Channel (FC) ports in the Pillar Axiom Replication Engine are recognized as initiator ports. After this verification, you can convert the appropriate ports to target ports.

The Replication Engine requires three types of host bus adapter (HBA) ports.

Initiator Ports (AIS)

The default configuration for a port on a Replication Engine is an initiator port. An initiator port communicates only with zoned target ports within the SAN fabric. Initiator ports must be zoned to all Slammer ports of all Pillar Axiom 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 initiator for target LUN mapping port communicates only with zoned target ports within the SAN fabric. Zone the AIT port to all Slammer ports of all Pillar Axiom systems that are registered to the Replication Engine.

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, backup and retention LUNs on the Pillar Axiom system.
- Write operations to a source LUN during a data recovery.

Target Ports (AT)

A target port communicates only with zoned initiator ports within the SAN fabric. The zoned initiator ports include the following:

- All Slammer ports from the Pillar Axiom systems that are registered to the Replication Engine.
- Any hosts that mount virtual snapshots 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 Slammer of the primary Pillar Axiom system.
- After a virtual snapshot is exported to a host, the host accesses the virtual snapshot through the AT port.

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

Related concepts

- *About How Pillar Axiom MaxRep Replication for SAN Works*

Related references

- *Supported FC Port Configurations*
- *Supported Fabric Zoning*

Related tasks

- *Verify All FC Ports Discovered as Initiator Ports*

Verify All FC Ports Discovered as Initiator Ports

During the initial installation, all Fibre Channel (FC) ports on the Pillar Axiom Replication Engine are automatically configured to be initiator ports. You need to verify that all HBA ports on the Replication Engine have been discovered and are configured as initiator ports.

1 Choose **Settings** > **Advanced Configuration** > **Replication Engine Ports Configuration.**

2 Expand the entry for the Replication Engine you are configuring.

3 Verify that all FC ports on the Replication Engine appear in the Initiator Ports table.

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

Related concepts

- *About FC Initiator and Target Ports*

Related tasks

- *Convert FC Ports to Target Ports*

Convert FC Ports to Target Ports

After you have verified that all of the Fibre Channel (FC) initiator ports have been recognized by the Pillar Axiom Replication Engine, you can choose one or more of these ports to serve as target ports.

1 Choose **Settings** > **Advanced Configuration** > **Replication Engine Ports Configuration.**

2 Expand the entry for the Replication Engine you are configuring.

3 Click **Convert Ports.**

   Result:
   The **Convert Initiator/Target Ports** menu is displayed.

4 Select one or more ports from the **Initiator Ports** list to convert to target ports.

   Note: Verify that the available port configurations are supported.

5 Click the move button (**>**) to transfer the selected ports to the **Target Ports** list.

6 Click **Done.**

Note: It may take several minutes for this operation to complete. While the ports are being converted to target ports, the port state is listed as `Transient Pending`.

Related concepts

- *About FC Initiator and Target Ports*

Related references

- *Supported FC Port Configurations*

Related tasks

- *Verify All FC Ports Discovered as Initiator Ports*

Convert FC Initiator Ports to LUN Mapping Ports

Choose one or more Fibre Channel (FC) ports to serve as initiator ports for target LUN mapping.

1. Choose Settings > Advanced Configuration > Replication Engine Ports Configuration.
2. Expand the entry for the Pillar Axiom Replication Engine you are configuring.
3. Click Create Group.

   Result:
   The system displays the Create Group for Target LUN Mapping menu.
4. Select one or more ports from the Initiator Ports list to convert to a target LUN mapping port.

   Note: Verify that the available port configurations are supported.
5. Click the move button (>) to transfer the selected ports to the Target LUN Mapping Ports list.
6. Click Done.

Related concepts

- *About FC Initiator and Target Ports*

Related references

- *Supported FC Port Configurations*

Related tasks

- *Convert FC Ports to Target Ports*

Supported FC Port Configurations

Each Pillar Axiom Replication Engine includes two host bus adapters (HBAs); each HBA has four ports. Supported port configurations vary depending on whether the Replication Engine is associated with the source LUNs or the target LUNs in the replication pairs.

Configure the Fibre Channel (FC) ports on each HBA as specified in the following tables.

Table 7 Recommended port configuration for source Replication Engines

Port number	Configuration
1	Initiator port (AIS)
2	Initiator for target LUN mapping port (AIT)
3	Target port (AT)
4	Target port (AT)

Table 8 Recommended port configuration for target Replication Engines

Port number	Configuration
1	Initiator port (AIS)
2	Initiator for target LUN mapping port (AIT)
3	Initiator for target LUN mapping port (AIT)
4	Target port (AT)

Related concepts

- *About FC Initiator and Target Ports*

Related tasks

- *Verify All FC Ports Discovered as Initiator Ports*

Supported Fabric Zoning

Each Pillar Axiom Replication Engine is shipped with two host bus adapters (HBAs). We recommend using a separate storage area network (SAN) fabric for each HBA.

The following recommendations apply:

- The supported SAN fabric zoning includes zoning each HBA port to the Pillar Axiom Slammer ports.
- Supported configurations include connecting all ports from the first HBA to one SAN fabric, and all ports from the second HBA connected to a separate SAN fabric.

Table 9 is an example of the supported zoning for a source Replication Engine configured with two target ports for each HBA. Each HBA is connected to a separate fabric: HBA1 is connected to Fabric A, and HBA2 is connected to Fabric B.

Table 9 Example recommended zoning

Fabric A	Fabric B
CSMAXREP01_HBA1_AIS_PORT1 Axiom01_CU0P0	CSMAXREP01_HBA2_AIS_PORT1 Axiom01_CU0P1
CSMAXREP01_HBA1_AIS_PORT1 Axiom01_CU1P0	CSMAXREP01_HBA2_AIS_PORT1 Axiom01_CU1P1
CSMAXREP01_HBA1_AIT_PORT2 Axiom01_CU0P0	CSMAXREP01_HBA2_AIT_PORT2 Axiom01_CU0P1
CSMAXREP01_HBA1_AIT_PORT2 Axiom01_CU1P0	CSMAXREP01_HBA2_AIT_PORT2 Axiom01_CU1P1
CSMAXREP01_HBA1_AT_PORT3 Axiom01_CU0P0	CSMAXREP01_HBA2_AT_PORT3 Axiom01_CU0P1
CSMAXREP01_HBA1_AT_PORT3 Axiom01_CU1P0	CSMAXREP01_HBA2_AT_PORT3 Axiom01_CU1P1
CSMAXREP01_HBA1_AT_PORT4 Axiom01_CU0P0	CSMAXREP01_HBA2_AT_PORT4 Axiom01_CU0P1
CSMAXREP01_HBA1_AT_PORT4 Axiom01_CU1P0	CSMAXREP01_HBA2_AT_PORT4 Axiom01_CU1P1

Each element in the path definition in Table 9 is defined in Table 10.

Table 10 Path definition key

Path element	Description
Replication Engine name	Example: CSMAXREP01
HBA name	Valid choices: • HBA1 • HBA2
Port configuration	Valid choices: • AIS (appliance initiator for source) • AIT (appliance initiator for target LUN mapping) • AT (appliance target)
Replication Engine HBA port number	Valid choices: • PORT1 • PORT2 • PORT3 • PORT4
Pillar Axiom system name	Example: Axiom01
Pillar Axiom Slammer control unit number and port number	Valid choices: • CU0P0 (control unit 0, port 0) • CU1P0 (control unit 1, port 0) • CU0P1 (control unit 0, port 1) • CU1P1 (control unit 1, port 1)

Related concepts

- *About FC Initiator and Target Ports*

Related tasks

- *Verify All FC Ports Discovered as Initiator Ports*

About iSCSI Initiator and Target Ports

Before you can create and use the replication pairs, verify that the Pillar Axiom Replication Engine iSCSI ports have been created. After creating the ports, convert them to target ports or an initiator for target LUN mapping ports, as needed.

For iSCSI replication, Replication Engines require three types of iSCSI ports:

Initiator Ports (AIS)

The default configuration for a port on a Replication Engine is an initiator port. An initiator port communicates only with zoned target ports within the SAN fabric. Initiator ports must be zoned to all Slammer ports of all Pillar Axiom 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 initiator for target LUN mapping port communicates only with zoned target ports within the SAN fabric. Zone the AIT port to all Slammer ports of all Pillar Axiom systems that are registered to the Replication Engine.

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, backup and retention LUNs on the Pillar Axiom system.
- Write operations to a source LUN during a data recovery.

Target Ports (AT) A target port communicates only with zoned initiator ports within the SAN fabric. The zoned initiator ports include the following:

- All Slammer ports from the Pillar Axiom systems that are registered to the Replication Engine.
- Any hosts that mount virtual snapshots 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 Slammer of the primary Pillar Axiom system.
- After a virtual snapshot is exported to a host, the host accesses the virtual snapshot through the AT port.

Related references

- *Supported iSCSI Port Configurations*

Related tasks

- *Verify iSCSI IP Addresses*
- *Configure iSCSI Target LUN Mapping Port*
- *Configure iSCSI Target Ports*

Verify iSCSI IP Addresses

During the initial Pillar Axiom MaxRep Replication for SAN installation, the system created four iSCSI Ethernet ports. Verify that these ports exist.

1. Choose Settings > Advanced Configuration > Replication Engine Ports Configuration.
2. Select the process service for the Pillar Axiom Replication Engine you are configuring.

