

Pillar Axiom



Administrator's Guide

ORACLE®

PILLAR AXIOM

Part Number: E27588-01
Pillar Axiom release 5.3
2012 January

Copyright © 2005, 2012, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

This software or hardware and documentation may provide access to or information on content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Copyright © 2005, 2012, Oracle et/ou ses affiliés. Tous droits réservés.

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf disposition de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, breveter, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est concédé sous licence au Gouvernement des Etats-Unis, ou à toute entité qui délivre la licence de ce logiciel ou l'utilise pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique :

U.S. GOVERNMENT RIGHTS. Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer des dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour ce type d'applications.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation.

Table of Contents

Preface

Chapter 1 Welcome to Pillar Axiom 600 Administration

About Pillar Axiom Storage Services Manager.	22
About Accessing Pillar Axiom 600 Applications.	24
About Client Application Download Formats.	26
Download the GUI Application.	26
Install the GUI Application with Windows Installer.	27
Install the GUI Application Archive File.	28
About Accessing the Pillar Axiom System.	30
Log In to the GUI.	31
Status Bar Description.	33
Configure Automatic Screen Updates.	35
Log Out of the GUI.	35
About Licensing Optional Premium Features.	37

Chapter 2 Manage Global Settings

About Global Settings Configuration.	38
Modify the Pillar Axiom System Time.	39
Modify Asset Information.	40
About Network Settings.	41
About the Network Interfaces.	41
About System Notifications.	43
About iSCSI Settings.	48
Configure iSCSI System Settings.	49
About Modifying Administrator Account Security Settings.	51
Modify Security Settings.	52
About SNMP Trap Host Management.	53
System Components That Can Be Monitored.	53
Create SNMP Hosts.	55

Modify SNMP Hosts.	56
Delete SNMP Hosts.	56
View SNMP Hosts.	57
Download the Pillar Axiom MIB.	58
Chapter 3 Manage Administrator Accounts	
About Creating Administrator Accounts.	59
Create a Pillar Axiom Administrator Account.	60
Display Administrator Account Details.	61
About Modifying Administrator Accounts.	62
Modify an Administrator Account.	62
Change Administrator Passwords.	63
Delete an Administrator Account.	64
Chapter 4 Manage Storage Groups	
Display Capacity Usage.	65
About Volume Groups.	67
Display Volume Group Details.	68
Create Volume Groups.	69
Modify Volume Group Attributes.	69
Delete a Volume Group.	70
About Moving Volumes to Different Volume Groups.	71
Move a Volume to a Different Volume Group.	71
About Storage Domains.	73
About Primary Storage Domains.	76
About Managing Storage Domains.	77
About Logical Volumes and Storage Domains.	83
Chapter 5 About Provisioning and Quality of Service	
Volume Capacity and Provisioning Overview.	85
Thinly Provisioned Volumes.	85
Free Capacity and Volume Creation.	87
Allocation of Thinly Provisioned Storage.	88
Growth Increments.	89
Capacity Overhead.	90
Parity in Reported Capacities.	91
Reclaiming Capacity.	91
About Quality of Service.	92
About Storage Classes.	92
About Priority Levels.	93

About Redundancy.	94
About Access Bias.	95
About I/O Bias.	96
Effects of Access Bias and I/O Bias.	97
About Enhanced Performance for Random Write Operations.	98
About Storage Profiles.	99
System Storage Profile Properties.	101
About RAID Array Stripes.	106
About Enhanced Performance for Oracle ASM.	106
About Managing Storage Profiles.	107

Chapter 6 Manage SAN Volumes and Hosts

Manage SAN LUNs.	111
Connection Status of Slammer Ports.	112
About Creating LUNs.	113
Display LUN Details.	124
About Modifying LUNs.	124
About Moving Logical Volumes.	130
Move a Volume to Another Storage Domain.	130
About Copying Logical Volumes.	132
Copy a LUN.	132
Disable the Data Path of a LUN.	133
Enable the Data Path of a LUN.	133
Delete a LUN.	134
About SAN Host Management.	135
Display SAN Host Settings.	136
About Modifying SAN Hosts.	136
Delete a SAN Host Entry.	140
Associate a SAN Host.	140
About Host Groups.	141
Download and Install the Pillar Axiom VDS Provider.	147

Chapter 7 Manage Data Protection

About Data Replicas and System Capacity.	149
About Copying and Cloning LUNs.	151
View Protection Schedules.	152
About Managing Clone LUNs.	153
Create an Immediate Clone LUN.	153
Delete a Clone LUN.	154

Delete All Clone LUNs.	155
Display Clone LUN Details.	155
Restore a LUN from a Clone LUN.	156
About Data Protection Schedules.	158
Create LUN Data Protection Schedules.	158
Modify a LUN Data Protection Schedule.	159
Delete a LUN Data Protection Schedule.	160
View a LUN Data Protection Schedule.	161
Manage a Replication Engine.	162
About the Pillar Axiom VSS Provider Plug-In.	163
Download and Install the VSS Provider Plug-In.	164
Chapter 8 Manage Software Components	
Display Software Versions.	166
About Updating the Pillar Axiom Software.	167
Download Firmware and Software Updates.	167
Upload the Software Package.	169
Confirm the Upgrade Paths.	169
Update the Pillar Axiom Software.	170
Schedule the Software Update.	171
Cancel a Scheduled Software Update.	172
About the Drive Firmware Update.	173
Upload the Drive Firmware Package.	173
Update the Drive Firmware.	174
Remove the Drive Firmware Package.	175
Chapter 9 Manage Hardware Components	
Display Hardware Component Status.	176
Display Additional Details for the FRUs.	177
Modify a Hardware Component Name.	178
About Hardware Replacement.	179
Identify the Hardware Component.	179
Replace a FRU.	180
About Brick Drive Insertion.	181
Accept a Foreign Drive.	182
About Managing Bricks.	185
About Adding Bricks to a Storage Domain.	185
Accept a Brick.	186
About Reassigning Bricks.	188

Reassign a Brick to Another Storage Domain.	188
Remove a Brick.	189
About the UPS Device.	191
Create a UPS Device.	191
View a UPS Device.	192
Modify a UPS Device.	192
Delete a UPS Device.	193
Chapter 10 Manage Event Logs, Notifications, Alerts, and Jobs	
About Event Logs.	194
Display the Event Log.	195
Delete an Event Log.	195
Display the Event Properties.	196
Filter Event Log Entries.	196
About Managing Event Notifications.	198
Display Event Notifications.	198
Event Notification Selection.	199
Create an Event Notification.	199
View Event Notification Details.	200
Modify an Event Notification.	201
Delete an Event Notification.	201
About Responding to System Alerts.	203
Manage System Alerts.	203
Display System Alerts.	204
Delete a System Alert.	204
About Clearing Pinned Data.	204
About Scheduled Jobs.	206
View a Job Schedule.	206
Modify a Job Schedule.	207
Delete a Job Schedule.	208
Chapter 11 Perform Diagnostic Operations	
About Pillar Axiom Diagnostics.	209
Display the System Status Summary.	211
About Data Consistency.	212
Verify Data Consistency.	213
About System Log Bundles.	214
View UI Client Logs.	215
Create a Log Bundle.	215

Collect Statistics.	216
Download Log Bundles.	217
Send Logs to Call-Home Server.	218
Delete Log Bundles.	218
About Slammer Diagnostics and Connectivity Testing.	220
Run Slammer Diagnostics.	221
View Slammer Diagnostics.	222
Slammer Connectivity Commands.	223
Test System Connectivity.	224
About PITMAN Diagnostic Tool.	225
Run PITMAN Diagnostics.	226
About the Brick Console.	227
View Brick Console.	228
Run Brick Commands.	229
Shut Down the Pillar Axiom System Software.	232
Restart the Pillar Axiom System Software.	233
About System Startup.	234
About System Halt Points.	236
Manage System Halt Points.	237
Continue System Startup.	238
Reset Pillar Axiom System.	239
Chapter 12 Manage Reports	
About Generated Reports.	240
Generate a Report.	241
Download a Report.	242
Delete a Report.	243
About Scheduled Reports.	245
Create a Reporting Schedule.	245
View a Reporting Schedule.	247
Modify a Reporting Schedule.	247
Delete a Reporting Schedule.	248
Chapter 13 Manage Statistics Trending	
About LUN Statistics and Trending.	249
About LUN Statistics.	250
View LUN Statistics.	251
About LUN Statistics Trending Charts.	251
Configure a LUN Statistics Trending Chart.	254

About SAN Slammer Statistics and Trending.	256
About SAN Slammer Statistics.	257
View SAN Slammer Statistics.	258
About SAN Slammer Statistics Trending Charts.	258
Configure a SAN Slammer Statistics Trending Chart.	260
Create a Chart Threshold.	262
Export a Trending Chart.	264
Print a Trending Chart.	265
Chapter 14 Managing Multiple Pillar Axiom Systems	
About Pillar Axiom MaxMan.	266
Run the Pillar Axiom MaxMan GUI Application.	268
Add Systems to the Monitored List.	269
Remove Systems From the Monitored List.	270
Manage a Specific Pillar Axiom System.	271
About Managing Configuration Files.	272
Create a Configuration File.	272
Open a Configuration File.	273
Modify a Configuration File.	274
Appendix A GUI Field Definitions	
Pillar Axiom System Limits.	275
Appendix B Configure Tab Reference Pages	
Administrator Accounts Overview Page.	280
Associate Hosts Dialog.	282
Create SAN Clone LUN, Quality of Service Tab.	284
Create SAN Clone LUN, Mapping Tab.	288
Create SAN Clone LUN, Data Protection Tab.	291
Copy SAN LUN, Quality of Service Tab.	293
Copy SAN LUN, Mapping Tab.	298
Copy SAN LUN, Data Protection Tab.	301
Create Administrator Account Dialog.	304
Create Job Schedule Dialog.	306
Create LUN Map Dialog.	308
Create SAN LUN, Quality of Service Tab.	309
Create SAN LUN, Mapping Tab.	314
Create SAN LUN, Data Protection Tab.	317
Create SNMP Host Dialog.	320
Global Settings Overview Page.	322

Groups Overview Page.	324
Host to LUN Mapping Overview Page.	325
LUN to Host Mapping Overview Page.	327
Manage SAN Host Groups, Groups Tab.	328
Manage SAN Host Groups, Hosts Tab.	329
Manage Storage Domains, Bricks Tab.	330
Manage Storage Domains, Storage Domains Tab.	332
Manage Storage Domains, Volumes Tab.	334
Manage Storage Profiles Dialog.	336
Manage Storage Profiles Overview Page.	342
Manage Volume Groups, Volume Groups Tab.	344
Manage Volume Groups, Volumes Tab.	346
Manage Volume Groups Dialog.	348
Modify Administrator Account Dialog.	350
Modify Asset Information Dialog.	352
Modify Host, Advanced Tab.	353
Modify Host, Pillar Axiom Path Manager Tab.	354
Modify Host, iSCSI Access Tab.	356
Modify Host, Ports Tab.	358
Modify iSCSI Port Settings Dialog.	360
Modify Job Schedule Dialog.	362
Modify LUN Number Dialog.	363
Modify Network Settings, Interfaces Tab.	364
Modify Network Settings, iSCSI Tab.	366
Modify Network Settings, Notification Tab.	370
Modify SAN LUN, Quality of Service Tab.	375
Modify SAN LUN, Mapping Tab.	380
Modify SAN LUN, Data Protection Tab.	383
Modify Security Settings Dialog.	386
Modify SNMP Host Dialog.	387
Modify System Time Dialog.	389
Networking Overview Page.	390
SAN Hosts Overview Page.	393
SAN LUNs Overview Page.	395
SAN Slammer Ports Overview Page.	399
SAN Storage Overview Page.	402
Security Settings Overview Page.	403
SNMP Hosts Overview Page.	404

Storage Domains Overview Page.	405
Storage Overview Page.	408
Usage Overview Page.	409
Summary Overview Page.	410
System Summary Page.	411
System Time Overview Page.	413
View Account Dialog.	414
View Host, Advanced Tab.	416
View Host, Pillar Axiom Path Manager Tab.	417
View Host, iSCSI Access Tab.	419
View Host, Ports Tab.	420
View SAN LUN, Quality of Service Tab.	422
View SAN LUN, Mapping Tab.	427
View SAN LUN, Data Protection Tab.	430
View SNMP Host Dialog.	433
Volume Groups Overview Page.	434

Appendix C Monitor Tab Reference Pages

Accept Brick Dialog.	437
Bricks Overview Page.	438
Configure Trending Chart, Chart Threshold Tabs.	441
Configure Trending Chart, Chart Thresholds Tab (LUNs).	441
Configure Trending Chart, Chart Thresholds Tab (Slammers).	442
Configure Trending Chart, Data Filtering Tabs.	445
Configure Trending Chart, Data Filtering Tab (LUNs).	445
Configure Trending Chart, Data Filtering Tab (Slammers).	445
Configure Trending Chart, Trend Configuration Tabs.	447
Configure Trending Chart, Trend Configuration Tab (LUNs).	447
Configure Trending Chart, Trend Configuration Tab (Slammers).	448
Create Chart Threshold Dialogs.	450
Create Chart Threshold Dialog (LUNs).	450
Create Chart Threshold Dialog (Slammers).	452
Create Event Notification Dialog.	454
Create Reporting Schedule Dialog.	456
Download Report Dialog.	458
Event Log Overview Page.	459
Event Notification Overview Page.	461
Events Properties Dialog.	462
Export Dialog.	464

Generate Report Dialog.	465
Generated Reports Overview Page.	466
Hardware Overview Page.	467
LUN Statistics and Trending Overview Page.	468
Manage System Alert Dialog.	470
Modify Brick, Components Tab.	471
Modify Brick, I/O Ports Tab.	473
Modify Scheduled Job Dialog.	475
Modify Event Notification Dialog.	477
Modify Reporting Schedule Dialog.	479
Modify Slammer, Components tab.	481
Modify Slammer, I/O Ports Tab.	483
Pilot Overview Page.	486
Reporting Overview Page.	487
Reporting Schedules Overview Page.	488
SAN Slammer Protocol Statistics and Trending Overview Page.	490
SAN Statistics and Trending Overview Page.	492
Scheduled Jobs Overview Page.	493
Set Event Log Filter Dialog.	494
Slammers Overview Page.	496
Statistics and Trending Overview Page.	498
Statistics Trending Dialogs.	499
LUN Statistics Trending Dialog.	499
Slammer Statistics Trending Dialog.	499
Summary of System Status Overview Page.	501
System Alerts Overview Page.	504
System Event Severities.	505
View Brick, Components Tab.	506
View Brick, I/O Ports Tab.	508
View Scheduled Job Dialog.	510
View Details Dialog (LUNs).	512
View Details Dialog (FC Slammers).	515
View Details Dialog (iSCSI Slammers).	519
View Event Notification Dialog.	524
View Reporting Schedule Dialog.	525
View Slammer, Components Tab.	526
View Slammer, I/O Ports Tab.	528
Uninterruptible Power Supplies Overview Page.	531

Create UPS Dialog.	533
Modify UPS Dialog.	534
View UPS Dialog.	536
Appendix D Protect Tab Reference Pages	
Data Protection Overview Page.	538
Protection Schedules Overview Page.	539
Create Data Protection Schedule Dialog.	540
Modify Data Protection Schedule Dialog (Protect tab).	542
View Data Protection Schedule Dialog.	544
SAN LUN Protection Overview Page.	546
Replication Engines Overview Page.	550
Appendix E Support Tab Reference Pages	
Add RAID Controller to Clear History Dialog.	551
Create Log Bundle Dialog.	552
Data Consistency Overview Page.	554
Delete Log Bundles Dialog.	555
Drive Firmware Overview Page.	556
Manage Halt Points Dialog.	557
Reset System Dialog.	558
Software Modules Page.	559
System Halt Points Overview Page.	562
System Logs Overview Page.	563
System Trouble Overview Page.	564
Test Connectivity Dialog.	565
Tools Overview Page.	566
Run PITMAN Diagnostics Dialog.	567
Update Software, Details Tab.	573
Update Software, Schedule Tab.	575
Upgrade Paths from Installed Package Dialog.	576
Upgrade Paths to Staged Package Dialog.	577
Utilities Overview Page.	578
Virtual Disk Service (VDS) Page.	580
Volume Shadow Copy Service (VSS) Page.	581
Appendix F Pillar Axiom MaxMan	
Manage the List of Axiom Systems Dialog.	582
Configuration Tab Reference Pages.	583
Storage Overview Page.	583

SAN Storage Overview Page.	583
SAN LUNs Overview Page.	584
SAN Hosts Overview Page.	587
Replication Engines Overview Page.	588
Software Modules Page.	589
Administrator Accounts Overview Page.	591
Health Tab Reference Pages.	593
Alerts and Events Overview Page.	593
Axioms Overview Page.	593
Bricks Overview Page.	596
Event Notification Overview Page.	597
Generated Reports Overview Page.	598
Hardware Overview Page.	599
Pilot Overview Page.	600
Recent Events Overview Page.	601
LUN Statistics and Trending Overview Page.	602
SAN Slammer Protocol Statistics and Trending Overview Page.	604
SAN Statistics and Trending Overview Page.	605
Scheduled Jobs Overview Page.	606
Slammers Overview Page.	607
Statistics and Trending Overview Page.	608
System Alerts Overview Page.	608
Uninterruptible Power Supplies Overview Page.	609
Index.	611

List of Figures

Figure 1 Pillar Axiom Storage Services Manager GUI. 22

Figure 2 Pillar Axiom Storage Services Manager log in screen. 32

Figure 3 Pillar Axiom Storage Services Manager status bar 33

Figure 4 Usage summary. 65

Figure 5 Default volume group example. 67

Figure 6 Nested volume groups. 68

Figure 7 Storage Domains, volume groups, and volumes. 75

Figure 8 Brick console. 227

List of Tables

Table 1 Oracle resources.	20
Table 2 Typography to mark certain content.	20
Table 3 Pillar Axiom software and system information.	24
Table 4 Default login values.	30
Table 5 Status bar details.	33
Table 6 Effect of Storage Domains on storage availability.	83
Table 7 Optimum number of RAID groups for best performance.	95
Table 8 Effects of access and I/O bias.	97
Table 9 Backup Storage Profiles.	101
Table 10 MSSQL Storage Profiles.	102
Table 11 MSXchg Storage Profiles.	102
Table 12 OracleDB Storage Profiles.	103
Table 13 OracleUCM Storage Profiles.	104
Table 14 Xen Storage Profiles.	104
Table 15 Pillar Axiom MaxRep Storage Profiles.	105
Table 16 Other Storage Profiles.	105
Table 17 NIM port status.	112
Table 18 Effect of Storage Domains on storage availability.	115
Table 19 Capacity usage by online data replicas.	149
Table 20 Effect of Storage Domains on Brick additions.	185
Table 21 Event severity and category selection.	199

Table 22 SAN Slammer commands.	223
Table 23 Report download formats.	241
Table 24 System operating limits.	275
Table 25 Field input limits.	277
Table 26 Job schedule recurrence intervals.	307
Table 27 Pillar Axiom event severities.	505
Table 28 Job schedule recurrence intervals.	543
Table 29 Software module types.	559
Table 30 PITMAN commands.	567
Table 31 Software module types.	590

Preface

Related Documentation

Information resources for all Pillar Axiom systems

- *Pillar Axiom Customer Release Notes*
- *Pillar Axiom Glossary*
- *Pillar Axiom System Architecture Overview*
- *Pillar Axiom CLI Reference Guide*
- *Pillar Axiom SMIPProvider Reference*
- *Pillar Axiom Implementation Tips for Link Aggregation*
- *Pillar Axiom Statistics Tools User Guide*
- *Pillar Axiom Hardware Installation Guide* for these platforms:
 - Pillar Axiom 300
 - Pillar Axiom 500
 - Pillar Axiom 600
- *Pillar Axiom Service Guide* for these platforms:
 - Pillar Axiom 300
 - Pillar Axiom 500
 - Pillar Axiom 600

Additional information resources for SAN systems

- *Pillar Axiom MaxRep for SAN User's Guide*
- *Pillar Axiom MaxRep for SAN Hardware Guide*
- *Pillar Axiom iSCSI Integration Guide for Windows Platforms*
- *Pillar Axiom Oracle Integration Guide*

Oracle Contacts

Table 1 Oracle resources

For help with...	Contact...
Support	https://support.oracle.com
Training	https://education.oracle.com
Documentation	<ul style="list-style-type: none">• 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 <i>system-name-ip</i> 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

Typographical Conventions

Table 2 Typography to mark certain content

Convention	Meaning
<i>italics</i>	Within normal text, words in italics indicate: <ul style="list-style-type: none">• A reference to a book title.• New terms and emphasized words.

Table 2 Typography to mark certain content (continued)

Convention	Meaning
	<ul style="list-style-type: none">• Command variables.
<code>monospace</code>	Indicates one of the following, depending on the context: <ul style="list-style-type: none">• The name of a file or the path to the file.• <i>Output</i> displayed by the system on the command line.
monospace (bold)	<i>Input</i> 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 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.

CHAPTER 1

Welcome to Pillar Axiom 600 Administration

About Pillar Axiom Storage Services Manager

The Pillar Axiom Storage Services Manager eliminates the complexity of provisioning tiered storage. For example, the graphical user interface (GUI) allows you to select the appropriate application profile to provision and tune the storage easily.

You can access the Pillar Axiom Storage Services Manager through its GUI.

Figure 1 Pillar Axiom Storage Services Manager GUI



Using the storage attributes you provide through the GUI, the Pillar Axiom Storage Services Manager implements predictive application performance characteristics before it physically provisions the storage. This feature puts you in control of resource allocation.

The Pilot policy controller is the management interface for the Pillar Axiom system. The simple, graphical management console and the Pillar Axiom software implemented in the Pillar Axiom system enables policy-based provisioning with the following characteristics:

- Dynamic performance prioritization

- Fault management
- Guided Maintenance

The storage management user interface is intuitive and allows you to deploy, provision, manage, and maintain a Pillar Axiom system easily without special training.

Note: As a companion product, the Pillar Axiom CLI can be used as well to manage a Pillar Axiom system. For information on how to use that product, refer to the *Pillar Axiom CLI Reference Guide*.

Related concepts

- [About Accessing Pillar Axiom 600 Applications](#)
- [About Accessing the Pillar Axiom System](#)

About Accessing Pillar Axiom 600 Applications

You can download the graphical user interface (GUI) for the Pillar Axiom Storage Services Manager and various utility software and access some limited information about the operation of the Pillar Axiom system. You can access these objects from the web client that is available on the Pilot policy controller.

A username and password are not necessary to access the Pillar Axiom system web pages.

The following table summarizes the type of content that is available from the management controller web pages.

Table 3 Pillar Axiom software and system information

Category	Description
Pillar Axiom Storage Services Manager graphical user interface (GUI) applications	<p>Provides links to the installation files for the Pillar Axiom Storage Services Manager and Pillar Axiom MaxMan applications.</p> <p>The GUI applications are available in the following formats:</p> <ul style="list-style-type: none">• Windows Installer: Provides the download link for the Windows installer in MSI format.• JAR and Run Scripts: Provides the download links to the self-contained JAR (Java archive) file and scripts in Zip and Tar archive formats.
Technical Documentation	<p>Provides links to the Pillar Axiom Storage Services Manager technical documentation in Adobe portable document format (PDF) format.</p>
Utilities	<p>Provides links to the following downloads:</p> <ul style="list-style-type: none">• Pillar Axiom Command Line Interface (CLI)• Pillar Axiom Virtual Disk Service Provider (VDS Provider)• Pillar Axiom Volume Shadow Copy Service Provider (VSS Provider)• Pillar Axiom Small Network Management Protocol (SNMP) management information base (MIB) text file• Pillar Axiom Statistics Tools
Recent System Alerts and Events	<p>Provides a list of system alerts that require administrator action and a list of the last 20 system events.</p>

Table 3 Pillar Axiom software and system information (continued)

Category	Description
System Information and Status	Provides a summary of the Pillar Axiom system information and status.

Note: The web page configuration provided by the web server on the Pilot is simple HTML. As such, content can be downloaded to a mobile device. For example, you can check at any time for system alerts and the system status on a mobile device wherever you are.

The Pillar Axiom Storage Services Manager GUI is supported on the following platforms:

Windows	Windows XP Windows Vista Windows 7 Windows Server 2003 Windows Server 2008
Linux	Fedora Core Ubuntu Oracle Enterprise Linux 5.x Oracle Enterprise Linux 6.x Red Hat Enterprise Linux 5
Solaris	Solaris 10 SPARC Solaris 10 x86, 64-bit

Linux and Windows platforms require Java version 1.6.0 or higher. MacIntosh platforms require Java version 1.6.0_24.

Note: For Windows, the MSI installer does not require that Java be installed.

Related concepts

- [About Client Application Download Formats](#)

Related tasks

- [Download the GUI Application](#)
- [Install the GUI Application Archive File](#)
- [Install the GUI Application with Windows Installer](#)

About Client Application Download Formats

The client application packages are available in a variety of formats for both Microsoft Windows and Linux operating systems. For archived file formats, you must decompress the files to your workstation before you can begin the installation.

Select from the following file formats:

- msi** Specifies a Microsoft Windows installer file. Use this file type to launch the software installation in automatic mode. Your environments might not allow automatic software installation.
- zip** Specifies a compressed archive file used in a Windows environment. Use this file type to decompress the files into a workstation folder for manual installation.
- tar** Specifies a non-compressed tape file archive method used in a Linux environment. Use this file type to extract the files into a workstation folder for manual installation.
- tgz** Specifies a compressed tape file archive method used in a Linux environment. Use this file type to decompress and extract the files into a workstation folder for manual installation.
- txt** Specifies a text file used in any operating system environment. This type of file is not compressed and usually contains configuration details, or other information.

Download the GUI Application

The software for the Pillar Axiom 600 graphical user interface (GUI) is available on the Pilot management controller, which is accessed from a web browser.

- 1 Start a web browser from your workstation.
- 2 In the address field, specify your Pillar Axiom system.

Valid address options:

- IP address of the Pilot management controller

- Name of the Pillar Axiom system if DNS name resolution is available
- 3 Click **Pillar Axiom Storage Services Manager GUI Applications**.
 - 4 Select a link for the software you want to download.
 - 5 Save the file to your client workstation.

In the next steps you will do one of the following:

- Uncompress the archived files
- Start the installation, if you selected an automatic installation file format

Related concepts

- [About Accessing Pillar Axiom 600 Applications](#)

Related tasks

- [Install the GUI Application Archive File](#)
- [Install the GUI Application with Windows Installer](#)

Install the GUI Application with Windows Installer

After you download the Windows installer for the Pillar Axiom Storage Services Manager graphical user interface (GUI), you need to install the files onto the workstation. Run the Microsoft Windows installation package to install the product on the workstation.

Note: Verify that you are allowed to run an automatic installation.