3. Verify that all of the iSCSI ports on the Replication Engine appear in the Initiator Ports table as eth0, eth1, eth2, and eth3.

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

Related concepts

- *About iSCSI Initiator and Target Ports*

Related references

- *Supported iSCSI Port Configurations*

Configure iSCSI Target Ports

After you have verified that all of the iSCSI initiator ports have been recognized by the Pillar Axiom Replication Engine, you can choose one or more of these ports to serve as target ports.

1. Choose **Settings** > **Advanced Configuration** > **Replication Engine Ports Configuration**.
2. Select the process service for the Replication Engine you are configuring.
3. Click **Convert Ports**.

   Result:
   The system displays the **Convert Initiator/Target Ports** menu.
4. Select one or more ports from the **Initiator Ports** list to convert to target ports.

   Note: Verify that the available port configurations are supported.
5. Click the move button (**>**) to transfer the selected ports to the **Target Ports** list.
6. Click **Done**.

Note: It may take several minutes for this operation to complete. While the ports are being converted to target ports, the port state is listed as `Transient Pending`.

Related concepts

- *About iSCSI Initiator and Target Ports*

Related references

- *Supported iSCSI Port Configurations*

Configure iSCSI Target LUN Mapping Port

Choose one or more iSCSI ports to serve as target LUN mapping ports.

1 Choose **Settings** > **Advanced Configuration** > **Replication Engine Ports Configuration.**

2 Select the process service for the Pillar Axiom Replication Engine you are configuring.

3 Click **Create Group**.

Result:
The **Create Group for Target LUN Mapping** menu is displayed.

4 Select one or more ports from the **Initiator Ports** list to convert to a target LUN mapping port.

Note: Verify that the available port configurations are supported.

5 Click the move arrow (**>**) to transfer the selected ports to the **Target LUN Mapping Ports** list.

6 Click **Done**.

Related concepts

- *About iSCSI Initiator and Target Ports*

Related references

- *Supported iSCSI Port Configurations*

Supported iSCSI Port Configurations

Each Pillar Axiom Replication Engine has a total of four Ethernet ports that are configured for access by Pillar Axiom MaxRep Replication for SAN.

The four Ethernet ports consists of two 1GB Ethernet ports, and two additional 1GB Ethernet ports on a network interface card (NIC). Configure Ethernet port 0 (eth0) for system management using the graphical user interface (GUI) and managing the replicated data. Configure the remaining ports (eth1, eth2, and eth3) as iSCSI ports.

Configure the Replication Engine iSCSI ports on the NIC as specified in the following tables.

Table 11 Supported source iSCSI NIC port configuration

Port number	Configuration
eth1	Initiator port (AIS)
eth2	Initiator for target LUN mapping port (AIT)
eth3	Target port (AT)

Table 12 Supported target iSCSI NIC port configuration

Port number	Configuration
eth1	Initiator port (AIS)
eth2	Initiator for target LUN mapping port (AIT)
eth3	Target port (AT)

Related concepts

- *About iSCSI Initiator and Target Ports*

Related tasks

- *Configure iSCSI Target LUN Mapping Port*

About Pillar Axiom System Registration

Register your Pillar Axiom systems with a Pillar Axiom Replication Engine so that they can be used with the Pillar Axiom MaxRep Replication for SAN software.

Registering the Pilot IP addresses of your Pillar Axiom systems enables Pillar Axiom MaxRep to discover the Pillar Axiom systems so that replication pairs can be created.

Once a Pillar Axiom system has been registered, LUNs on that Axiom system can be used to configure replication pairs. You can view registered Axiom system details or histories, modify registered Axiom system addresses and credentials, and unregister previously registered Axiom systems.

Related references

- *View Axiom Systems*

Related tasks

- *Register the Pillar Axiom Systems*
- *Manage Registered Pillar Axiom Systems*

Register the Pillar Axiom Systems

Register each Pillar Axiom system you will be using for replication with the Pillar Axiom MaxRep Replication for SAN software.

Log in to the primary Pillar Axiom Replication Engine to begin Pillar Axiom system registration.

1. Choose Settings > Axiom > Register Axiom.
2. Enter the IP address of the Pillar Axiom system you want to register in the Axiom IP field.

   Use the IP address of the public interface to the Pillar Axiom Pilot.
3. In the Login and Password fields, enter the login credentials of a user with Administrator 2 or higher privileges for the Pillar Axiom system.
4. Click Next.
5. From the Process Service drop-down menu, select the IP address of the Replication Engine that will serve as the primary Replication Engine for this Pillar Axiom system.
6. Click Register.

Result:
In the Manage Axioms page, the Pillar Axiom system you just registered appears first in the Unregistered Axioms table as Pending. After the registration task completes, the Pillar Axiom system appears in the Registered Axioms table.

7 (Optional) Click Register New Axiom in the Unregistered Axioms table title bar to repeat the registration process for another Pillar Axiom system.

Related concepts

- *About Pillar Axiom System Registration*

Related references

- *View Axiom Systems*

Related tasks

- *Manage Registered Pillar Axiom Systems*

Manage Registered Pillar Axiom Systems

After registering the Pillar Axiom system with the Pillar Axiom Replication Engine, you can manage the Axiom system from the Pillar Axiom MaxRep Replication for SAN graphical user interface (GUI).

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

- Rediscover newly added LUNs.
- Modify the Pillar Axiom system IP address.
- Update login credentials.
- Review Pillar Axiom system information and details.
- Review activity history.

1 Choose Settings > Axioms > Manage Axioms.

2 In the Registered Axioms table title bar, choose one of the following:

  - View Axiom: Displays detailed information about the Pillar Axiom system you just registered in the Axiom LUN Explorer.
  - Force Delete Write Splits: Clears the write split for LUNs that are configured for protection. You need to provide your password, and to select the Axiom system and one or more LUNs for which you want to clear the write split.

Important! Use this option only if stale write splits have remained after a replication pair failure, and you need to clear the stale write splits to create a new protection plan. During normal operations, you do not need to delete write splits.

3 In the Action column of the Registered Axioms table, choose one of the following:

- Re-Discover: Discovers any LUNs that were created after the selected Pillar Axiom system was registered. Use the History action to confirm the Axiom discovery.
- Unregister: Removes the selected Pillar Axiom system from the Registered Axioms list.
- Modify: Changes the IP address or credentials for the selected Pillar Axiom system.
- Information: Displays detailed information about the selected Pillar Axiom system.
- History: Displays historical information about the selected Pillar Axiom system.

Related concepts

- *About Pillar Axiom System Registration*

Related references

- *View Axiom Systems*

Related tasks

- *Register the Pillar Axiom Systems*

View Axiom Systems

View details about the Pillar Axiom systems that are registered with a Pillar Axiom Replication Engine.

To see the Axiom system details navigate to Protect > Axioms > View Axioms.

The Axiom system details are shown in the Axiom LUN Explorer. The Axiom LUN Explorer (explorer) displays detailed information about the registered Pillar Axiom systems and the replication LUNs.

The explorer allows you to perform the following activities:

- Filter the list of Pillar Axiom systems to a single Axiom system.
- Collapse the hierarchal tree that displays the LUNs.
- Manage the Pillar Axiom systems.

- Update the list of discovered host bus adapter (HBA) ports and available LUNs.
- Scroll through the list of Pillar Axiom system, HBAs, and LUNs. Selecting an item displays detailed information on the right side of the explorer page.

The Axiom LUN Explorer displays the following information in a hierarchical manner:

Axiom system name

Identifies the information about the registered Pillar Axiom system:

- Pillar Axiom 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 13 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 concepts

- *About Pillar Axiom System Registration*

Related tasks

- *Manage Registered Pillar Axiom Systems*
- *Register the Pillar Axiom Systems*

About Pillar Axiom Replication Engine Settings

Pillar Axiom MaxRep Replication for SAN provides options for configuring the Pillar Axiom Replication Engine for operational use. After making changes to the Replication Engine, protect your configuration settings with a back up copy.

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

- Backup and restore the Replication Engine settings

  Backs up your Replication Engine configuration to a Pillar Axiom system so you can restore the Replication Engine in case it fails.

- Clear file replication log

  Specifies the 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 Pillar Axiom MaxRep Replication for SAN uses for file transfers.

Related references

- *Pillar Axiom Replication Engine Thresholds*

Related tasks

- *Back Up the Replication Engine Settings*
- *Restore the Replication Engine Settings*

Back Up the Replication Engine Settings

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

1. Choose **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.

Result:
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 concepts

- *About Pillar Axiom Replication Engine Settings*

Related tasks

- *Restore the Replication Engine Settings*

Restore the Replication Engine Settings

You can restore the Pillar Axiom Replication Engine settings to the original location.

1 Choose **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 concepts

- *About Pillar Axiom Replication Engine Settings*

Related tasks

- *Back Up the Replication Engine Settings*

Pillar Axiom Replication Engine Thresholds

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

The following thresholds can be set in the Pillar Axiom MaxRep Replication for SAN software. 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 14 Pillar Axiom Replication Engine threshold settings

Threshold	Description	Location
Resync File	When the resync cache folder exceeds the Resync File Threshold, the replication pair is throttled. The default Resync File Threshold for a protection plan is 16 GB. **Note:** Throttling occurs when the Replication Engine receives the source data faster than its cache area can release it to the target LUN. In some cases throttling can be caused by the loss of the WAN or when the available WAN bandwidth is not keeping up with the source throughput. Under normal conditions, the system sends the data to the cache volume. When the bandwidth permits, the system sends the cache volume data to the target LUN.	Set the default threshold in the protection plan Replication Options.
Differential	When the resync cache folder exceeds the Resync File Threshold, the replication pair is throttled. The default Resync File Threshold for a protection plan is 16 GB.	Set the default threshold in the protection plan Replication Options.
RPO	When the recovery point objective (RPO) exceeds the specified limit, an email alert is sent.	Set the RPO threshold in the protection plan Replication Options.
Disk Space Warning	When 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 concepts

- *About Pillar Axiom Replication Engine Settings*

About Remote Replication Engine Configuration

Pillar Axiom MaxRep Replication for SAN software discovers the remote Pillar Axiom Replication Engine that is running the control service, which is referred to as the primary Replication Engine. The license installed on the primary Replication Engine is applied to any remote Replication Engines.

The Pillar Axiom MaxRep software must be previously installed on any remote Replication Engines. Remote Replication Engines are licensed from the primary Replication Engine. Verify that the remote Replication Engines are connected by confirming that they are listed in the Remote Replication Engine advanced configuration setting page.

Related concepts

- *About Pillar Axiom Replication Engine Settings*
- *About Capacity Based Licenses*

Related tasks

- *Configure Remote Replication Engines*
- *Verify Remote Replication Engine Connection*
- *Apply Your License*

Configure Remote Replication Engines

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

In a remote replication scenario, complete the following settings from the primary Replication Engine.

- Set the initiator ports, target ports, and target ports for LUN mapping.
- Use the primary Replication Engine to apply the license to the secondary Replication Engine.

Related concepts

- *About FC Initiator and Target Ports*
- *About iSCSI Initiator and Target Ports*

Related tasks

- *Apply Your License*

Verify Remote Replication Engine Connection

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

1 Choose 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 concepts

- *About Remote Replication Engine Configuration*

Related tasks

- *Configure Remote Replication Engines*

Chapter 4

Configure Data Protection

The Pillar Axiom MaxRep Replication for SAN allows you to configure the Pillar Axiom systems for replication.

Data protection options include:

- Create and manage data protection plans.
- Configure replication options (called profiles).
- Analyze profile settings.

About 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.

For 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 concepts

- *About Application Consistency Protection Plans*
- *About Protection Plan Creation*

Related references

- *Data Protection Plan Management*

About Protection Plan Creation

Data protection plans specify the parameters for replication. Creating a protection plan is the same process for a synchronous or asynchronous Pillar Axiom MaxRep Replication for SAN systems.

Before you can create a protection plan for data protection, the following prerequisites must be met:

- The primary and secondary Pillar Axiom systems must be registered with the same Pillar Axiom Replication Engine.
- The Replication Engine ports must be zoned to the Pillar Axiom Slammer ports.
- The Replication Engine ports must be configured with at least one of each of the following port types:
  - Initiator ports
  - Initiator ports for target LUN mapping
  - Target ports
- An appropriately sized retention LUN must be configured and discovered by the Replication Engine.
- The source and target LUNs that form the replication pairs must be created on the source and target Pillar Axiom systems.

  Note: If the source LUN is already in use by a host, its mapping is not affected, but any mappings of a target LUN that was previously presented to a host are removed during the configuration.
- The Replication Engine must have an appropriate license with adequate capacity available to replicate the LUN.

Related concepts

- *About FC Initiator and Target Ports*
- *About iSCSI Initiator and Target Ports*
- *About Protection Plans*
- *About Source and Target LUNs*
- *About Capacity Based Licenses*

Related tasks

- *Create a Data Protection Plan*
- *Register the Pillar Axiom Systems*

Create a Data Protection Plan

Create data protection plans from the primary Pillar Axiom Replication Engine.

1. Choose **Protect** > **Axioms** > **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 Axiom from the **Select Axiom** drop-down list.

   Result:
   After you select the Axiom system, the Select Primary LUN table provides you with a list of available primary LUNs.
5. Select each source LUN that needs to be protected as part of this protection plan from the **Select Primary LUNs** list.

   Note: You have selected the LUN when a check mark displays next to the LUN name.
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 Axiom and the Replication Engine are in different networks, enable this option to establish communication between the primary Pillar Axiom 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 Axiom 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 Pillar Axiom system.
7. Click **Next**.

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

Related concepts

- *About Protection Plans*
- *About Protection Plan Creation*

Related references

- *Replication Options*
- *Data Protection Plan Management*

Related tasks

- *Select Target LUNs*

Select Target LUNs

After you select the source LUNs, select the corresponding target LUNs on the secondary Pillar Axiom system.

1 From the **Secondary Axiom** drop-down list, select the secondary Pillar Axiom system.

   Important! Do not select **Allow smaller sized targets to select**. This option allows you to select target LUNs that are smaller than their source LUNs. Replication of a source LUN to a target LUN that is too small will result in a failed replication.

2 In the **Select Secondary LUNs** table, click **Select**.

3 In the **Secondary Axiom LUNs** pop-up window, select each target LUN that will provide protection as part of this protection plan.

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

   - **Use Secondary Replication Engine NAT IP address for Source**: When the primary Axiom and the Replication Engine are in different networks, enable this option to establish communication between the primary Pillar Axiom 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 Axiom 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 Pillar Axiom system.

5 Click **Next**.

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

Related concepts

- *About Source and Target LUNs*
- *About Source and Target LUNs*

Related tasks

- *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 From the **Replication Options** table, select the **Sync option.**

Valid choices:

- **Direct Copy**: For synchronous replication.
- **Fast Copy**: For asynchronous replication.

3 To set the number of concurrent pairs to resynchronize in the **Batch Resync** field.

4 Set the **Resync File Threshold.** In most cases, the default setting of 16 GB is sufficient.

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

5 To set a time frame for when resynchronizations are allowed for the replication pairs in the protection plan, select **Start automatic resync** and specify the required time interval.

Example:
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 might require manual intervention if the protection plan requires resynchronization.

6 Select the **Compression** option.

Valid options:

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

7 Set the **RPO Threshold** to the maximum amount of time that the pair can be allowed to fall behind synchronous mode.

When the pair falls behind synchronous mode, the Replication Engine starts sending alerts to the administrator.

8 Set the **Differential File Threshold** as needed. In most cases, the default setting of 64 GB is sufficient.

9 Click **Next**.

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

Related references

- *Replication Options*

Related tasks

- *Create a Data Protection Plan*

Replication Options

Replication pairs can be configured for different patterns of replication through the replication options available in the protections plans that are provided by Pillar Axiom MaxRep Replication for SAN.

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

Note: The synchronous or asynchronous configuration of the Pillar Axiom MaxRep system determines the available replication options.

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 for Fibre Channel (FC) attached synchronous replication. However, we recommend that you use 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 can be 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 first two pairs reach differential sync, the next two pairs start step 1 of the resynchronization process. The recovery point will originate only from the resynchronization start time, not the pair configuration time.

Automatic Resync Options

Automatic resynchronization is used when a replication pair is required to address data inconsistencies automatically. During replication, if there is any inconsistency from either of the agents (on primary or secondary server), a Resync required (under Monitor > Protection Status > Volume Protection) field is set to Yes indicating that a resynchronization is required to ensure data consistency.

When the Automatic Resync Option is enabled and the replication pair has a Resync required set 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

Fast Sync

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

The Fast Sync option specifies that Pillar Axiom MaxRep reads a data

		block on the source LUN and calculates the unmatched data in a hash. The same blocks of data are read on the target LUN and a corresponding hash is calculated. The hash is transferred over the network between the source and target Replication Engines. If the data hashes match, it means that the data matches on the target LUN. Because the data matches, data is not transferred over the network. 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 Replication Engines as only differing data hashes are transmitted between the Replication Engines.
	Direct Copy	Copies data directly between source and target LUNs without requiring verification. This option is recommended when both source and target LUNs are accessible from the same Replication Engine or clustered HA pair of Replication Engines. A direct copy occurs mainly in synchronous replication configurations with a single Replication Engine or a clustered pair of Replication Engines.
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.	
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.	

RPO Threshold	Specifies the threshold recovery point objective (RPO) in minutes. If RPO increases beyond this limit, email alerts are sent to the configured email ID.

Related concepts

- *About Protection Plans*
- *About Protection Plan Creation*
- *About Application Consistency Protection Plans*

Related references

- *Data Protection Plan Management*

Define Retention Policy

The final step in creating a protection plan is to define a retention policy for retaining changes to the data that is protected by the plan.

A retention policy defines certain plan parameters:

- How far back in time that you would like to be able to recover the data on your target LUN
- Where you want to store the data that has changed in that period

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

1. Define the retention period in the **Retain all data for** row of the Retention Policy table.

   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. This number is the initial CDP retention window.

   Note: Your capacity-based license may restrict the retention period.

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

3. Specify a limit to the amount of storage space for retention logs on the **Restrict retention storage space to** row.

   The restriction on storage space is used to avoid allowing protected LUNs within a single protection plan to take an unnecessary proportion of the retention log space.

4 Select the insufficient storage space option from the On insufficient storage space drop-down 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, we recommend that you select Purge older retention logs. In the event that the Pillar Axiom 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 row, set the threshold for sending an alert when retention logs reach a percentage of the available storage.