- 1 Locate the client software file on the workstation. For an automatic installation, the file extension is `.msi`.
- 2 Double-click the file to begin the installation.
- 3 Follow the instructions for the installation.

Result:

When the installation is complete, the following objects are created:

**Pillar Axiom Storage
Manager**

A shortcut on the Windows desktop to run the Pillar Axiom Storage Services Manager.

**c:\Program Files
\Oracle Corporation**

A directory to store all the files necessary to run the Pillar Axiom Storage Services Manager or the Pillar Axiom MaxMan application.

Related concepts

- [About Client Application Download Formats](#)
- [About Accessing Pillar Axiom 600 Applications](#)

Related tasks

- [Download the GUI Application](#)
- [Run the Pillar Axiom MaxMan GUI Application](#)
- [Log In to the GUI](#)

Install the GUI Application Archive File

After you download the graphical user interface (GUI) application archive for the Pillar Axiom 600 storage system, extract the files to a workstation before using the software. The archive contains a self-contained JAR (Java archive) file and scripts to run the Pillar Axiom Storage Services Manager and Pillar Axiom MaxMan applications.

- 1 Locate the client software archive file on the workstation.
- 2 Extract the contents of the archive file to a directory of your choosing on the client host where you expect to be using the software.
 - For Windows, use a zip utility to extract the files.
 - For Linux, use `tar` to extract the files.

Result:

The following objects are created:

- `pds-axiomgui-selfContainedJar.jar`

The client executable for the Pillar Axiom Storage Services Manager and the Pillar Axiom MaxMan applications.

- `pillar_eula_text.rtf`

The Pillar Data Systems end user license agreement.

- `runPillarAxiomStorageManager.bat`

(Windows only) The client batch file to run the Pillar Axiom Storage Services Manager application.

- `runPillarAxiomStorageManager.sh`

(Linux only) The client shell file to run the Pillar Axiom Storage Services Manager application.

- `runPillarAxiomMaxMan.bat`

(Windows only) The client batch file to run the Pillar Axiom MaxMan application.

- `runPillarAxiomMaxMan.sh`

(Linux only) The client shell file to run the Pillar Axiom MaxMan application.

- 3 (Optional) Add the directory where you extracted the contents of the archive files to your PATH environment variable so that you can run the executable from any directory on your system.

Example:

Assuming the archive was extracted to a root directory named `AxiomGUI`, the following examples illustrate how to add that directory to the PATH variable.

Linux `% export PATH=${PATH}:/AxiomGUI`

Windows `C:\ set PATH=%PATH%;\AxiomGUI`

Tip: To make this change permanent, edit the PATH variable by navigating to **My Computer > Properties > Advanced > Environment Variables**.

Related concepts

- [About Accessing Pillar Axiom 600 Applications](#)
- [About Client Application Download Formats](#)

Related tasks

- [Download the GUI Application](#)
- [Log In to the GUI](#)
- [Run the Pillar Axiom MaxMan GUI Application](#)

About Accessing the Pillar Axiom System

After you have installed the Pillar Axiom Storage Services Manager software package on a client workstation, you can run the application to access a Pillar Axiom system.

The first time that you use the Primary administrator account to log in to the graphical user interface (GUI), use the following default values:

Table 4 Default login values

Field	Default value
Pilot IP address	10.0.0.2
Login Name	administrator
Password	pillar

To login to the GUI application, use one of the following options:

- For a newly installed Pillar Axiom system in which the Pilot IP address has not been changed, use an address of 10.0.0.2, which was set at the factory. Typically, this address is what you also used to download the GUI application.
- If the Pilot IP address has been changed to a customer-specific address, use that address.

Alternatively, if you configured the IP address to a DNS host name, you can use that host name to log into the Pillar Axiom system.

If you forget the Primary system administrator password, you can reset it in these ways:

Tip: If you forget the Primary system administrator password, you can reset it using either of these two methods:

- Use a Type 1 Administrator account, if one exists, to reset the password. A support administrator cannot reset the Primary system administrator password.
- Contact the Oracle Pillar Customer Support for the encrypted file (for resetting the password). The Oracle Pillar Customer Support will send you the encrypted file and give you instructions on how to install the file.

After logging in to the Pillar Axiom system, you can perform administrator tasks. At any given time, the following number of administrator sessions can be active:

- 5 active sessions for each administrator account
- 25 total at any given time

Note: The default time-out period is 20 minutes. When a session is inactive for more than the time-out period, the system terminates that session.

Related concepts

- [About Accessing Pillar Axiom 600 Applications](#)

Related references

- [Modify Security Settings Dialog](#)

Related tasks

- [Log In to the GUI](#)
- [Log Out of the GUI](#)
- [Modify Security Settings](#)

Log In to the GUI

Using the Pillar Axiom Storage Services Manager graphical user interface (GUI), you can access the Pillar Axiom 600 system to perform administrative tasks such as provisioning and tuning your storage.

Prerequisites:

The Pillar Axiom Storage Services Manager software package has been installed on your client workstation.

- 1 Launch the Pillar Axiom Storage Services Manager application.
 - For the Windows executable, double-click `C:\Program Files\Oracle Corporation\Pillar Axiom Storage Services Manager.exe`.
 - For the Windows archive, run the `runPillarAxiomStorageManager.bat` batch script.
 - For Linux, run the `runPillarAxiomStorageManager.sh` shell script.

Result:

The login screen appears:

Figure 2 Pillar Axiom Storage Services Manager log in screen



- 2 For **Axiom name**, specify the Pillar Axiom system to which you want to connect.

Valid values:

- IP address of the Pilot management controller.
- Name of the Pillar Axiom system as configured in your site naming services for the Pilot.

- 3 For **Login name**, enter your login name.
- 4 For **Password**, enter your password.
- 5 Click **Login**.

Result:

The GUI opens to the Asset Information overview page, or the last page you visited when you last logged off.

Related concepts

- [About Pillar Axiom Storage Services Manager](#)
- [About Client Application Download Formats](#)
- [About Accessing Pillar Axiom 600 Applications](#)

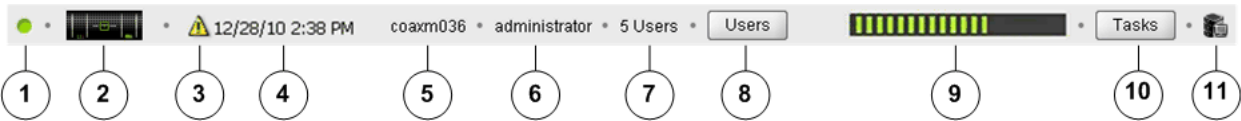
Related tasks

- [Install the GUI Application with Windows Installer](#)
- [Install the GUI Application Archive File](#)
- [Log Out of the GUI](#)

Status Bar Description

In addition to context-sensitive help, the Pillar Axiom Storage Services Manager GUI makes readily available certain vital information about the operation of the Pillar Axiom system. This information is displayed in the status bar at the bottom of each overview window.

Figure 3 Pillar Axiom Storage Services Manager status bar



Legend	1 System status	7 Number of administrators
	2 Hardware status	8 Display all administrators
	3 System alert	9 Progress of current background task
	4 Last system alert	10 Display all background tasks
	5 System name	11 Display Pillar Axiom system communications
	6 Current administrator	

Table 5 Status bar details

Status bar component	Description
System status	Displays the overall system status. A status of Normal (green) requires no action. If, however, the status is Warning (yellow) or Critical (red), click the icon to view the System Summary page to identify the cause of the status.
Hardware status	Displays the overall system status of the hardware components. A status of Normal (uncolored) requires no action. If, however, the status is Warning (yellow) or Critical (red), to view the Hardware overview page so the cause of the status can be identified, click this icon.

Table 5 Status bar details (continued)

Status bar component	Description
System alert	To open the System Alerts overview page and to respond to any events that require intervention, click this icon. The icon displays when an active system alert is present on the Pillar Axiom system.
Last system alert	Displays the date and time of the last system alert that occurred on the system. This information lets you know, especially when multiple events exist, whether a new system alert has been generated. The date and time displays when an active system alert is present on the Pillar Axiom system.
System name	Displays the system name.
Current administrator	Displays the name of the administrator account that is currently logged in to the system.
Number of administrators	Displays the number of administrator accounts currently logged in to the system.
Display all administrators	Click this icon to open the Current User Session dialog and to view details of the administrators who are currently logged in to the system.
Progress of current background task	Displays the progress of the currently running task.
Display all background tasks	Click this icon to open the Background Processes dialog. From this dialog, you can also open the View Axiom Communication Details dialog (see below).
Display Pillar Axiom system communications	Click this icon to open the View Axiom Communication Details dialog. The details include: <ul style="list-style-type: none"> Recent and pending action requests Action request historical log

Related concepts

- [About Responding to System Alerts](#)

Configure Automatic Screen Updates

You can disable automatic screen refresh if your Pillar Axiom system takes a long time to refresh the screen contents.

If you have a very large system configuration or a large configuration that experiences heavy activity, the system might take a few minutes to refresh the screen contents. This delay might interrupt normal operations on the system. You can disable the automatic screen refresh and manually update the screen contents, as necessary.

- 1 From the menu bar, choose **Tools > Configure Automatic Screen Updates**.
- 2 Select the option to enable or disable automatic screen updates.

Valid options:

- **Enable Automatic Screen Updates**
- **Disable Automatic Screen Updates**

Tip: To refresh the screen when the automatic updates is disabled, enter Ctrl-Alt-R from your keyboard.

Log Out of the GUI

When you have completed your administrative tasks, log out from the Pillar Axiom Storage Services Manager. If you do not log out, the following situation might arise:

- An unauthorized user may gain access to the Pillar Axiom system from your workstation.
- One login session is tied up unnecessarily until your session is automatically logged out when the inactivity time limit is reached.

To log out, choose one of the following menu items:

Axiom > Log off Disconnects from the current Pillar Axiom system, allowing you to log in to another system.

Axiom > Exit Disconnects from the current Pillar Axiom system and closes the Pillar Axiom Storage Services Manager application.

Related concepts

- [*About Accessing the Pillar Axiom System*](#)

Related tasks

- [*Log In to the GUI*](#)

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 600 storage system:

- Pillar Axiom SecureWORMfs - System Perpetual
- Pillar Axiom Storage Domains - System Perpetual
- Pillar Axiom Copy Services Bundle - System Perpetual
- Pillar Axiom MaxRep Replication for NAS - Terabyte Perpetual

The following features are currently licensed on the 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

CHAPTER 2

Manage Global Settings

About Global Settings Configuration

The first time you log into the Pillar Axiom system you should perform several tasks to configure your system.

The following list summarizes the tasks to configure the system-wide settings:

- Set and synchronize the time across all Pillar Axiom components.
- Enable and configure Dynamic Host Configuration Protocol (DHCP) support and transmission characteristics of the management ports.
- Set system-wide iSCSI settings if your configuration requires all iSCSI connections to use CHAP, Access Control, or both. If access control is defined for each initiator, you do not need to configure iSCSI at the system level.
- Define an electronic mail server in your network that receives Pillar Axiom alerts and forwards them to administrator email accounts.
- Enable Call-Home, a feature that notifies Pillar Data Systems about issues in the system.
- Define time-out periods and failed login attempts.

The success of other configuration tasks depends on the system-wide settings. For example, if you do not configure the email server, the system cannot send alerts.

Related tasks

- [*Modify the Pillar Axiom System Time*](#)
- [*Configure the Management Interface*](#)
- [*Configure iSCSI System Settings*](#)
- [*Configure Email Notification Settings*](#)
- [*Configure Call-Home Settings*](#)
- [*Modify Security Settings*](#)

Modify the Pillar Axiom System Time

Configure the Pillar Axiom system time so that event and logging timestamps are accurate and time-dependent applications, such as email, work properly.

- 1 From the **Configure** tab, click **Global Settings > System Time**.
- 2 Choose **Actions > Modify System Time**.
- 3 Choose the method for configuring the system time:
 - **Use Internal Hardware Clock:** Allows you to set the system time manually.
 - **Use External Time Source:** Synchronizes the system time with an external NTP server.

Important! Do not attempt to use a Windows system as an NTP server unless that system has a third party NTP service such as Meissner installed.

Note: If the primary NTP server is not available, the Pillar Axiom system consults the secondary servers in round-robin fashion until a connection is made.
- 4 Depending on which option you selected, enter the system time manually or the NTP server details.
- 5 To save the system time setting, click **OK**.

Related references

- [Modify System Time Dialog](#)
- [System Time Overview Page](#)

Modify Asset Information

You may want to change the name of the system that is displayed in the Pillar Axiom Storage Services Manager.

- 1 From the **Configure** tab, click **Summary > System**.
- 2 Choose **Actions > Modify Asset Information**.
- 3 Enter the necessary information in any of the following fields:
 - **Name**
 - **Description**
 - **Location**
 - **Contact Name**
 - **Contact Phone**
 - **Asset Number**

Note: Pillar recommends that you enter the name and phone for more than one contact.

- 4 Click **OK** to save your changes.

Related references

- [Modify Asset Information Dialog](#)

About Network Settings

Configure the Pillar Axiom system network settings to ensure proper communication with the system.

Configuring the system network establishes communication to the following areas:

- Between the Pilot management controller and the end user data network
- To the email server, which sends alerts and notifications of system events

Related concepts

- [About the Network Interfaces](#)
- [About iSCSI Settings](#)
- [About System Notifications](#)

About the Network Interfaces

The management interface provides connectivity between the end user data network and the Pillar Axiom Pilot management controller. You can choose which method to use to assign the primary IP addresses to the management interface on the Pilot:

- Dynamic Host Configuration Protocol (DHCP), which assigns a primary IP address dynamically when the Pilot starts.
- Static IP Address assigns a permanent, primary IP address to a control unit (CU) in the Pilot as well as alternate IP addresses for the ports on the partner CU. If the management software cannot access the primary IP address, it accesses an alternate IP address.