For synchronous replication, we recommend keeping the default 80% setting.

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

Result:
The volume appears in the Retention Volumes table.

7 Click Next.

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

Related concepts

- *About Capacity Based Licenses*

Related references

- *Data Protection Plan Management*

Related tasks

- *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 Pillar Axiom 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 concepts

- *About Protection Plans*

Related references

- *Data Protection Plan Management*

Related tasks

- *Create a Data Protection Plan*

About Application Consistency Protection Plans

When you are running applications in Windows that support Volume Shadow Copy Service (VSS) Provider plug-in, you will want to create application consistent bookmarks. 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.

Before you create a data protection plan for application consistency, you need to install the MaxRep agent on the server that accesses the LUNs that you want to protect and verify that the agent has been registered with the primary Replication Engine. Then you need to create a protection plan and configure a consistency policy for your application in the protection plan. After you verify that the consistency policy job was successfully activated, you can test your application consistency setup by creating a recovery snapshot.

Related concepts

- *About the MaxRep Agents*

Related tasks

- *Verify MaxRep Agent Installation*
- *Create a Data Protection Plan*

Verify MaxRep Agent Installation

Verify that the application host that is running the MaxRep agent is registered with the primary Pillar Axiom Replication Engine.

1. Start the Pillar Axiom MaxRep Replication for SAN software on the Replication Engine that is running the control service.
2. Choose Settings > Settings > License Management > Apply License.
3. Verify that the name of the host appears in the list of Licensed Hosts.

Related concepts

- *About the MaxRep Agents*

Related references

- *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 is to be protected and create bookmarks in the data as roll back targets.

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

1. Choose 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.
   - If you want to protect data for a specific Windows application, select the application from the Application Agent list:
     - Microsoft Exchange Server 2003, 2007, or 2010
     - Microsoft SQL Server 2000, 2005, or 2008
     - Oracle (Unix/Linux), RAC, CFS
   - If you want to create consistency bookmarks for a particular volume rather than for a specific application, specify the actual volumes on the host in the Other Volumes field.
6. Click Save.

   Result:
   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.
   - Choose 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 Properties for the `InMageVssProvider` event, and verify that the bookmark tags were successfully sent to the remote server.

Related concepts

- *About Application Consistency Protection Plans*

Related tasks

- *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 by creating a virtual snapshot and confirming that application consistency bookmarks were created as expected.

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

2 Select the check box that is next to 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 concepts

- *About Application Consistency Protection Plans*

Related tasks

- *Create a Virtual Snapshot*

Data Protection Plan Management

After you have successfully created a protection plan, the Pillar Axiom MaxRep Replication for SAN interface 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** > **Axioms** > **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 1:N protection plan when you take any of these actions on an existing plan:

- Add another primary Pillar Axiom system.
- Add a target LUN on an existing primary Axiom 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 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 consistency policy and run it or to manage an existing 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
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 and displays the *protection direction*, which is listed as one of the following:
  - Forward Protection: Replication occurs rom the primary Pillar Axiom system to the secondary Axiom system, which is the default direction.
  - Backward Protection: Replication occurs from the secondary Pillar Axiom system to the primary Axiom system.

	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 any problems with a failed protection plan.
Modify	Allows you to make changes to the protection plan. When you click **Modify**, a dialog is displayed with the following options: ■ **Modify Replication Options**: Allows you to modify the protection plan replication options. ■ **Modify Retention Policy**: Allows you to specify the length of time to retain the replicated 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 or slowed down. If you selected a secondary Axiom system when you created the protection plan, the following options are available from the **Modify** action. ■ **Create incomplete**: Allows you to edit the protection plan starting at the last incomplete field. ■ **Inactive**: Allows you to edit all of the protection plan. ■ **Active**: Allows you to edit the protection plan. However, you

cannot select a new primary Pillar Axiom system.

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.

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.
- Create a multi–hop protection plan.
- 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 delete the plan.

Deletion Pending
An administrator has initiated the deletion of the protection plan.

Last Modified Time
Indicates the most recent time that the protection plan was modified.

Related concepts

- *About Protection Plans*

Related tasks

- *Create a Data Protection Plan*

Display Protection Plan Summary

You can view a summary of a Pillar Axiom MaxRep Replication 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 Choose Protect > Axioms > Manage Protection Plan.

2 From the Protection table, select the protection plan to edit.

3 Click Summary.

Result:
The system displays details about the protection plan.

Related references

- *Data Protection Plan Management*
- *Application Protection Monitoring*

Display Protection Plan Details

You can view the details of a Pillar Axiom MaxRep Replication 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. Choose **Protect** > **Axioms** > **Manage Protection Plan**.
2. Select the protection plan to edit from the Protection table.
3. To view the plan details, click **Plan Details**.

   Result:
   The system displays details about the protection plan.

Related references

- *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. Choose **Protect** > **Axiom** > **Manage Protection Plan**.
2. Locate the protection plan to be activated in the **Protection** table.
3. Click **Activate** in the **Action** column for the protection plan.

4 Click **Save** on the Summary page.

Result:
The **Activation Status** changes to **Prepare Target Pending** for newly created protection plans or to **Active** for existing protection plans that have been activated.

Related references

- *Data Protection Plan Management*

Related tasks

- *Create a Data Protection Plan*

Modify Protection Plan Replication Options

Modify the protection plan replication options when secure transport to the secondary Pillar Axiom system or automatic resynchronization is necessary.

1 Choose **Protect** > **Axioms** > **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 references

- *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 Pillar Axiom Replication Engine should keep the data for the replication pairs.

1 Choose **Protect** > **Axioms** > **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 commit your changes, click **Save**.

Related references

- *Data Protection Plan Management*

Related tasks

- *Define Retention Policy*

Deactivate a Protection Plan

Deactivate a protection plan to suspend replication. This option allows you to clean the Continuous Data Protection (CDP) logs.

1 Choose **Protect** > **Axioms** > **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 references

- *Data Protection Plan Management*
- *Application Protection Monitoring*

Restart a Protection Plan Resync

Remapping a source or target LUN might cause the resynchronization process to slow down or stop. Restarting the resynchronization process ensures that the protection plan runs properly.

1 Choose **Protect** > **Axioms** > **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 references

- *Data Protection Plan Management*
- *Application Protection Monitoring*

Related tasks

- *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 Choose **Protect** > **Axioms** > **Manage Protection Plan.**

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

3 Click **Delete.**

4 Review the protection plan details.

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

Related references

- *Data Protection Plan Management*
- *Application Protection Monitoring*

Pause or Resume a Protection Plan

You can pause or resume the activity of a selected protection plan.

1 Choose **Protect** > **Axioms** > **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 protection details as necessary.

6 Change the replication mode.

Valid options:

- Pause Replication
- Resume Replication

Related references

- *Data Protection Plan Management*
- *Application Protection Monitoring*

CHAPTER 5

Monitor Data Protection

About Monitoring Data Protection

When you log in to Pillar Axiom MaxRep Replication for SAN the Monitor tab summary displays. The tab displays a high-level overview of the health of your Pillar Axiom Replication Engines, application consistency file and volume protection. The Monitor tab also displays any alerts or notifications that may need your attention.

Note: The first time you log in to Pillar Axiom MaxRep Replication for SAN, the following message displays:

```
This Replication Engine Server is not yet licensed. Navigate
to the License Management page to upload a license.
```

Navigate to **Settings** > **License Management** and follow the instructions on the License Management page to upload and apply your license.

The Monitor tab displays three sections:

Protection Health Shows the healthy, warning, critical, or inactive status of the protection plans, volumes, replication pairs, and file replication jobs in your system. The information is shown as percentages in the form of a pie chart.

Alerts and Notifications Shows the events that need your attention 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.

Control Service/ Process Service Health Shows information about the Replication Engines and contains one tab for the Control Service that runs on the primary Engine and one tab for each Process Service that runs on each active Engine.

- The **Control Service** tab shows the health of the Control Service processes that run on the primary Replication Engine. The Control Service is the primary service used to configure the replication process and policies.

- ○ The **Process Service** 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.

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.

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.

The Protection Status menu contains the following items:

Application Protection	Monitors the status of your application protection replication pairs.
Volume Protection	Monitors the status of your volume replication pairs.
File Replication	Monitors the status of your file replication pairs.
Rollback/Snapshot Progress	Follows the progress of any rollbacks or snapshots.
Agent Heartbeat	Checks the status of communication between the Replication Engines and any agents that are running on your system.
Versions and Updates	Lists the versions of the software, services, and agents on the Replication Engines.

Related concepts

- *About Capacity Based Licenses*
- *About Alerts*
- *About Reports*

Related references

- *Application Protection Monitoring*
- *Monitor Rollback or Snapshot Progress*
- *Agent Heartbeat Monitoring*
- *Versions and Updates*

Application Protection Monitoring

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

To display the Application Protection page, choose **Monitor** > **Protection Status** > **Application Protection**. All of your application protection plans are listed in the **Protection Plan** table. Click the plus sign beside the name of a protection plan to expand the plan details.

When you expand a protection plan, the system displays the following for the plan:

- Scenario Type
- Server
- Protection Direction
- Status
- Summary
- Last Modified Time

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 associated Pillar Axiom system can be determined by the last 4 digits of the LUID, which would match the last four digits of the Pillar Axiom system's serial number.

Health Displays the health status of the volume replication pair and its associated Pillar Axiom 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.

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 in differential sync or the pair 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 will stall. 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 a Pillar Axiom Replication Engine process service or on a secondary server.

Note: If the data that is in transit exceeds the Differential File Threshold that is set in the replication settings for the protection plan, the replication will stall. The replication stalls while moving from write order fidelity Data Mode into Meta Mode, which is not write order fidelity. The occurrence of this type of stall emphasizes the need for proper values for these settings.

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, which includes 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, which includes 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 concepts

- *About Monitoring Data Protection*

Related tasks

- *Display Protection Plan Details*
- *Display Protection Plan Summary*

LUN Protection Monitoring

Allows you to display details about the protected volume (LUN) replication pairs. If the list is too long, you can filter the search results.

To display the Volume Protection page, choose **Monitor** > **Protection Status** > **Volume Protection**. The names of the primary server and the secondary server that support volume replication pairs are listed under the **Source Host** and **Target Host** drop-down menus respectively. By default, all of the volume replication pairs are displayed. 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.

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 Pillar Axiom 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 Pillar Axiom 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 in differential sync or the pair 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 Differential File Threshold that is set in the replication settings for the protection plan, the replication will stall. The replication stalls while moving from write order fidelity Data Mode into Meta Mode, which is not write order fidelity. The occurrence of this type of stall emphasizes the need for proper values for these settings.

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
Selecting this option removes the read-only mode to unlock the secondary volume on the secondary server.

RPO Threshold
Sends alerts if the recovery point objective (RPO) exceeds the selected threshold. Alerts are sent to the designated user and to the Alerts and Notifications section in the Pillar Axiom MaxRep interface.

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 that can be used for storing files during resynchronization, in MB.

Differential File Threshold (MB)	Indicates the maximum storage capacity that can be used for storing files during the differential synchronization, in MB.
Compression	Indicates whether data will be compressed. 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 amount of CDP retention storage capacity available and for the period of time that it will be retained.

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 references

- *Application Protection Monitoring*

Related tasks

- *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 drop-down menus respectively. By default, all of the file replication pairs are displayed.

File replication pairs are listed in the File Protection Status table. 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 is 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 given 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 to be replicated from the Source Host.

Target Host Indicates the secondary server name. This secondary server is the server that will host the replicated data from the source host in the protection plan.

Target Directory Indicates the secondary server directory, to which the replicated data from the source host will be replicated.

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 is set at a value that is greater than 1 GB, Internet Explorer will not be able to handle the file. However, Firefox will support up to 2 GB. The recommended workaround is to 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 concepts

- *About MaxRep for Replication Logs*

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 tasks

- *Monitor Rollback Progress*
- *Monitor Snapshot Progress*

Monitor Rollback Progress

You can monitor the progress of a secondary Pillar Axiom LUN rollback operation.

1. Choose **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.

   Important! A rolled back LUN cannot be used as a secondary LUN for any other replication pair unless the rolled back LUN is released at the **Monitor Rollback** page.
3. To release a rollback drive, select it and click **Release Drive**.

Related references

- *Monitor Rollback or Snapshot Progress*

Monitor Snapshot Progress

You can monitor the progress of a recovery snapshot or scheduled snapshot operation.

1. Choose **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. To release a drive, select one or more pairs and click **Release Drive**.

   Result:
   The recovery snapshots are deleted from the secondary Pillar Axiom system.
4. To force a deletion of a snapshot, select one or more pairs and click **Force Delete**.

   Result:
   The recovery snapshots are deleted by force from the Replication Engine.

Related references

- *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. Choose **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) Select one or more schedules and click **Delete Scheduled Jobs** to delete the schedule.

Related references

- *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. Choose **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) Select one or more pairs and click **Release Drive** to delete the recovery snapshots from the secondary Pillar Axiom system.
5. (Optional) Select one or more pairs and click **Force Delete** to force the deletion of the recovery snapshots from the Pillar Axiom Replication Engine.

Related references

- *Monitor Rollback or Snapshot Progress*

Agent Heartbeat Monitoring

Agent heartbeat monitoring checks agent communication between the Pillar Axiom Replication Engine and the registered Pillar Axiom systems.

From the Pillar Axiom Storage Services Manager, choose **Protect** > **Replication Engine**.

The Replication Engine overview page shows the following information:
Agent Status

Identifies the communication status of the MaxRep agents registered with the Pillar Axiom system. Valid states:

○ All Communicating

- Warning
- Unknown

Service Status

Identifies the health of the processes running on the Replication Engine. Valid states:

- Normal
- 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 Pillar Axiom MaxRep Replication for SAN software version 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, Pillar Axiom MaxRep sends the designated user an alert email. The Replication Engine also sends an SNMP trap to the Pillar Axiom system for callhome processing. You can configure the amount of time before an alert is sent by choosing Settings > Agent Settings.

The reasons for the agent server 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 concepts

- *About Pillar Axiom Replication Engine Settings*

Related references

- *Application Protection Monitoring*

Versions and Updates

Version numbers and updates to your control service Pillar Axiom Replication Engine, process service Replication Engines, and agents are listed on the Versions and Updates page.

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 when clicked.

Host Name Displays the host name of the agents.

Process Engine Version Indicates the versions of the Replication Engines on which the process service is running.

Process Engine Installation Date Indicates the dates of installation of the Replication Engines on which the process service is running.

Installation Path Indicates the path of installation of the Replication Engines on which the process service is running.

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 have been applied to the agents when clicked.

Host Name Displays the host name of agents.

Volume Replication Indicates the version of VX agent. A VX agent is a host-based volume splitter that enables application protection and replication.

File Replication Indicates the version of FX agent. An FX agent is a host-based filesystem splitter that enables application protection and replication.

Sentinel Driver Indicates the version of sentinel driver.

Product Version Indicates the product version.

Related concepts

- *About Monitoring Data Protection*

Balance Process Service Loads

A single process service can be used by many Pillar Axiom Replication Engines, which can lead to degraded performance. You can choose to add additional network interface cards (NICs) to the process service and assign them to desired NICs. Bandwidth control becomes possible for engines, if they are using separate NIC cards for communication.

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

1 From the Pillar Axiom MaxRepgraphical user interface (GUI), choose Settings > Advanced Configuration > Process Server Load Balancing.

  Result:
  The Agent - Process Server NIC Mapping 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 MaxRep agent to use 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 references

- *Balance Traffic Loads Settings*
- *MaxRep Agent Settings*

Related tasks

- *Display Host Logs*

Balance Traffic Loads Settings

Allows you to specify the parameters for balancing traffic loads on the Pillar Axiom MaxRep Replication for SAN Pillar Axiom 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 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 tasks

- *Balance Process Service Loads*

Display Network Configuration

The network configuration page provides details about the process services running on the Pillar Axiom Replication Engine.

1 Choose 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 references

- *MaxRep Agent Settings*

Related tasks

- *Balance Process Service Loads*
- *Display Host Logs*

Manage Bandwidth Usage

You can manage bandwidth usage by creating bandwidth policies.

The process services for all known Pillar Axiom Replication Engines are listed in the Configure Bandwidth Utilization table on the Bandwidth Shaping page.

1 Choose Protect > Provisioning > Manage Bandwidth Usage.

Result:
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 Pillar Axiom 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**.

   Example:
   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**.

   Result:
   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 concepts

- *About Reports*

Related tasks

- *View Bandwidth Reports*

About Reports

Pillar Axiom MaxRep Replication for SAN provides two types of reports: bandwidth reports and health reports.

Bandwidth reports

- ○ Provides information on the incoming and outgoing FTP traffic for each Replication Engine on your system.
- ○ Provides the FTP 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 by 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 tasks

- *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. Choose **Monitor** > **Reports**.
2. Click **Bandwidth Reports** to view the default bandwidth report for your primary Pillar Axiom system.

   If necessary, select a different Pillar Axiom Replication Engine from the **Select Host** drop-down list.
3. To see a graphical view of the bandwidth report, choose one of:
   - **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 concepts

- *About Reports*

Related tasks

- *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 Choose 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 options:

   - 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 concepts

- *About Reports*

Related tasks

- *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 concepts

- *About Reports*

Related tasks

- *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 Choose **Protect** > **Axioms** > **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.

Result:
The system displays health reports about and settings for the replication pair.

Related concepts

- *About Reports*

Related references

- *Replication Reports Settings*

Related tasks

- *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. Choose **Protect** > **Axioms** > **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**.
9. (Optional) To configure the settings on another protection plan, select the plan from the **Move to Another Plan** and then click **Move**.
10. (Optional) To create a new protection plan using the existing settings, select **Create New Plan**, enter the plan name, and then click **Move**.

Related references

- *Replication Reports Settings*

Related tasks

- *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

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 throttled duration in hours, which 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. Select the value to display the cumulative details. Values include:

- RPO Health
- Throttle Health
- Retention Health
- Resync Health
- Replication Accuracy

Related references

- *Log Management*

Related tasks

- *Display Replication Pair Reports*
- *Configure Replication Pair Settings*
- *Display Host Logs*
- *Display Pillar Axiom Replication Engine Logs*
- *Display Audit Logs*
- *Download Logs*

About MaxRep for Replication Logs

Pillar Axiom MaxRep Replication for SAN collects a variety of logs that collect user actions and host and Pillar Axiom Replication Engine activities.