The Call-Home feature, when enabled, allows the Pillar Axiom system to send to the Pillar Data Systems Call-Home server (callhome.support.pillardata.com) the following types of information:

- System log bundles
- System status
- System configuration information

Also, the email server can be enabled to send event notifications to a list of recipients.

To send the Call-Home information and the email messages, the names of the recipients of that information need to be resolved into IP addresses. A Domain Name Server (DNS) is used to resolve those names.

You can define a primary and a secondary DNS. The system uses the primary DNS to resolve recipient names into IP addresses. If the primary server cannot be reached when outward-bound messages are sent, the system uses the secondary DNS.

Configure the Management Interface

Configure the management interface by setting the IP addressing method (static or dynamic) for the Pilot.

Important! When providing static IP addresses for the management interface, be sure that you enter the correct addresses and that the addresses are reachable over the management network. Otherwise, you will not be able to access the system. If you enter unreachable addresses or have forgotten the addresses, contact the Oracle Pillar Customer Support to get an encrypted file that can be used to reset the IP addresses to the factory default settings.

- 1 From the **Configure** tab, click **Global Settings > Networking**.
- 2 Choose **Actions > Modify Network Settings**.
- 3 From the **Interfaces** tab, choose how you want the Pillar Axiom system to assign IP addresses:
 - Click **Enable DHCP** if your system assigns IP addresses automatically using a Dynamic Host Configuration Protocol.
 - Click **Static IP Address** to manually configure the IP addresses. Enter the values for the fields provided.
- 4 (Optional) Choose the **Transmit Setting**.

Note: When your Ethernet network contains an auto-negotiation feature, leave this option at the default setting, **Auto**.
- 5 To save your changes, click **OK**.

Related references

- [Modify Network Settings, Interfaces Tab](#)

Related tasks

- [Create an Event Notification](#)
- [Configure DNS Settings](#)

Configure DNS Settings

You can set the primary and secondary Domain Name Server (DNS) to resolve email addresses to IP addresses. The DNS settings allow the Pillar Axiom system to send Call-Home configuration information and event notifications to designated email recipients.

- 1 From the **Configure** tab, click **Global Settings > Networking**.
- 2 Choose **Actions > Modify Network Settings**.
- 3 From the **Interfaces** tab, enter the **Primary DNS Server IP** address.
- 4 Enter the **Secondary DNS Server IP** address.
- 5 To save your changes, click **OK**.

Related concepts

- [About the Network Interfaces](#)

Related references

- [Modify Network Settings, Interfaces Tab](#)

Related tasks

- [Configure the Management Interface](#)

About System Notifications

The Pillar Axiom system provides various methods of setting up system notifications, including:

- **Event Notifications**

A Simple Mail Transfer Protocol (SMTP) email message that notifies recipients of specified system events. System events include informational, warning, or critical events such as the creation of a logical volume or the occurrence of a hardware or software problem. Event notifications are optional and supplement normal event logging and Call-Home notification. (Formerly called an *alert*).

- **System Alerts**

These resources are notifications that the Pillar Axiom generates to identify conditions that warrant investigation *and* action.

System Alerts include, for example:

- Notifications about resources that are not fully operational, indicating a need for maintenance.
- Notifications about storage running low, indicating a need for reallocation or cleanup of resources or possibly the purchase of additional storage. This kind of information is important when an administrator has implemented thin provisioning.

- **Call-Home**

A feature of a Pillar Axiom system that, when enabled, allows the system to notify Oracle Pillar Customer Support of critical issues specific to a Pillar Axiom system. No customer data is transmitted. Call-Home transfers files over the Internet using one of the following user-selected methods:

- SCP: Uses the secure copy (SCP) method with 1024-bit encryption and secure keys.
- HTTPS: Uses the Hypertext Transfer Protocol Secure method by sending files directly to Pillar or through a proxy server for security purposes. This method can also be used when the Pillar Axiom system does not have direct access to the Internet.

You must define an email server to receive alerts and event notifications and to send email messages to designated recipients.

Pillar Axiom systems also support the following protocols for monitoring the configuration of various system components:

- **Storage Management Initiative Specification (SMI-S).**

A storage management standard developed by Storage Networking Industry Association (SNIA) that allows multivendor software support of heterogeneous storage devices. Through SMI-S profiles, administrators can query, for example, device credentials, copy services, masking and mapping of Fibre Channel ports, and so forth.

- **Simple Network Management Protocol (SNMP).**

A standard network protocol that is used to monitor Slammers, Bricks, and the drives within the Bricks. Through SNMP traps, administrators can monitor, for example, central processing unit (CPU) temperature and field replaceable unit (FRU) removal and insertion.

Configure Email Notification Settings

Configuring email notifications allows system administrators to receive messages from the Pillar Axiom system.

- 1 From the **Configure** tab, click **Global Settings > Networking**.
- 2 Choose **Actions > Modify Network Settings**.
- 3 From the **Notification** tab, select the option **Enable Email Notifications** located in the Email Notification area.
- 4 Enter the configuration settings for the email server.
- 5 To save your changes, click **OK**.

Related references

- [Modify Network Settings, Notification Tab](#)

About Managing Call-Home Settings

Manages the Call-Home settings on a Pillar Axiom system and notifies the Oracle Pillar Customer Support of status and configuration information or any issues.

Call-Home is a feature that, when enabled, allows the system to send the status and configuration information to the Oracle Pillar Customer Support; no customer data is sent. The Call-Home feature also notifies the Oracle Pillar Customer Support about issues in the Pillar Axiom system. For example, when a component operates in degraded mode or fails, the system automatically performs failover actions. Although a component failure does not cause downtime, manual intervention is sometimes required to repair or replace the failed component. The system sends a Call-Home message to initiate the repair or replacement process.

Call-Home log collection can be initiated by one of the following methods:

- **Manual:** The administrator has requested a log collection.
- **Event-triggered:** An event has triggered the Call-Home.
- **Periodic:** A specified time has elapsed since the Call-Home was triggered.

The Pillar Axiom system maintains a directory of data files, each of which captures a Call-Home session. Whenever one of these data files is overwritten or thrown away, a log entry is made noting that fact. The collection of data files represent the ten most recent Call-Home sessions. The system administrator can select a session file and download it to a client machine or send it directly to the currently targeted server. Call-Home sessions can also be sent to a local Call-Home server. Contact the Oracle Pillar Customer Support for details.

Configure Call-Home Settings

Configuring the Call-Home settings allows the Pillar Axiom system to send the event logs and messages to Pillar Data Systems.

- 1 From the **Configure** tab, click **Global Settings > Networking**.
- 2 Choose **Actions > Modify Network Settings**.
- 3 From the Notification tab Call-Home Configuration area, choose the type of server to configure to receive Call-Home notifications:
 - To configure a Pillar Axiom system, click the **Use Pillar Server** option.
 - To configure a local server, click the **Use Local Server** option.
- 4 Set the server properties as needed.
- 5 Select the **Enable large file transfers** to allow the system to send additional log files to the Call-Home server.
- 6 Enter the number of recent events to send.
- 7 To save your changes, click **OK**.

Related references

- [Modify Network Settings, Notification Tab](#)

Test Call-Home

You can confirm that the network settings are configured correctly for the Call-Home feature. This confirmation ensures that event logs can be sent to Pillar.

The system sends a Call-Home message to verify that Call-Home feature is correctly configured.

Note: Only Primary Administrator or Administrator 1 accounts are allowed to test Call-Home.

- 1 From the **Configure** tab, click **Global Settings > Networking**.
- 2 From the Network Settings overview page, choose **Actions > Test Call-Home**.
- 3 Confirm that you want to send test Call-Home information to the specified Call-Home server and click **OK**.

Note: Wait at least 10 minutes before testing Call-Home again.

Related references

- [Modify Network Settings, Notification Tab](#)

Related tasks

- [Configure Email Notification Settings](#)
- [Modify Call-Home Settings](#)

Modify Call-Home Settings

Modify the Call-Home settings when the server IP address changes or there is a change to the password used to access the server.

- 1 From the **Configure** tab, click **Global Settings > Networking**.
- 2 Choose **Actions > Modify Network Settings**.
- 3 From the **Notification** tab, update the configuration settings for the email server and Call-Home triggers.
- 4 To save your changes, click **OK**.

Related references

- [Modify Network Settings, Notification Tab](#)

About the Call-Home Matrix

The Call-Home matrix consists of the subset of Pillar Axiom system events that generate a Call-Home. The matrix also defines which logs to send to the Call-Home server.

To help them diagnose a system issue, the Oracle Pillar Customer Support might send you a file containing the Call-Home matrix. Obtain the Call-Home matrix file from Oracle Pillar Customer Support. However, only the support administrator can upload the Call-Home matrix to the system.

When uploaded to the system, the Call-Home matrix updates the software on the Pilot. If the system contains a custom Call-Home matrix, uploading a new matrix will overwrite the custom settings.

A software update also overwrites the matrix file. The support administrator might need to upload the matrix again after a software update. Contact the Oracle Pillar Customer Support for information about the matrix before you upload the file.

Upload the Call-Home Matrix

You might need to upload a custom Call-Home matrix to the Pilot. Upload the matrix to update the list of events that trigger a Call-Home or update the logs sent to the Call-Home server.

Prerequisite: You must be logged in as a support administrator to access the **Upload Call-Home Matrix** menu item.

Obtain an updated Call-Home matrix from the Oracle Pillar Customer Support.

Important! A software update overwrites the Call-Home matrix. You might need to upload the custom matrix after a software update. Contact Oracle Pillar Customer Support for information about the impact the new Call-Home matrix might have on your system.

- 1 From the **Configure** tab, click **Global Settings > Networking**.
- 2 From the Network Settings overview page, choose **Actions > Upload Call-Home Matrix**.
- 3 From the Upload Call-Home Matrix dialog, click the browse button [...] to proceed.
- 4 Navigate to and select the Call-Home matrix file that you received from the Oracle Pillar Customer Support.
- 5 Click **Open**.
- 6 From the Upload Call-Home Matrix dialog, click **OK** to upload the matrix file.

Related concepts

- [About Managing Call-Home Settings](#)
- [About the Call-Home Matrix](#)

Related references

- [Modify Network Settings, Notification Tab](#)

Related tasks

- [Configure Email Notification Settings](#)
- [Modify Call-Home Settings](#)

About iSCSI Settings

If you have iSCSI hosts configured to use Challenge Handshake Authentication Protocol (CHAP), access control, or both, you must also set up system-wide

iSCSI settings. This configures the authentication and access controls on the Pillar Axiom system in which the host must match to gain access.

If you have CHAP and access control configured for each initiator, you do not need to configure iSCSI globally.

The Internet Storage Name Service (iSNS) facilitates automated discovery, management, and configuration of iSCSI devices on a TCP/IP network. iSNS provides intelligent storage discovery and management services comparable to those found in Fibre Channel networks, allowing a commodity IP network to function in a capacity similar to that of a storage area network.

The iSNS feature expects all Pillar Axiom iSCSI ports to have access to the same primary iSNS server. This rule is necessary so that all iSCSI ports can expect the same result when querying the iSNS database for the set of initiators that are members of the Pillar Axiom Discovery Domain Set.

Important! If an iSCSI port has no access or loses access to the iSNS server, the Pillar Axiom system reports iSNS error events but continues to operate normally. For iSNS Access Control to function correctly, at least one Pillar Axiom iSCSI port must have access to the iSNS server during a restart; otherwise, all iSCSI logins are rejected.

For information on configuring the Microsoft iSNS Server, refer to the *Pillar Axiom iSCSI Integration Guide for Windows Platforms*.

Related concepts

- [About Licensing Optional Premium Features](#)

Related references

- [Modify Network Settings, iSCSI Tab](#)

Related tasks

- [Modify iSCSI Port Settings](#)

Configure iSCSI System Settings

You can set the system-wide Internet Small Computer System Interface (iSCSI) initiator ports authentication settings that applies to all iSCSI hosts.

- 1 From the **Configure** tab, click **Global Settings > Networking**.
- 2 Choose **Actions > Modify Network Settings**.
- 3 From the iSCSI tab, enter values to configure the initiator ports.
- 4 To save your changes, click **OK**.

Related concepts

- [*About Licensing Optional Premium Features*](#)

Related references

- [*Modify Network Settings, iSCSI Tab*](#)

About Modifying Administrator Account Security Settings

You can change the security settings for system administrator accounts, including:

- Set the number of consecutive failed login attempts that the Pillar Axiom system allows. When the threshold is exceeded, the system disables the account and writes an entry in the event log. Only a Primary Administrator or Administrator 1 account can re-enable the account, and the system resets the counter upon a successful login. If you do not set this value, there is no limit to the number of consecutive, unsuccessful login attempts.
- Set the session time-out so that the Pillar Axiom system terminates an administrator's session after a given period of inactivity. If you do not set this value, inactive sessions are terminated after 20 minutes.

Modify Security Settings

Configure the Pillar Axiom system security by limiting the number of failed login attempts and setting a time limit for inactive administrator login sessions.

- 1 From the **Configure** tab, click **Global Settings > Security**.
- 2 Choose **Actions > Modify Security Settings**.
- 3 To define the administrator login limits, enter the values in the failed login attempts and session time-out fields.

The session time-out value must be between 0 and 999 minutes. The default time-out is 20 minutes.

- 4 (Optional) Enter a login screen message.
- 5 To save the security settings, click **OK**.

Related concepts

- [About Creating Administrator Accounts](#)

Related references

- [Modify Security Settings Dialog](#)

About SNMP Trap Host Management

If you use Simple Network Management Protocol (SNMP) management applications to monitor network devices, you can define SNMP trap hosts to receive Pillar Axiom traps. Any workstation that has an SNMP-based management application installed on it can be a trap host.

Pillar Axiom systems support SNMP version 2c. SET operations from SNMP management applications are not supported.

A *management information base (MIB) table* is a plain text file that provides the details on all components for which Pillar provides management information.

Note: You can define event notifications as an alternative to SNMP.

Related tasks

- [Download the Pillar Axiom MIB](#)

System Components That Can Be Monitored

The Simple Network Management Protocol (SNMP) management information base (MIB) is self-documenting and lists Pillar Axiom system resources that you can monitor. Download the MIB (a text file) from the Utilities page of the Pilot management interface.

Some of the Pillar Axiom resources that a system administrator can monitor are listed below. Some of this information can be used, for example, to graph or otherwise track the trend lines of certain resources, such as that for storage space and its utilization and for I/O operations for each second (IOPS) over certain time periods.

System Alerts. These resources are notifications that the Pillar Axiom generates to identify conditions that warrant investigation *and* action.

System Alerts include, for example:

- Notifications about resources that are not fully operational, indicating a need for maintenance.
- Notifications about storage running low, indicating a need for reallocation or cleanup of resources or possibly the purchase of additional storage. This kind of information is important when an administrator has implemented thin provisioning.

Call-Home or Manual Log Collection. Querying these resources, the administrator can check:

- Time of collection
- Availability status
- Type of information contained in the logs

Running Tasks. Some tasks running in the background are normal management jobs such as scheduled clone replications, scheduled upgrades, and so forth, or are the result of some administrative action. Other tasks, however, might indicate a condition in the Pillar Axiom system worth investigating, such as:

- Pilot restarts
- System restarts
- Topology rediscovery

This category is also useful for seeing when a planned task has completed or may need recovery, such as when replicating a very large logical volume.

Scheduled Tasks. Querying this resource allows the administrator to determine which tasks are scheduled and when they are scheduled. Knowing this information can be useful in determining whether some traps or events can be expected.

Software Versions. Capturing software versions is useful in a large data center where a single SNMP management utility can keep the administrator from having to log into each Pillar Axiom system individually for the same information to determine which machines need updates or to discover whether a particular software update is complete.

Storage Usage. Monitoring short and long term trends in capacity usage helps the system administrator avoid getting a System Alerts warning that, for example, Clone LUNs are being deleted to free up capacity. Because you can over allocate logical volumes when taking advantage of the thin provisioning feature, such volumes need to be monitored and may require additional physical storage.

System Configuration. Use a central SNMP resource to view the configuration and status of the resources of multiple systems, including:

- LUNs
- Interfaces
- Clones
- LUN mapping and masking

Traps. Traps are equivalent to email-based administrator alerts and provide another means of alerting system administrators to unfavorable storage conditions, which may or may not result in a System Alert.

Create SNMP Hosts

You can configure any workstation as a simple network management protocol (SNMP) host. Set the threshold of the monitored event that will trigger a trap message to the SNMP host.

If you want to configure the SNMP server, but not receive trap messages, clear the Receive Traps option.

- 1 From the **Configure** tab, click **Global Settings > SNMP**.
- 2 Choose **Actions > Create SNMP Host**.
- 3 Enter a **Name** for the SNMP host.
- 4 Enter the values in the **Host IP** and **Community String** fields to specify where the traps are directed.

The community string must contain at least six characters.

- 5 (Optional) Select the **Receive Traps** option to enable the **Trap Port Number** field.
- 6 Enter the **Trap Port Number** value:
 - For SNMP queries, use port 161
 - For SNMP traps, use port 162
- 7 Choose the **Severity threshold**:

Informational	Requires no action for events that are information only.
Warning	Requires no immediate action for minor conditions that you can address at your convenience.
Critical	Requires prompt action to prevent system failures or offline conditions.

- 8 To save the SNMP configuration, click **OK**.

Related concepts

- [About SNMP Trap Host Management](#)

Related references

- [SNMP Hosts Overview Page](#)
- [Pillar Axiom System Limits](#)
- [Create SNMP Host Dialog](#)

Related tasks

- [Create an Event Notification](#)
- [Modify SNMP Hosts](#)
- [View SNMP Hosts](#)
- [Delete SNMP Hosts](#)

Modify SNMP Hosts

You can modify the hosts that receive Simple Network Management Protocol (SNMP) traps. You may, for example, need to modify the IP address of the trap host if you install your SNMP-based management application on a different administrative workstation.

- 1 From the **Configure** tab, click **Global Settings > SNMP**.
- 2 From the SNMP Hosts overview page, select an SNMP host to modify.
- 3 Choose **Actions > Modify SNMP Host**.
- 4 Enter values for the attributes that you want to modify.
- 5 To save the modified SNMP configuration, click **OK**.

Related concepts

- [About SNMP Trap Host Management](#)

Related references

- [SNMP Hosts Overview Page](#)
- [Modify SNMP Host Dialog](#)

Related tasks

- [Create an Event Notification](#)

Delete SNMP Hosts

You can delete a host from the Simple Network Management Protocol (SNMP) configuration. For example, you may do this after you uninstall an SNMP-based management application from someone's workstation.

- 1 From the **Configure** tab, click **Global Settings > SNMP**.
- 2 From the SNMP Hosts overview page, select an SNMP host to delete.
- 3 Choose **Actions > Delete SNMP Host**.
- 4 When prompted to confirm the deletion, click **OK** to delete the trap hosts.

Related concepts

- [About SNMP Trap Host Management](#)

Related references

- [SNMP Hosts Overview Page](#)
- [Create SNMP Host Dialog](#)

Related tasks

- [Create an Event Notification](#)

View SNMP Hosts

You can review a list of Small Network Management Protocol (SNMP) host that are configured on the Pillar Axiom system. For example, you may need to know community string that a host uses for receiving traps.

- 1 From the **Configure** tab, click **Global Settings > SNMP**.
- 2 Review the list of SNMP trap hosts and ensure that the SNMP host details are what you expect.
- 3 To view details about a specific host, select a host from the list and choose **Actions > View SNMP Host**.

Related concepts

- [About SNMP Trap Host Management](#)
- [About Licensing Optional Premium Features](#)

Related references

- [SNMP Hosts Overview Page](#)
- [View SNMP Host Dialog](#)

Related tasks

- [Create SNMP Hosts](#)
- [Modify SNMP Hosts](#)
- [Delete SNMP Hosts](#)

Download the Pillar Axiom MIB

The Simple Network Management Protocol (SNMP) management information base (MIB) table lists Pillar Axiom 600 system resources that you can monitor. The file is available on the Pilot management controller, which is accessed from a web browser.

- 1 Start a web browser from your workstation.
- 2 Specify the IP address of the Pilot management controller or the name of the Pillar Axiom system as the address to open.
- 3 Click **Utilities**.
- 4 Click **Download Pillar Axiom SNMP MIB** link.
- 5 Save the file to your client workstation.

Related concepts

- [About SNMP Trap Host Management](#)
- [About Accessing Pillar Axiom 600 Applications](#)

Related references

- [System Components That Can Be Monitored](#)

CHAPTER 3

Manage Administrator Accounts

About Creating Administrator Accounts

You can create multiple administrator accounts in a Pillar Axiom system. Additional accounts are not necessary, but they are useful if you want to delegate administrator responsibilities. For example, you might choose to create:

- One administrator account. In this way, a designated person can assume responsibility while the Primary system administrator is on vacation. Assign this account to the Administrator 1 role.

Tip: Pillar strongly recommends that you set up a Type 1 Administrator account when you install the system. Besides the Primary system administrator, only a Type 1 Administrator can modify an account password (including that of the Primary system administrator) without knowing the previous password.

- One or more administrator accounts with read-only privileges. In this way, managers can monitor the system but they cannot change configuration details. Assign these accounts to the Monitor role.

You can create any number of administrator accounts. However, only 25 account sessions can be active at any given time.

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 references

- [Create Administrator Account Dialog](#)

Related tasks

- [Modify an Administrator Account](#)
- [Delete an Administrator Account](#)

Display Administrator Account Details

You can display details about all administrator accounts or about a specific administrator account. You may want to review which accounts are disabled or have incomplete contact information.

- 1 From the **Configure** tab, click **Global Settings > Administrator Accounts**.
- 2 Review the displayed information to ensure that the account details are what you expect.

Related references

- [Administrator Accounts Overview Page](#)
- [Modify Administrator Account Dialog](#)

Related tasks

- [Create a Pillar Axiom Administrator Account](#)
- [Delete an Administrator Account](#)

About Modifying Administrator Accounts

If you delegate administrative tasks to other administrators, you might need to:

- Modify account attributes (for example, change an administrator's password or disable an account other than the Primary system administrator account).
- Change administrator account security settings.
- Delete obsolete accounts.

At times, you might need to modify the attributes of an administrator account. A Primary system administrator and people who are assigned to the Administrator 1 role can modify their own or another administrator's account.

Some changes take effect immediately. For example, an administrator's session is terminated when you disable or delete the administrator account.

Other changes affect the administrators the next time that they log in, for example, when you modify their password or modify the session time-out value.

Modify an Administrator Account

You can modify the administrator account details, such as disabling the account, changing the user password, and updating the user contact information.

- 1 From the **Configure** tab, click **Global Settings > Administrator Accounts**.
- 2 Select an account name from the Administrator Accounts list that you want to modify.
- 3 Click **Actions > Modify Account**.
- 4 Enter values for the attributes that you want to modify.

Note: You cannot disable the Primary system administrator or the Pillar Support accounts.

- 5 To save your changes, click **OK**.

Related references

- [Modify Administrator Account Dialog](#)

Related tasks

- [Create a Pillar Axiom Administrator Account](#)
- [Delete an Administrator Account](#)

Change Administrator Passwords

You can change administrator passwords if they forget their password and cannot log into the system.

- Primary system administrators and administrators who are assigned to the Administrator 1 role can change the password of any administrator account.

Tip: If you forget the Primary system administrator password, you can reset it using either of these two methods:

- Use a Type 1 Administrator account, if one exists, to reset the password. A support administrator cannot reset the Primary system administrator password.
 - Contact the Oracle Pillar Customer Support for the encrypted file (for resetting the password). The Oracle Pillar Customer Support will send you the encrypted file and give you instructions on how to install the file.
- Administrators who are assigned to the Administrator 2 or Monitor roles can change their own passwords.
- 1 From the **Configure** tab, click **Global Settings > Administrator Accounts**.
 - 2 Select an account name from the Administrator Accounts list to that you want to modify.
 - 3 Click **Actions > Modify Account**.
 - 4 Enter the new password in both fields.
 - 5 To save your changes, click **OK**.

Related references

- [Modify Administrator Account Dialog](#)

Related tasks

- [Create a Pillar Axiom Administrator Account](#)
- [Delete an Administrator Account](#)

Delete an Administrator Account

You may need to delete an administrator account, for example when someone who has an account leaves the company.

- 1 From the **Configure** tab, click **Global Settings > Administrator Accounts**.
- 2 Select an account name from the Administrator Accounts list to that you want to remove.
- 3 Click **Actions > Delete Account**.

Result:

The system displays the Delete Account dialog.

- 4 When prompted to confirm the deletion, click **OK** to delete the administrator account.

Related references

- [Administrator Accounts Overview Page](#)
- [Modify Administrator Account Dialog](#)

Related tasks

- [Create a Pillar Axiom Administrator Account](#)

CHAPTER 4

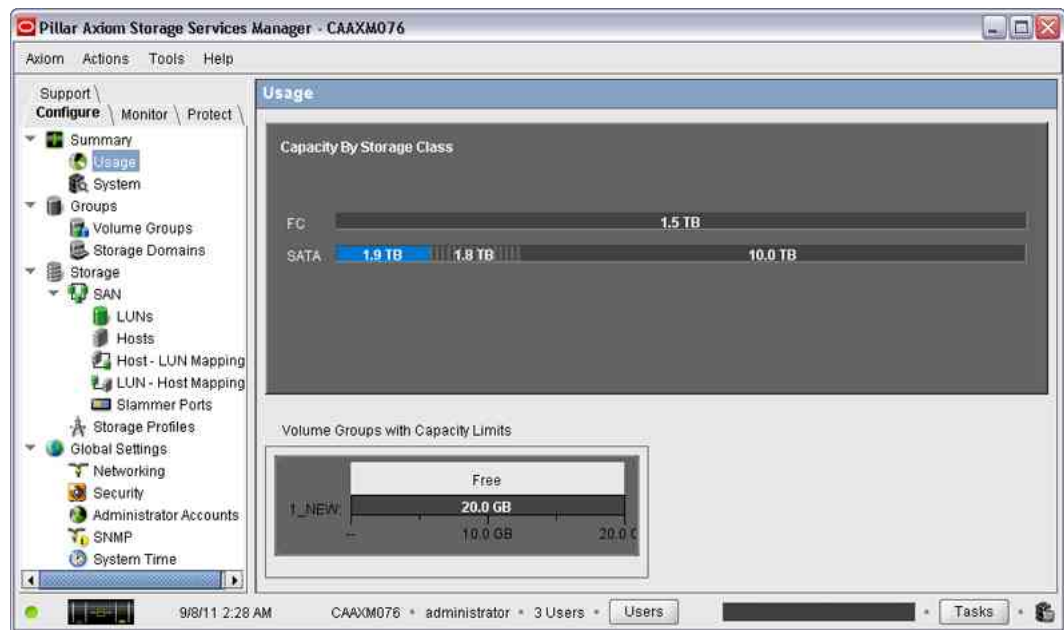
Manage Storage Groups

Display Capacity Usage

At any time, you can display the actual capacity usage of a logical volume and compare that usage to the total system capacity and assigned capacity limits.