The host logs that are collected include logs of the activities of the MaxRep agents running on host systems, Replication Engine logs of activities of the Replication Engines, and audit logs of user activities.

Separate pages are available for viewing or downloading host logs, Replication Engine logs, and audit logs. A Download Logs page is also available for downloading host or Replication Engine logs from a single page.

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
This page lists, for the current Replication Engine, the available Replication Engine activity logs for the Pillar Axiom agents that are running on the hosts.

Replication Engine Logs
This page 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
This page contains lists of host and Replication Engine logs that can be downloaded as a zip or tar archive file.

Audit Logs
This page contains the Audit Log table, listing all user actions on the current Replication Engine.

Log Management

Allows you to review the exception events that have occurred in the Pillar Axiom Replication Engine. You can also edit the settings for log collection and retention from this page.

Log Rotation List

Select 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 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 edit the policy settings.

Edit Log Rotation Settings

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
Select this option to specify the number of days to retain the data log.

Space based
Select this option to limit the size (in MB) of the data log.

Save
Select this option to retain your changes.

Back
Select this option return back to the Log Management page. If you select this option without first clicking Save, you will lose your changes.

Related concepts

- *About MaxRep for Replication Logs*

Related tasks

- *Download Logs*

Display Host Logs

The activities of a MaxRep agent are passed to the Pillar Axiom Replication Engine in the form of host log files.

1 To select a host, choose **Monitor** > **Logs** > **Host Logs**.

Result:
A list of the logs that are available to view displays.

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.

Result:
The log is displayed as a text file in your default text editor.

Note: If the default text editor does not format the text properly, the log file will need to be saved and opened using 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 concepts

- *About MaxRep for Replication Logs*

Related references

- *Log Management*

Related tasks

- *Download Logs*

Display Pillar Axiom Replication Engine Logs

The data statistics, data transfer, debugging, and auditing actions that take place in the Replication Engine are collected as Pillar Axiom Replication Engine logs.

1 To select a Replication Engine log, choose **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.

Result:
The log is displayed as a text file in your default text editor.

Note: If the default text editor does not format the text properly, the log file will need to be saved and opened using another text editor, such as gVim or Notepad++.

4 You can view the following logs as needed:

Table 15 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 the user interface 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 MaxRep agent after compression or decompression at the Replication Engine.
Traplog	Replication Engine tap event generated messages.
rsyncd	Remote synchronization related messages.
FX job logs	Logs related to FX job logs.

Table 15 Available Replication Engine logs (continued)

Log name	Description
Application	Logs of application protection.
array_register	Logs of array registration.
array	Logs of array protection.
array service	Logs of array services.
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	HA 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.

Table 15 Available Replication Engine logs (continued)

Log name	Description
tman_monitor_disks	Disk monitoring logs.
tman_monitor_ha	Logs for high availability (HA) service.
tman_monitor_protection	Logs for monitor protection.
tman_monitor_ps	Logs for Process Service monitor.
tman_monitor_reports	Logs for report generation.
tman_volsync	Logs for volsync.
Vsnapprocess_vsnap log	vsnap process logs.

Related concepts

- *About MaxRep for Replication Logs*

Related references

- *Log Management*

Related tasks

- *Download Logs*

Display Audit Logs

Administrator interactions with the Pillar Axiom MaxRep Replication for SAN user interface are stored on the Replication Engine in audit logs.

1 To view the audit logs, choose Monitor > Logs > Audit Logs.

All actions by all users are displayed in the Audit Logs table by default.

2 Enter a user name, keyword, or start and end time, and then click Search to filter the audit logs displayed in the table.

Note: The entries are displayed in pages. Use the FIRST, NEXT, PREVIOUS, and LAST selections at the top right of the current page to navigate through multiple pages.

The following information about each user interaction is displayed in the Audit Logs table:

Table 16 Audit log contents

Field	Description
User	Name of the administrator who performed the action
Date/Time	Data and time of the administrator action
IP Address	IP address from which the action was performed
Log Details	Detailed description of the administrator action

Related concepts

- *About MaxRep for Replication Logs*

Related references

- *Log Management*

Related tasks

- *Download Logs*

Download Logs

All host logs and Pillar Axiom Replication Engine logs are listed on the Download Logs page. This page enables you to download any required log from one page.

You can download all the logs or only those in which you are interested.

1. Choose 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 MaxRep agent activity.
   - Select the name of the host from which to download the host or 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.**

Result:
After the archive is completed, the screen will refresh.

4 Click **Download Logs** to download the newly created archive.

5 Choose to open or save the file.

Related concepts

- *About MaxRep for Replication Logs*

Related references

- *Log Management*

About Alerts

Alerts provide important information about Pillar Axiom MaxRep Replication for SAN. Alert notifications can be sent from Simple Network Management Protocol (SNMP) traps and by the system when events occur. These notifications are sent to designated email recipients.

You can configure which Pillar Axiom MaxRep Replication for SAN alerts will trigger a notification. Each new administrator account is configured with a default set of alert notifications. Edit this list as required for a specific administrator.

Email and SNMP trap alerts are sent by default for the following events:

- RPO SLA Threshold Exceeded
- Resync Required
- Agent/Process Service Not Responding
- Replication Engine Secondary Storage Warning
- File Agent job Error
- Agent Has Logged Alerts
- License Expiry And Related Issues
- Bandwidth Shaping Alerts
- Licensed Capacity Threshold Exceeded
- Licensed Capacity Utilization Has Reached Limit
- Daily Protection Health Report Day(s)
- Insufficient Retention Space
- Source Volume Resized
- Process Service Uninstalled
- Replication Engine Debug Info
- Application Protection Alerts

Related references

- *Alerts and Notifications*

Related tasks

- *Edit a User Account*
- *Configure Email Notifications*
- *Configure SNMP Notifications*

Configure Email Notifications

You can configure Pillar Axiom MaxRep Replication for SAN to send notify email recipients of various alerts.

Email delivery of alert notifications requires that the mail server settings and the email address settings of at least one user be configured.

Note: In addition, email alerts and SNMP traps can be activated for the Control Service Node Failover Alert.

1 To set the mail server settings, choose Settings > Replication Engine Settings > Mail Settings.

2 To set the email addresses to receive alerts, choose 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 concepts

- *About Alerts*

Related references

- *Alerts and Notifications*

Related tasks

- *Edit a User Account*

Configure SNMP Notifications

You can configure Pillar Axiom MaxRep Replication for SAN to notify administrators of Pillar Axiom Replication Engine events through Simple Network Management Protocol (SNMP) traps.

Prerequisites:

- You must have an existing Pillar Axiom MaxRep Replication for SAN administrator account before configuring the SNMP settings.
- 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.

Note: In addition, email alerts and SNMP traps can be activated for the Control Service Node Failover Alert.

1. To set the email alerts, choose Settings > User Management > Manage Users.
2. In the Configured System Users table, select Edit.
3. From the Add Trap Listener fields, enter the IP address (or the DNS host name of the host running the SNMP trap listener) and the trap port number.
4. (Optional) If you have more than one SNMP trap server, click Add and enter the additional host information.
5. From the Alert Notification section, under the Trap column, select or deselect the Alert Category or Alert Categories for which you want to receive notifications.
6. To keep your settings, click Save.

Related concepts

- *About Alerts*

Related references

- *Alerts and Notifications*

Related tasks

- *Configure Email Notifications*
- *Edit a User Account*

Alerts and Notifications

By default, Pillar Axiom MaxRep Replication for SAN sends the following email alerts and SNMP traps for notifications of situations that may require corrective action.

Table 17 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: • Resynchronization required might be set due to data inconsistency. • Primary Pillar Axiom LUN has been resized. • Secondary Pillar Axiom LUN is exposed in read/write mode. • Configuration server failover during high availability (HA) scenario. • Manual resynchronization has been requested through the UI.	If a resynchronization was requested manually from the user interface (UI), no action is required. The Plan will resynchronize automatically. 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. Restart a resynchronization from the Pillar Axiom Replication Engine UI.

Table 17 Email alerts and notifications (continued)

Event	Cause	Corrective action
	- Protection plan has been manually deactivated through the UI.	
MaxRep agent not responding	This email is sent when the agent is unable to communicate with the Replication Engine within 900 seconds. Possible causes: - Agent service may not be started. - A firewall may be blocking the agent. - Network failure. - The host may be down.	Possible actions: - Disable any firewalls. - Ensure that the Agent service is running. - Check if the Pillar Axiom system is connected to the correct Replication Engine.
Replication Engine secondary storage warnings and alerts	The storage capacity of a filesystem mounted on the Replication Engine exceeds the storage capacity warning threshold that is configured in the UI. **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 four volumes on the Replication Engine: - `/` - `/home` Possible actions: - Increase the threshold. - 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.
License expiry and related issues	An alert is sent seven days before the license expires and continues until the new license is uploaded.	Contact Oracle Pillar Customer Support to obtain new licenses.
Licensed Capacity Utilization Has Reached Limit	With capacity based licensing, when the full capacity of the license is consumed by replication pairs, an alert is sent. The alert is sent until you upload a higher capacity license or	Contact Oracle Pillar Customer Support to upgrade your license. Delete unneeded replication pairs to reduce capacity used.