- 1 From the **Configure** tab, click **Summary > Usage**.
- 2 Review the displayed information to ensure that the capacity usage is what you expect.

Figure 4 Usage summary



Note: A Pillar Axiom system uses binary units to calculate and display the capacity of physical storage and the size of logical volumes:

1 MB = 1024^2 (1,048,576) bytes

1 GB = 1024^3 (1,073,741,824) bytes

1 TB = 1024^4 (1,099,511,627,776) bytes

Related references

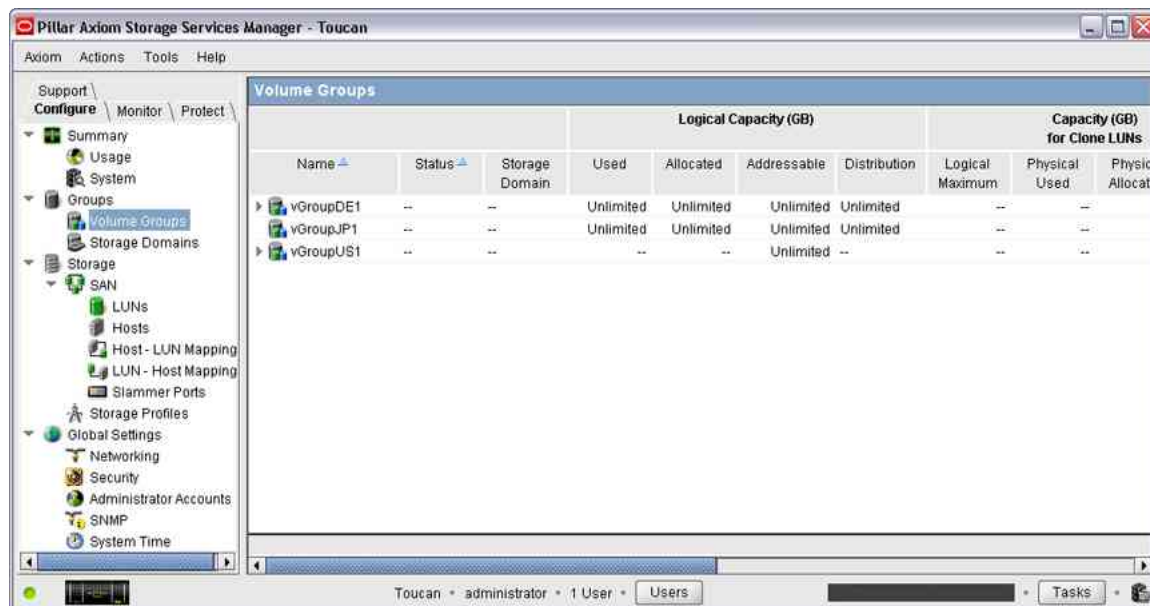
- [*Usage Overview Page*](#)

About Volume Groups

Volume groups are organizational units that can contain any grouping of logical volumes and nested volume groups.

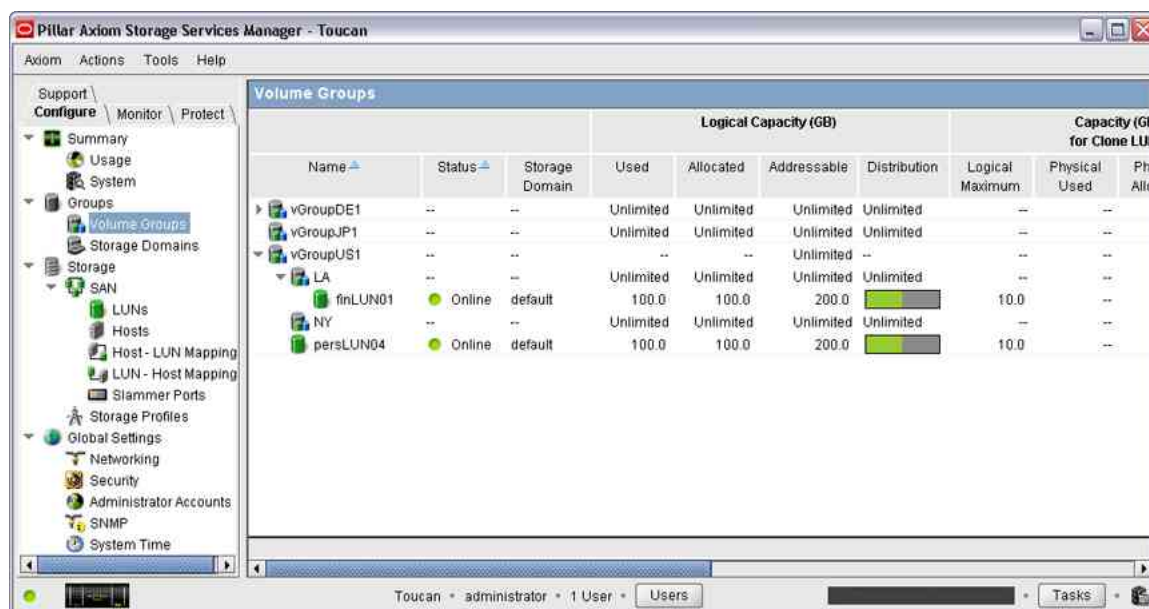
If you do not create nested volume groups, create all volumes within the nested groups to create a broad, shallow hierarchy.

Figure 5 Default volume group example



If you create nested volume groups, create the logical volume within Volumes or a nested volume group to create a narrow, deep hierarchy.

Figure 6 Nested volume groups



Related concepts

- [About Moving Logical Volumes](#)
- [About Storage Domains](#)

Related references

- [Manage Volume Groups, Volume Groups Tab](#)

Display Volume Group Details

- 1 From the **Configure** tab, click **Groups > Volume Groups**.
- 2 Review the characteristics of all available volume groups.

If desired, you can reorganize these groups, change their maximum capacities, or both.

Related tasks

- [Create Volume Groups](#)
- [Delete a Volume Group](#)
- [Modify Volume Group Attributes](#)

Create Volume Groups

Volume groups allow you to organize logical volumes into organizational units.

1 From the **Configure** tab, click **Groups > Volume Groups**.

2 Choose **Actions > Manage Volume Groups**.

3 Click **Create**.

Result:

The system creates a new row for the volume group.

4 Select (or highlight) the new volume group and enter the **Name** in the Volume Group column.

5 (Optional) Choose a **Parent Volume Group Name** entry to create a hierarchical structure where your new volume group is a child of the selected parent.

6 Enter the maximum capacity limits for the volume group.

- Enter 0 to specify an unlimited capacity for the volume group. This setting means that the capacity of logical volumes and nested volume groups can be increased without constraints.
- Enter a value that specifies the combined maximum capacity to which the associated objects can grow.

7 (Optional) Click **Remove** to immediately delete the selected row.

8 Click **OK** to save your changes.

Related concepts

- [About Volume Groups](#)
- [About Moving Logical Volumes](#)

Related references

- [Manage Volume Groups, Volume Groups Tab](#)
- [Manage Volume Groups, Volumes Tab](#)

Modify Volume Group Attributes

At times, you may want to modify certain attributes of a volume group. For example, you may want to nest one volume group within another.

- 1 From the **Configure** tab, click **Groups > Volume Groups**.
- 2 From the Volume Groups overview page, choose **Actions > Manage Volume Groups**.
- 3 Select a volume group you want to modify.
If you want to change the attributes of a nested volume group, click on the *parent* volume group in the list.
- 4 Enter new attribute values as needed.
- 5 To save the modified volume group, click **OK**.

Related concepts

- [About Volume Groups](#)
- [About Moving Logical Volumes](#)

Related references

- [Manage Volume Groups, Volume Groups Tab](#)
- [Manage Volume Groups, Volumes Tab](#)
- [Volume Groups Overview Page](#)

Related tasks

- [Move a Volume to a Different Volume Group](#)

Delete a Volume Group

You can delete a volume group after you have reassigned all its logical volumes to different volume groups.

- 1 From the **Configure** tab, click **Groups > Volume Groups**.
- 2 From the Volume Groups overview page, choose **Actions > Manage Volume Groups**.
- 3 Select a volume group you want to delete.
Note: If a volume group contains any objects, move or delete those objects before you delete the volume group.
- 4 To immediately delete the volume group, click **Remove**.

Related concepts

- [About Volume Groups](#)
- [About Moving Logical Volumes](#)

Related references

- [Manage Volume Groups, Volume Groups Tab](#)
- [Manage Volume Groups, Volumes Tab](#)
- [Volume Groups Overview Page](#)

Related tasks

- [Move a Volume to a Different Volume Group](#)

About Moving Volumes to Different Volume Groups

You can break the association between a logical volume and a volume group.

To do so, move the logical volume to a different volume group, which associates the logical volume with the new volume group. You can create additional volume groups, if needed.

You perform the following actions:

- Add more volume groups to your current organizational model and move one or more logical volumes into the new volume group.

For example, if your current organizational model is based on location and your company recently opened a sales office in Tokyo, create a new Japan volume group and move appropriate logical volumes into it.

- Create a new organizational model and move all logical volumes into the new volume groups.

For example, if your current organizational model is based on location and you want to reorganize based on corporate structure, create new departmental volume groups. Move logical volumes from the volume groups that are named for countries into the volume groups that are named for departments.

Move a Volume to a Different Volume Group

You may need to modify nested volume groups. For example, after you created a new volume group you can move existing volume groups into the new one.

While you are selecting a new parent volume group destination for your logical volume, you can preview the effects of your change in the Volume Groups overview page.

- 1 From the **Configure** tab, click **Groups > Volume Groups**.
- 2 From the Volume Groups overview page, choose **Actions > Manage Volume Groups**.
- 3 Select a logical volume or nested volume group from the list of volumes.
- 4 From the **Parent Volume Group Name** drop-down list, select the volume group you want as the new parent.
- 5 Click **OK** to move the selected items to another volume group.

Related concepts

- [About Volume Groups](#)
- [About Moving Logical Volumes](#)

Related references

- [Manage Volume Groups, Volume Groups Tab](#)
- [Manage Volume Groups, Volumes Tab](#)
- [Volume Groups Overview Page](#)

Related tasks

- [Modify Volume Group Attributes](#)

About Storage Domains

Storage Domains allow storage administrators to assign logical volumes to a specific collection of Bricks. Such assignments can be made to reduce contention among volumes, to implement different levels of security for those volumes, or both.

Note: Storage Domains might limit the ability of the system to provide the best optimization of the storage arrays and system performance.

A Storage Domain is defined as:

A subset of a virtual storage pool consisting of a defined group of Brick storage enclosures. This group can consist of any assortment of Bricks, regardless of Storage Class, capacity, or any other attribute. A Storage Domain is typically used to provide specific allocation or security features for a collection of logical volumes.

An administrator can allocate each Brick to a defined Storage Domain. When no administrator-defined domains exist, all Bricks reside in the default domain.

Storage administrators typically use Storage Domains for the following reasons:

User group separation	In this scenario, storage administrators can isolate application data to specific Bricks on a department basis (for internal cloud environments) or on a customer basis (in external cloud environments). This isolation eliminates inter-application contention for I/O services and provides charge-back capabilities.
Protocol separation	In this scenario, storage administrators can place application data on separate Bricks based on protocol and connectivity. This separation eliminates any chance of inter-application contention for I/O services. For example, an administrator could create a NAS domain, a SAN iSCSI domain, and a SAN FC domain.
Application I/O isolation	Storage administrators can create Storage Domains for use in specific applications and tiers of storage to eliminate unwanted Brick contention. For example, an administrator can create a

replication domain for incoming replication data and another domain for archival or backup of local data.

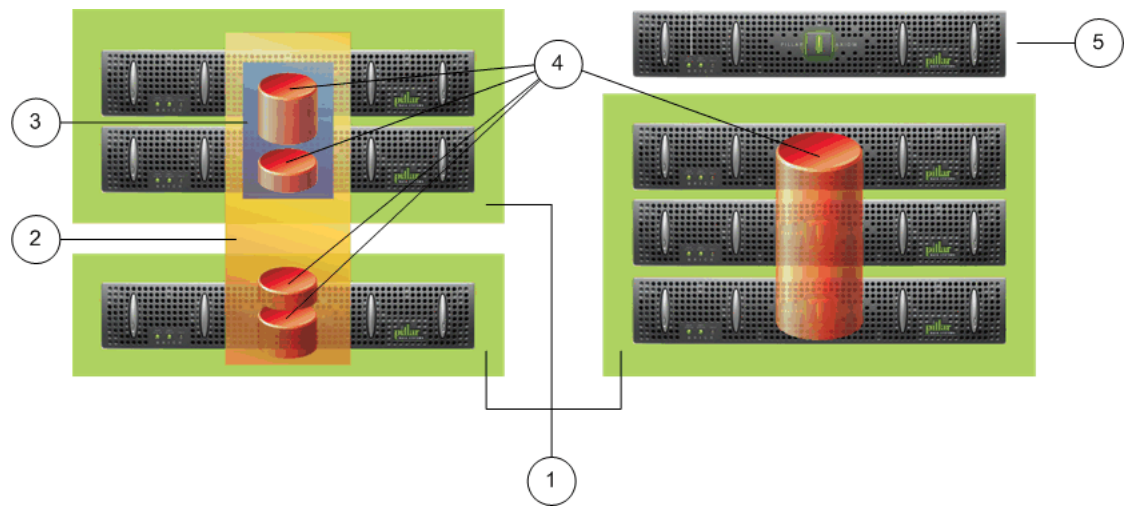
Data security Storage administrators can place logical volumes that contain sensitive data on a particular Storage Domain. If the data needs to be destroyed, the drives within those Bricks can be destroyed without the administrator having to be concerned with preserving less sensitive data. Placing those volumes in their own Storage Domain ensures that those volumes do not share Bricks with less sensitive material.