Table 17 Email alerts and notifications (continued)

Event	Cause	Corrective action
	remove a replication pair to return the replicated capacity to the defined capacity.	
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.
Insufficient Retention Space	Insufficient capacity is available in one or more retention LUNs for the specified protection plan.	Possible actions: ● Edit the retention policy and increase the retention space to accommodate more logs. ● 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 Pillar Axiom 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 concepts

- *About Alerts*

Related tasks

- *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 references

- *Alerts and Notifications*
- *Unable to Write Replication Data*
- *Slow Replication During Resynchronization*
- *Slow Replication During Differential Synchronization*

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 references

- *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 Pillar Axiom 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 references

- *Protection Plan Error Resolution*

Slow Replication During Differential Synchronization

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 Pillar Axiom 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 references

- *Protection Plan Error Resolution*

About Statistics

Pillar Axiom MaxRep Replication for SAN provides two types of statistics: data change rates and network traffic rates.

Date Change Rates

Select the **Data Change Rates** option to display statistical charts that provide information about the compressed and uncompressed data changes on the primary Pillar Axiom system. The charts show daily and monthly history. Pie charts represent the compressed and uncompressed data capacity for each Pillar Axiom system. Pillar Axiom MaxRep Replication for SAN stores detailed trending charts that contain historical change rates as well.

Network Traffic Rates

Select the **Network Traffic Rates** option to display 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 concepts

- *About Protection Plans*

Related references

- *Network Traffic Rates*

Related tasks

- *View Trending Data Change Rates*

View Trending Data Change Rates

You can monitor the data changes on the primary Pillar Axiom system. 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, choose **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 concepts

- *About Statistics*

Related tasks

- *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, choose Monitor > Statistics > Data Change Rates > Detailed Trending.
2. Select a trending chart to view its details. Chart links:

Daily Cumulative Data Change Graphs

Select a link to display a historical record of the cumulative daily change rate.

Monthly Cumulative Data Change Graphs

Select a link to display a historical record of the cumulative monthly change rate.

Related tasks

- *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, choose **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 per 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 concepts

- *About 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. Choose **Protect** > **Axioms** > **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.

   Result:
   The system displays statistics about and settings for the replication pair.

Related concepts

- *About Statistics*

Related references

- *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 Pillar Axiom system.
Primary Volume	Indicates the name of the source LUN of the replication pair.
Remote Server	Indicates the name of the secondary or remote Pillar Axiom 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 Pillar Axiom MaxRep Replication 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 Pillar Axiom system is enabled.

Secure Source to Replication Engine-Process Service

Indicates whether secure transport, or encryption, from the primary Pillar Axiom 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 Pillar Axiom 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 tasks

- *Display Replication Pair Statistics*

About Profiling

The Profiler is a tool to help identify resource requirements. Create a profile of your primary Pillar Axiom system 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), required storage, and so on. This helps to accurately predict resource requirements between sites and on the secondary Axiom. During profiling only data change rates at the primary Axiom 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 planners 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 tasks

- *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 Pillar Axiom MaxRep Replication for SAN.

When you set up profiling, you create a protection plan to gather information about the LUNs on your primary Pillar Axiom system to be protected.

1. Log in to the primary Pillar Axiom Replication Engine.
2. Choose **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 **Axiom LUNs Profiling** from the **Proceed With** list to create a profile for your primary Pillar Axiom system and then click **Next**.
5. Provide a description for your profile and then select the name of your **Primary Axiom** from the list.
6. Select the LUNs on the primary Axiom 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 concepts

- *About Profiling*

Related tasks

- *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. Choose **Protect** > **Profiling** > **Analyze Your Result.**
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. Default = 0.35.
   - **Retention Window** in days. Default = 3.
3. Select one or more of the replication pairs in the **Pairs Configured** table and then click **Analyze.**

   Result:
   The Results 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 concepts

- *About Profiling*

Related tasks

- *Set Up Profiling*

CHAPTER 6

Recover Protected Data

About Data Recovery

The Pillar Axiom MaxRep Replication for SAN allows you to create and manage data recovery scenarios for the Pillar Axiom systems.

Specific data sets can be recovered in the form of virtual snapshots or physical copies. You can also use the data validation and backup mechanism to create backup and rollback recovery scenarios, and you can use the disk, volume, or LUN recovery mechanism to create or schedule recovery snapshots.

The Recover tab provides options that allow you to perform the following actions:

- Create and manage recovery snapshots.
- Schedule snapshots.
- Create backup and rollback scenarios.
- Monitor snapshot and recovery progress.

Related concepts

- *About Virtual Snapshots*
- *About Physical Copies*
- *About Backup Recovery*
- *About Drive and Volume Recovery*
- *About Protection Plans*

About 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 LUN or to create a new LUN copy.

A virtual snapshot is a virtual LUN that is created on the Pillar Axiom Replication Engine, which then can be mounted to an alternate host. Although the host is accessing the LUN from the Replication Engine, the actual data is located on the target LUN and the retention storage path located on the secondary Pillar Axiom system.

Creating a virtual snapshot does not interfere with the current replication. However, the following situations can impact the retention log LUN.

If a virtual snapshot that is readable and writable shares a LUN with the retention log of a replication pair, the retention log LUN can be filled up as changes are made to the readable and writable virtual snapshot.

Related concepts

- *About Data Recovery*

Related tasks

- *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 located in the More section of the Recover tab.

1. Choose Recover > More > Create Recovery Snapshots.
2. Select the replication pair for which you want to create a virtual snapshot and then click Recover.
3. In Recovery Based On, select whether you want to base your snapshot on a specific point in time or on an application consistency bookmark.
   - If you are using a specific time, specify the time.

- If you are using an application consistency bookmark, select it from the **Search Result** list.

4. In the **Drive Type** section, select **Virtual**.
5. If you want to be able to read or write to your virtual snapshot, select **Read/Write.**

   Clear the selection to make the virtual snapshot read only.

   If **Read/Write** is selected, a Retention LUN must be specified in **Data Log Path.**
6. Choose **Export** to export the snapshot.

   Note: Any changes that are written to the virtual snapshot will be written to the exported retention LUN. If the retention LUN does not have enough storage capacity, other protection plans that use the retention LUN might pause or purge old data . The actions are defined by the protection plan retention policy.
7. Select the **AccessControlGroup Name** to which the snapshot will be exported.
8. Click **Finish** to create the virtual snapshot.
9. Select a LUN for the virtual snapshot and click **Next.**

   Note: You cannot use LUN number 0.
10. To map the virtual snapshot, 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.

Note: To simplify the management of the ACGs the **Access Control Group Information** automatically includes all of the hosts present in the registered Pillar Axiom system.

Note: Make sure the ports of the host to which the recovery snapshot is exported are zoned using the target initiator (AT) ports using the **Replication Engine Target Ports** option.

Related concepts

- *About Virtual Snapshots*

Related tasks

- *Test a Virtual Snapshot*

Test a Virtual Snapshot

Verify that your virtual snapshot appears on the host.

1. After a rescan on the host, you should see a new drive.

   In Windows 2008, you may 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: LUN 0 can be seen by the host and the virtual snapshot, however you cannot map to this LUN.

2. When the drive is online, it should receive a drive letter and you should be able to see its label.

3. You should be able to browse to the drive and check its contents to make sure replication is working as expected.

Related concepts

- *About Virtual Snapshots*

Related tasks

- *Create a Virtual Snapshot*

About Physical Copies

A physical copy is a fully usable LUN and can be remapped from the Pillar Axiom system to any host that has access to the Pillar Axiom SAN.

To create a physical copy, you take a bookmark or a given point in time and create a full block level copy to a physical LUN on the target side.

From the Pillar Axiom Storage Systems Manager, you first create a LUN on the secondary Pillar Axiom system. This LUN must be the same size or larger than the target LUN for which you want to create a physical copy. Then, on the secondary Pillar Axiom system, you map the LUN to an appliance initiator for a target (AIT) port. The mapping enables the Pillar Axiom Replication Engine to see the LUN, and you can create the physical copy. After you release the physical copy, you can map it to a different host for validation.

Related concepts

- *About Data Recovery*

Related tasks

- *Create a Physical Copy*
- *Test a Physical Copy*

Create a Physical Copy

Create a physical snapshot (or copy) of the target LUN to protect the data from disaster at the primary site. When the replication is local, the target is local; otherwise, the target LUN is remote.

1. Create a LUN on the target side that is the same size or larger than the target LUN for which you want to create a physical copy.

   You could thinly provision the target LUN as well.

2. Map the new LUN to the appliance initiator port (AIT) for the target LUNs on the target Pillar Axiom Replication Engine.

3. Note the LUN ID (LUID) of the LUN to be used for the physical copy.

4. To create the physical copy, from the Pillar Axiom MaxRep Replication for SAN software on the primary Replication Engine, choose Recover > More > Create Recovery Snapshots.

   Note: You might need to rescan the Replication Engine HBAs and Pillar Axiom system LUNs.

5 In the Replication Pair Details table, select the replication pair for which you want to create the physical copy and then click **Recover**.

6 Under Recovery Options, choose whether to create the physical copy 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 Axiom 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 copy.

12 To check the LUN activity in the Pillar Axiom system, choose **Monitor** > **SAN** > **LUNs** in the Pillar Axiom Storage Services Manager.

Look at the average IOps and Throughput values for the physical copy volume. Both values should be zero for the physical copy volume before you proceed.

Note: The Pillar Axiom MaxRep software should stop you from releasing the volume if the volume is busy. Regardless, you should verify whether the volume is busy on the Pillar Axiom system before you proceed.