Brick or hardware retirement As drives age, the probability of failure increases. Storage Domains can efficiently move data to newer Bricks that have larger capacities as well as updated RAID controllers.

[Figure 7](#) illustrates a collection of Storage Domains and a sample distribution of logical volumes across those domains. This illustration shows the relationships among the following collection of objects:

- Three Storage Domains
- Two volume groups (one nested)
- Five logical volumes
- Seven Bricks

Figure 7 Storage Domains, volume groups, and volumes

**Legend**

1 Storage Domains	4 Logical volumes
2 Volume group	5 Unassigned Brick
3 Volume group (nested)	

In the illustration, the outer volume group (item 2, the orange box) contains a nested volume group (item 3, the blue box). The nested volume group contains two logical volumes (item 4, the red cylinders), while the outer (or parent) volume group contains two volumes of its own. Volume groups can also span multiple Storage Domains.

Note: Volume groups are always optional, as illustrated by the Storage Domain on the right side of the illustration, which contains a volume that is not part of a volume group.

The preceding figure also shows an example of a Brick that is not assigned to any Storage Domain. This state is temporary. While in this state, the capacity of the Brick is not included as free or available capacity. Causes of an unassigned state for a Brick:

- Newly added to the system
- About to be removed from the system
- In transition from one Storage Domain to another

Storage administrators can perform regular management actions for any logical volume residing in a Storage Domain, including:

- Create logical volumes within a domain.
- Create Volume Copies within a domain.

- Create clones of logical volumes contained in a domain.
- Move logical volumes to a different volume group.
- Delete logical volumes from a domain.

Note: All allocation for a logical volume is confined to the Bricks within a Storage Domain. In other words, the extents associated with a volume cannot span more than one domain.

Related concepts

- [About Primary Storage Domains](#)
- [About Adding Bricks to a Storage Domain](#)
- [About Moving Logical Volumes](#)
- [About Reassigning Bricks](#)
- [About Licensing Optional Premium Features](#)

Related tasks

- [Create a Storage Domain](#)
- [Delete a Storage Domain](#)
- [Modify a Storage Domain](#)

About Primary Storage Domains

Each Pillar Axiom system has exactly one primary Storage Domain. This domain contains system overhead, including all system configuration data.

In general, a primary Storage Domain must contain at least two Bricks. However, a Storage Domain may be as small as a single Brick. Such a system would have only one domain, which would be the primary Storage Domain.

Multiple domains cannot be created on a system with fewer than three Bricks. This restriction means that the primary domain must contain two Bricks before any other domain gets even one.

You can remove a Brick from a primary Storage Domain only under the following conditions:

- If the system contains serial ATA (SATA) Bricks, you must leave at least one SATA Brick.
- If the system contains no SATA Bricks, you must leave at least two Fibre Channel (FC) Bricks.

Note: A primary Storage Domain cannot consist only of SSD Bricks.

For a new Pillar Axiom system, or after a system reset, the following scenarios occur, in sequence:

- The system starts with no system configuration or persistence.
- When powered up, the system assigns all the Bricks that it discovers to a newly created, default, primary Storage Domain.
- The system then writes the initial configuration to all the Bricks.
- If three or more Bricks are available, the system then gives you an opportunity to move the Bricks into individual Storage Domains before volume configuration begins.

Related concepts

- [About Licensing Optional Premium Features](#)

About Managing Storage Domains

A storage administrator occasionally needs to perform certain management actions on a Storage Domain.

When a Pillar Axiom system starts up, that system has at least one Storage Domain. That domain is referred to as the *primary* or *default* Storage Domain. If that system has at least three Bricks, you can create additional Storage Domains by removing one or more of those Bricks from the default domain and adding them to the new domain.

A number of scenarios are possible depending on the existence of Storage Domains and the activities you perform that involve logical volumes and Bricks. The Pillar Axiom system responds in a variety of ways depending on the scenario.

Related concepts

- [About Storage Domains](#)
- [About Creating Storage Domains](#)
- [About Adding Bricks to a Storage Domain](#)
- [About Moving Logical Volumes](#)
- [About Reassigning Bricks](#)
- [About Licensing Optional Premium Features](#)

Related tasks

- [Create a Storage Domain](#)
- [Reassign a Brick to Another Storage Domain](#)
- [Move a Volume to Another Storage Domain](#)

About Creating Storage Domains

When logical volumes already exist on a Pillar Axiom system, creating a Storage Domain can cause data migration.

The system notifies you that creating a Storage Domain and attempting to perform any of the following actions will cause data migration:

- Assign specific volumes to the Storage Domain.
- Assign a Brick to that domain when that Brick has one or more logical volumes or portions of volumes residing on that Brick.

Important! The Storage Domain in either case must have sufficient free capacity to hold the entire volume that will be migrated.

The system also provides you the following information:

- A list of the volumes (and their associated repositories) that will require data migration.
- A message indicating whether enough capacity exists to move those volumes into the chosen Storage Domain.
- A message indicating whether enough capacity exists for the remaining volumes to reside in an existing Storage Domain.

Related concepts

- [About Primary Storage Domains](#)
- [About Adding Bricks to a Storage Domain](#)
- [About Moving Logical Volumes](#)
- [About Reassigning Bricks](#)

Related tasks

- [Create a Storage Domain](#)
- [Reassign a Brick to Another Storage Domain](#)
- [Move a Volume to Another Storage Domain](#)

Create a Storage Domain

Storage Domains allow you to assign logical volumes to a specific collection of Bricks. Such assignments can be made to reduce contention among volumes, to implement different levels of security for those volumes, or both. Storage Domains allow administrators, for example, to partition storage for specific users or departments in a public or private cloud storage environment.

When you create a Storage Domain for regular use, we recommend that you assign the following minimum number of Bricks to that domain:

- Two serial ATA (SATA) or solid state device (SSD) Bricks
- Three Fibre Channel (FC) Bricks

When you need to replace one or more Bricks in an existing domain, you typically would create a new Storage Domain, assign Bricks to it, and then move the logical volumes from the existing domain to the newly created domain. In this scenario, you can create the new domain without any Bricks with the purpose of assigning the Bricks later.

In the above scenario, if you are replacing Bricks in the current primary Storage Domain, for the new domain, we recommend that you have *at least* two Bricks of the same Storage Class, in the following order of preference:

- First, SATA.
- If not SATA, then FC.
- If not FC, then SSD.

Note: We recommend a minimum of two Bricks of the same Storage Class to ensure that the Persistence VLUN, which contains the system configuration information, retains double redundancy.

A non-primary Storage Domain can contain as few as one Brick of any Storage Class.

Important! If you place only a single Brick of the lowest Storage Class in the new non-primary domain and the domain is promoted to primary, the redundancy of the Persistence VLUN reverts to single redundancy.

- 1 From the **Configure** tab, click **Groups > Storage Domains**.
- 2 Choose **Actions > Manage Storage Domains**.
- 3 On the Storage Domains tab, click **Create**.

Result:

A new row in the Storage Domains table appears.

- 4 In the blank Storage Domain field, enter the name of the new domain.
- 5 Click **OK**.

The new Storage Domain now appears in the list of domains.

After you create the Storage Domain, assign one or more Bricks to the domain so you can locate logical volumes in the domain. The number of Bricks that you add to a domain directly affects the performance of that domain.

Related concepts

- [About Storage Domains](#)
- [About Adding Bricks to a Storage Domain](#)
- [About Licensing Optional Premium Features](#)

Related tasks

- [Reassign a Brick to Another Storage Domain](#)
- [Move a Volume to Another Storage Domain](#)

Modify a Storage Domain

Sometimes you might want to change the name of an existing Storage Domain.

Tip: If you want to perform any of the following modifications, perform the task dedicated specifically to that purpose:

- Reassign a Brick that belongs to one Storage Domain to a different Storage Domain.
- Move a logical volume from one Storage Domain to a different Storage Domain.

These two types of modification cannot be done by performing this task.

- 1 From the **Configure** tab, click **Groups > Storage Domains**.
- 2 Choose **Actions > Manage Storage Domains**.
- 3 On the Storage Domain tab, click on the name of the Storage Domain that you want to modify.
- 4 Enter a new name for the Storage Domain.
- 5 Click **OK**.

Related tasks

- [Move a Volume to Another Storage Domain](#)
- [Reassign a Brick to Another Storage Domain](#)

Delete a Storage Domain

When you no longer need a Storage Domain that you created, you can delete it.

Prerequisites:

- The Storage Domain that you want to delete must not contain any logical volumes. If the Storage Domain contains any logical volumes, you must first delete those volumes or move them to another domain.
- The Storage Domain that you want to delete must not have any Bricks assigned to the domain. If any Bricks are assigned to the domain, you must first perform the following actions:
 - If any of the Bricks contain any logical volumes, delete those volumes or move them to another domain.
 - Reassign the Bricks to another domain.

- 1 From the **Configure** tab, click **Groups > Storage Domains**.
- 2 Choose **Actions > Manage Storage Domains**.
- 3 On the Storage Domain tab, highlight the Storage Domain that you want to delete, and then click **Remove**.
- 4 Click **OK**.

Result:

One of the following will occur:

- If the operation is successful, the domain is removed from the list of domains.
- If the operation is unsuccessful, the system does not remove the domain and displays an appropriate error dialog:
 - The domain contains one or more logical volumes.
 - The domain has one or more Bricks assigned to it.

If the operation is unsuccessful, move any volumes residing on the domain to another domain and reassign the Bricks, as appropriate.

Related concepts

- [About Licensing Optional Premium Features](#)

Related tasks

- [Move a Volume to Another Storage Domain](#)
- [Reassign a Brick to Another Storage Domain](#)

Set a Storage Domain as the Primary

Circumstances can arise in which you might want to transfer the Persistence VLUN, which contains the system configuration data, from the current primary Storage Domain to a different domain.

Prerequisites:

- A non-primary Storage Domain.
- The following lists the minimum recommended number of Bricks in the order of preference:
 - First, two serial ATA (SATA).
 - Second, two Fibre Channel (FC).
 - Third, two solid state device (SSD).

Note: If you have more than one Storage Class in the non-primary Storage Domain, the Pillar Axiom storage system migrates to SATA, if that class is available. If SATA is not available, the system migrates to FC, if that class is available. If SATA and FC are not available, the system migrates to SSD.

When the non-primary Storage Domain becomes the primary domain, the previous primary domain loses its primary status and the system migrates the system data to the new primary domain. The administrator cannot cancel this special data migration.

- 1 From the **Configure** tab, click **Groups > Storage Domains**.
- 2 Highlight the Storage Domain that you want to become the new primary domain and choose **Actions > Set as Primary Storage Domain**.
- 3 To set the non-primary Storage Domain as the new primary domain, click **OK**.

Result:

The systems begins migrating all system configuration and persistence data to the new primary domain.

Important! After you click **OK**, you cannot cancel this data migration.

Important! After promoting a non-primary Storage Domain to primary, you should verify that the volume named PERSISTENCE has been moved to the Bricks in the new primary domain. To verify proper migration, use the `axiomcli storage_allocation` command provided by the Pillar Axiom CLI application. When executing this command, include the `-brick` and `-list` options. For more information, refer to the *Pillar Axiom CLI Reference Guide*.

Related concepts

- [About Primary Storage Domains](#)
- [About Licensing Optional Premium Features](#)

About Logical Volumes and Storage Domains

The impact of creating a logical volume depends on whether administrator defined Storage Domains exist.

Table 6 Effect of Storage Domains on storage availability

Do administrator defined Storage Domains exist?	Impact
No	<p>All storage is available. The entire storage pool comprises the default Storage Domain.</p> <p>No choice exists in placing the logical volume on a specific set of Bricks.</p>
Yes	<p>Because storage is segmented, you need to select a specific Storage Domain when creating a logical volume. This fact can cause storage space to be under utilized.</p> <p>The system allocates the new volume using only those Bricks that reside in the specified domain.</p> <p>Note: A clone repository resides in the same Storage Domain in which the source volume resides.</p>

Related concepts

- [*About Storage Domains*](#)
- [*About Moving Logical Volumes*](#)
- [*About Creating LUNs*](#)
- [*About Licensing Optional Premium Features*](#)

CHAPTER 5

About Provisioning and Quality of Service

Volume Capacity and Provisioning Overview

Note: A Pillar Axiom system uses binary units to calculate and display the capacity of physical storage and the size of logical volumes:

1 MB = 1024^2 (1,048,576) bytes

1 GB = 1024^3 (1,073,741,824) bytes

1 TB = 1024^4 (1,099,511,627,776) bytes

Related concepts

- [*Thinly Provisioned Volumes*](#)
- [*Free Capacity and Volume Creation*](#)
- [*Allocation of Thinly Provisioned Storage*](#)
- [*Growth Increments*](#)
- [*Capacity Overhead*](#)
- [*Parity in Reported Capacities*](#)
- [*Reclaiming Capacity*](#)

Thinly Provisioned Volumes

Traditionally, when storage is allocated to an application, the allocation is dedicated to that application. This assignment prevents other applications from accessing this capacity, even when the amount allocated is never used. Because of this allocation strategy, the capacity is stranded and cannot be leveraged in support of additional needs.