13 To release the physical copy from the Replication Engine, choose **Recover** > **More** > **Monitor Shapshot/Rollback Progress** in the Pillar Axiom MaxRep software.

14 In the Recovery Pair Status list, select the recovery pair and click **Release Drive**.

Related concepts

- *About Physical Copies*

Related tasks

- *Test a Physical Copy*
- *Confirm Application Consistency Virtual Snapshot*

Test a Physical Copy

Verify the integrity of the physical snapshot of the data that was created for disaster recovery.

1. To remap the LUN to a different host for validation, on the secondary Pillar Axiom system, choose **Configure** > **SAN** > **LUNs** in the Pillar Axiom Storage Services Manager.
2. Right-click the physical copy LUN and choose **Modify LUN**.
3. In the Mapping tab, remove the mapping for the Pillar Axiom Replication Engine and create the mapping for the host you will use to validate the data.
4. Go to the server and 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 concepts

- *About Physical Copies*

Related tasks

- *Create a Physical Copy*

About Backup Recovery

You can use backup scenarios to set up an automated backup policy that will schedule a physical copy or a virtual snapshot to be created and presented to a backup media server. Virtual snapshots are generally preferred for backups.

Backup scenarios are also used to validate data on the target server. Rather than use a scenario for data validation, you might choose to manually create a virtual snapshot instead.

You can use rollback scenarios in an asynchronous replication configuration to set up a policy for rolling back data that is saved on the secondary site.

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 physical copy first to ensure that you are selecting the appropriate rollback time period.

Related concepts

- *About Data Recovery*
- *About Virtual Snapshots*

Related tasks

- *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 Pillar Axiom Replication Engine without disrupting ongoing replication.

1 Choose **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 **Virtual** or **Physical** under Drive Type.

Tip: For backups, you might want to select **Virtual**.

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: Runs the scenario once when the specified application consistency bookmark. 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.

Result:
The backup scenario displays in the Recovery Scenarios table.

Related concepts

- *About Backup Recovery*

Related tasks

- *Create a Rollback Scenario*

Create a Rollback Scenario

You can create a scenario whereby target LUNs that are designated for backup but not available are rolled back to a point in time for recovery purposes.

During replication, a target LUN is locked and cannot be accessed by users or applications. A rollback scenario allows you to recover the data at the point in time that the LUN was unavailable. Replication stops during rollback, suspending any policies that are associated with the replication pair. The rollback allows all the data to be recovered from the source LUN and applied to the target LUN.

1 Choose Recover > Create Rollback Scenario.

2 Select the protection plan to which you want to add the rollback scenario from the Select Plan drop-down 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**.

7 To run the saved rollback scenario, choose **Recover** > **Manage Backup/Rollback Scenarios**.

8 Locate the rollback scenario in the Recovery Scenarios list and then click **Run** in the Actions column.

Related concepts

- *About Backup Recovery*

Related tasks

- *Run a Backup Scenario*

Run a Backup Scenario

The backup scenario is working when you set the scenario to an active run state.

1 Choose **Recover** > **Data Validation and Backup** > **Manage Backup/Rollback Scenarios**.

2 Select the protection plan for which you want to test from the Recovery Scenarios table and then click **Run**.

3 Verify the information on the Create Data Validation and Backup Scenarios page and then click **Run**.

Result:
The system displays the Recovery Scenarios table again.

4 Verify that the backup scenario Execution Status field is displayed as **Active**.

Related concepts

- *About Backup Recovery*

Related tasks

- *Create a Rollback Scenario*

About Drive and Volume Recovery

You can create recovery snapshots at any time, or you can schedule the creation of a recovery snapshot on a regular basis. You can also roll back a LUN on your secondary Pillar Axiom system to a previous time or to a recovery point.

Recovery snapshot A recovery snapshot can be based on a specific time, or it can be based on a specific application consistency bookmark.

Scheduled snapshot A time-based recovery snapshot can be scheduled to be created at a specified time and frequency.

Secondary Axiom rollback A LUN on the secondary Pillar Axiom system can be rolled back to a specified time or to a specific application consistency bookmark.

Related concepts

- *About Data Recovery*

Related tasks

- *Create Recovery Snapshots*
- *Schedule Recovery Snapshots*
- *Perform Secondary LUN Rollback*

Create Recovery Snapshots

You can create recovery snapshots of one or more replication pairs by selecting Recover > More > Disk/Volume/LUN Recovery > Create Recovery Snapshots.

All the replication pairs that are being protected are listed in the Replication Pair Details table. Select a pair or a group of pairs, or click Search to list only those pairs on a specified source host, target host, or volume.

1. Select a replication pair or group of replication pairs.
2. (Optional) Click View Recovery Range to see the Recovery Point Accuracy graphs for the selected pair or group of pairs.

   You can change the time frame for the graph by moving the Start Time and End Time controls in the bar below the graph and then by clicking Re-Generate Graph. You can revert to the original graph by clicking Reset.
3. Click Recover.
4. Select Using Time or Using Application Consistency Event Based in the Recovery Options table.

- If you select **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.
- If you select **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

5 Select **Physical** or **Virtual** as the drive type for the snapshot.

- If you select **Physical**, choose from the available physical volumes to store the snapshot.
- If you select **Virtual**, leave **Read/Write** checked and provide the data log path from the drives suggested for storing Data log files, or uncheck this option and you will not need to provide the data log path. Choose **Virtual Drive** and leave the mount point text box blank, or choose **Virtual Mount Point** if you need to mount the virtual snapshot on a Linux system.

6 Click **Next**.

Review the recovery details.

7 Click **Finish** to create the recovery snapshot.

Related concepts

- *About Drive and Volume Recovery*

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 Pillar Axiom system. Without the recovery snapshot, data recovery only includes the data at the time the replication was initiated.

1 Choose **Recover** > **More** > **Create Scheduled Snapshots.**

2 Select the replication pair and click **Create Snapshot**.

3 Follow the instructions for creating a physical copy 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 concepts

- *About Drive and Volume Recovery*

Related references

- *Replication Options*

Related tasks

- *Create a Physical Copy*
- *Create a Virtual Snapshot*

Perform Secondary LUN Rollback

After creating the rollback scenario, you can rollback a secondary LUN to a specified recovery point.

All replication pairs that are not included in a protection plan are listed in the Replication Pair Details table. Select a pair or click **Search** to list only those pairs on a specified source host, target host, or volume. To roll back a LUN that is included in a protection plan, create a rollback scenario for the plan and then run the rollback scenario.

1 Choose **Recover** > **More** > **Disk/Volume/LUN Recovery** > **Perform Secondary LUN Rollback.**

2 Select a replication pair.

3 (Optional) Click **View Recovery Range** to see the Recovery Point Accuracy graphs for the selected pair or group of pairs.

   You can change the time frame for the graph by moving the **Start Time** and **End Time** controls in the bar below the graph and then by clicking **Re-Generate Graph**. You can revert to the original graph by clicking **Reset.**

4 Click **Rollback.**

5. Click **OK** to approve deletion of the replication pair.
6. Click **OK** to approve deletion of the retention logs.
7. Select **Using Time** or **Using Application Consistency Event Based** in the Recovery Options table.
   - If you select **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.
   - If you select **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. Click **Save** to start the secondary LUN rollback.

Related concepts

- *About Drive and Volume Recovery*

Related tasks

- *Create a Rollback Scenario*

Glossary

The following terms are used with these meanings in the Pillar Axiom 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 Pillar Axiom 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 Pillar Axiom 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 Pillar Axiom 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 filesystem 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 running on the primary Replication Engine 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 filesystem splitter that enables application protection and data replication.

home LUN
A LUN on the Pillar Axiom 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 requires a synchronous and an asynchronous replication license.

physical replication copy
A point-in-time full volume copy of a target LUN. The full replication copy can be accessed directly from the Pillar Axiom system.

Pillar Axiom MaxRep Replication 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 Pillar Axiom MaxRep Replication for SAN.

Pillar Axiom system
The Pillar Axiom system is a complete and integrated full-featured network storage system.

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 Pillar Axiom 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 Pillar Axiom 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 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

Pillar Axiom hardware required for Pillar Axiom MaxRep.

Replication Engine cache

The memory available on the replication engine for staging the data that is associated with replication operations.

Replication Engine target LUNs

The LUNs on the Pillar Axiom system identified as a destination for replication. These LUNs must be created on the Pillar Axiom system prior to configuring replication.

Replication Engine target ports

The ports on the Replication Engine that receive I/O commands from any initiator, usually from the Pillar Axiom 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 Pillar Axiom 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 replication copy
Mechanism to automate periodically creating recovery points to which data can be rolled back.

source LUN
The LUN designated for replication that is located on the primary Pillar Axiom system.

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 Pillar Axiom system will not be acknowledged until it has been written to both the primary Pillar Axiom system and the Replication Engine.

virtual snapshot
Differential snapshot accessible only through the Replication Engine. Pointer-based representative of a set of LUNs presented through the appliance. May have performance overheads but requires less time to create. Not meant for production usage. Allows recovery without stopping replication.

VX agent
Host-based volume splitter that enables application protection and replication.

write splitter
The Pillar Axiom feature that controls the data write operations by splitting the write data between the primary Pillar Axiom and the Replication Engine. The write splitter runs on the Slammer.

Index