Thin provisioning mitigates these issues by allowing storage administrators to leverage this unused capacity for a logical volume by performing these actions:

- Allocate capacity based on future needs.
- Draw on a common pool of storage as capacity is consumed.

Thin provisioning allows an administrator to create a logical volume of any size without committing that capacity at that time. Each application has what appears

to be all the storage needed for ongoing operations, but without the physical capacity locked to a particular volume.

Administrators can create logical volumes up to the maximum addressable logical capacity that is allowed for the OS, with little physical storage assigned to the volume. As data is written to the thinly provisioned volume and capacity is consumed (called *in-fill*), the system automatically allocates additional capacity to the logical volume in increments.

Note: Solid-state drive (SSD) Bricks do not support thinly provisioned volumes.

A logical volume is thinly provisioned when its addressable logical capacity is larger than its initially allocated logical capacity. A logical volume can be thinly provisioned by any amount.

Storage is provided when write operations to the logical volume require regions that are not allocated.

Note: The additional space may not be contiguous with previous allocations.

Thin provisioning depends on the relationship between the initial values you set for the following parameters:

- *Allocated logical capacity* that the system makes available to the logical volume. This value is labeled **Total Capacity** after successful volume creation.
- *Addressable logical capacity* to which the logical volume can grow. Because of rounding that is performed internally, this value can be up to 2 GB less than the allocated logical capacity. After the system successfully creates the volume, addressable logical capacity is labeled **Growth Max**.

Note: Growth occurs only within the Storage Class on which the volume is based and within the Storage Domain in which the volume is defined.

The allocated logical capacity can be any value, up to and including the addressable logical capacity.

Tip: If you do not desire thin provisioning, set the allocated logical capacity equal to the addressable logical capacity.

When a system contains a mix of storage types (Storage Classes), new volume allocation cannot cross storage boundaries. The allocation occurs only within the specified Storage Class.

Related concepts

- [About Licensing Optional Premium Features](#)

Free Capacity and Volume Creation

A minimum amount of free space is required to create a new logical volume. The actual amount of physical capacity that is consumed from the system free space when you create a new logical volume depends on several factors.

These factors are:

- The RAID geometry of the volume.
- The redundancy Quality of Service (QoS) setting of the volume.

To determine the actual physical capacity needed, the system adds the following:

- To account for parity, the system increases the requested capacity by different amounts, depending on the RAID geometry:
 - 20% for RAID 5 (SATA)
 - 10% for RAID 5 (FC)
 - 100% for Distributed RAID or RAID 5 with Wide Stripe
- If redundancy for the volume is set to Double, the system doubles the physical allocation.

For example, if the requested capacity for a logical volume is 250 GB, and the volume uses RAID 5 geometry in SATA storage, the system allocates an additional 50 GB. If the volume has a redundancy setting of Double, the system allocates an additional 300 GB, for a total physical allocation of 600 GB.

If a request to create a logical volume fails because of capacity issues, it would be for the following reasons:

- Insufficient capacity remains in the Storage Class or Storage Domain that is specified for the volume.
- Sometimes, the system may need to round your request to a slightly larger size, which then is greater than available capacity.
- You have requested double redundancy, but sufficient capacity is not available on two different Bricks within the specified Storage Class.
- You have requested a Quality of Service (QoS) priority setting of Premium, but sufficient capacity does not exist on that storage band.

Related concepts

- [*Capacity Overhead*](#)
- [*Parity in Reported Capacities*](#)

Allocation of Thinly Provisioned Storage

The capacity reserved for thin provisioning, which is part of the system overhead, is accounted for in the available capacity that the system reports. In other words, what the system reports as available capacity is fully available for the provisioning of logical volumes.

For storage area network (SAN) systems, the degree to which a LUN is thinly provisioned depends on the nature of the host applications that access the LUN. If only specific portions of a LUN are ever accessed by applications, the thinness of that LUN remains the same. As applications attempt to access more and more different areas of the LUN, the system allocates more and more physical space for the LUN, causing the thinness to decrease.

Some applications access most or all of the addressable space for a volume. In these cases, the volume transitions from being thinly provisioned to being fully provisioned while the application executes. An example of such an application is the `mkfs` utility, which creates a filesystem on a partition. As `mkfs` executes and formats the filesystem, most or all of the partition is written by the application, causing the underlying volume on the Pillar Axiom system to become fully provisioned. In cases such as these, creating the underlying volume using thin provisioning has little value.

The Windows operating system reserves a substantial amount of metadata for a filesystem that has been formatted as an NTFS (New Technology File System) volume. The layout of this metadata causes an early allocation of thinly provisioned space. The primary NTFS metadata consists of the following objects:

- Boot record, which is written to both the beginning and the end of the volume.
- Master File Table (MFT), which is written to both the beginning and the middle of the volume.

To prevent the MFT from becoming fragmented, Windows reserves a buffer around the MFT. The size of this buffer is configurable and can be 12.5%, 25%, 37.5%, or 50% of the drive space. Windows will not create new files in this buffer region until the unused space is consumed. Each time the rest of the drive space becomes full, the buffer size is halved. This strategy provides new space for additional write operations.

Pillar does not recommend creating a thinly provisioned LUN that is filled up greater than 90% on the first in-fill, especially with NTFS. NTFS writes all over the LUN causing allocations that do not match the amount of data that is written. A heavily used NTFS filesystem running without much free capacity will eventually use up all the capacity unless the filesystem is de-fragmented periodically. NTFS favors writing into new allocated space instead of reusing previously written space. NTFS works with thin provisioning initially but can quickly use up more allocation than the amount of data the filesystem would show as used.

Because thin provisioning uses Slammer resources and affects performance, a good use of thin provisioning would be for a LUN that has the following characteristics:

- An initial allocation equal to the amount of existing data, plus 10%. This value becomes the allocated logical capacity.
- An addressable logical capacity that is twice the allocated capacity, plus 10%.

For example, given 420 GB of file data, the administrator should configure the allocated logical capacity of the LUN to be approximately 470 GB and the addressable logical capacity to be approximately 1 TB.

Note: How much capacity NTFS uses depends on many factors, including the size of writes, where the writes are made, and other factors such as the type of storage used in the storage pool.

On Linux platforms, EXT2 and EXT3 filesystems write metadata over the entire range of logical block addresses (LBAs) of the LUN. The drive is organized into block groups and metadata exists at the beginning of each block group. This configuration typically causes the entire LUN to be provisioned when the administrator creates a filesystem. This full provisioning occurs because the metadata write is below the allocation unit used by Pillar Axiom systems. This condition causes the system to expand every allocation extent to the maximum size.

In summary, the success of utilizing thin provisioning depends on the filesystem or the application using the LUN.

Growth Increments

When the system allocates capacity for a logical volume, the system divides the allocation into slices (called *growth increments*) and uses as many of them as it needs.

Each growth increment is between 1 and 2 GB. For example, if the volume is 2 TB, the system may use between 1024 and 2048 growth increments for the allocation. The exact value depends on the combination of the following choices that characterize the underlying storage for the volume:

- Type of Brick (SSD, Fibre Channel, or serial ATA)
- RAID geometry (RAID 5 or Distributed RAID)
- Strip size (normal or 1 MB)

Note: When the system needs to grow or in-fill a logical volume, the system returns an error if sufficient capacity does not exist within the Storage Class associated with the volume, even when sufficient capacity exists in other Storage Classes.

Capacity Overhead

Plans for the provisioning of logical volumes must take into account the extra capacity the system allocates to overhead.

To accommodate the level of RAID protection required to allocate a newly created logical volume, the system adds a certain amount of overhead to a request for the capacity of the volume. The capacity consumed and reported for RAID 5 logical volumes includes that overhead. This overhead varies, depending on the RAID geometry and Storage Class assigned to the volume. For RAID 5, the overhead is as follows:

Serial ATA drives and SSDs	20%
Fibre Channel drives	10%

For Distributed RAID, the capacity consumed and reported for logical volumes is twice the requested amount, regardless of Storage Class.

Besides the overhead allocated to a logical volume when the volume is created, the Pillar Axiom system allocates 50 GB of physical capacity in each of the serial ATA (SATA) and Fibre Channel (FC) Storage Classes as an in-fill reserve. The system reserves this physical capacity to help prevent inadvertent exhaustion of system physical capacity when thinly provisioned volumes are created. The system uses this capacity when physical capacity needs to be assigned to a thinly provisioned volume, and all other physical capacity in that Storage Class has been consumed.

The size of this reserve capacity is included in the calculations for the free, available, and total system capacities that are displayed by the graphical user interface (GUI) and the command line interface (CLI).

Parity in Reported Capacities

RAID arrays have both physical and virtual capacity.

The physical capacity of a RAID array that is reported includes capacity for parity. Sizes reported in capacity usage summaries and the sizes reported for total, used, and free system capacities are in terms of raw physical capacities.

The virtual capacity of a RAID array that is reported, however, does not include capacity for parity. The ratio between the virtual capacity and the physical capacity depends on whether the storage is RAID 5 or Distributed RAID:

RAID 5: serial ATA (SATA) drives and solid state drives (SSDs)	5:6
RAID 5: Fibre Channel (FC) drives	10:11
Distributed RAID: FC, SATA, and SSD drives	1:2

Reclaiming Capacity

When a user deletes a logical volume, the system reconditions the space (by writing a predefined bit pattern) before reclaiming it for reuse. As the previously allocated capacity frees up, it becomes available for allocation.

Note: When a large volume is being deleted, the operation can take awhile for all the capacity to be reclaimed. Because of this additional time needed for reconditioning, the amount of used capacity plus the free capacity may not equal the total capacity. During this time, the graphical user interface (GUI) displays the amount of capacity remaining to be reconditioned.

About Quality of Service

Quality of Service (QoS) describes a collection of policies that an administrator can implement by defining various properties of a logical volume. Administrators can use these policies to adjust the performance of those volumes.

Quality of Service is defined as follows:

The set of capacity and performance attributes, including redundancy, that administrators assign to logical volumes. Administrators can assign different QoS attributes to each logical volume and allocate system resources that are based on user requirements.

QoS policies are available for the following properties:

- Preferred storage media, known as *Storage Class*
- Processing queue priority and data access efficiency, known as *priority*
- Number of mirror copies, known as *redundancy*
- Performance optimization, known as a combination of *access bias* and *I/O bias*

About Storage Classes

The Storage Class feature allows you to specify the preferred storage media to use for a logical volume.

A Storage Class is defined as:

A categorization of physical storage, each category having distinct characteristics with regard to performance characteristics of data access. Example Storage Classes in a Pillar Axiom system are serial ATA (SATA), Fibre Channel (FC), and solid state drive (SSD). Pillar Axiom systems allow an administrator to explicitly manage volume placement within the overall system storage pool, first by Storage Domain, then by Storage Class, and finally by relative priority level within that Storage Class.

Pillar Axiom systems support the following three Storage Classes:

- SATA

- FC
- SSD SLC (solid state drive, single-level cell)

Note: Which Storage Classes are available on a particular Pillar Axiom system depends on the types of Brick storage enclosures you have installed on the system.

A Storage Class has these attributes:

- A newly created logical volume is associated with a single Storage Class.
- The Pillar Axiom Storage Services Manager graphical user interface (GUI) shows the capacity available within each Storage Class.
- The system will not create a logical volume when the available space for the associated Storage Class is insufficient to accommodate the capacity requested for the volume.

For FC and SATA Storage Classes, the striping of a logical volume is across a number of drives in a collection of RAID groups. The number of drives depends on the Quality of Service (QoS) priority setting for the volume. For the SSD SLC Storage Class, striping for a volume is across all available drives, regardless of the priority setting.

Related concepts

- [About RAID Array Stripes](#)

Related references

- [Create SAN LUN, Quality of Service Tab](#)
- [Effects of Access Bias and I/O Bias](#)

About Priority Levels

You can specify the priority level of a logical volume to manage the amount of system resources that are allocated to this volume compared to the amount allocated to other volumes.

In addition to determining the placement of data onto specific areas of the drive platters relative to the drive spindles, the priority level of a volume determines the processing *queue priority* for that volume. Queue priority defines the percentage of Slammer CPU cycles that are dedicated to the volume.

A given priority level specifies the layout of data that is stored in the Pillar Axiom system. If sufficient Bricks are present in the Storage Domain that is hosting the logical volume, to enhance the performance of the volume, the system places a higher priority volume on a greater number of Bricks when compared to a lower priority volume. For example, for a logical volume that resides in SATA storage

media and that has a priority level of Premium or High, the system stripes the volume across eight RAID groups. If, however, that volume has a priority level of Low or Archive, the system stripes the volume across only four RAID groups.

Related concepts

- [About Redundancy](#)

Related references

- [System Storage Profile Properties](#)

About Redundancy

You can use the redundancy Quality of Service (QoS) property to specify how many mirror copies of the original data of a logical volume are stored online.

Important! Pillar highly recommends that you consult with a Pillar Customer Support professional for assistance with sizing your system and creating your logical volumes.

Redundancy options include:

- Standard** Stores original data only. Data striping over multiple RAID groups maintains full redundancy, even without mirror copies.
- Double** Stores original data and one mirror copy, with data striping over multiple RAID groups.

A RAID group is defined as:

A collection of physical drives within a Brick that stores user data. Fibre Channel (FC) Bricks provide one RAID group, which consists of 11 drives. Serial ATA (SATA) and solid-state drive (SSD) Bricks provide two RAID groups, each of which consists of 6 drives.

Note: Double redundancy can only provide true redundancy if your system has enough Bricks on which to allocate the logical volume such that no two mirror copies share a RAID group.

If the free space in the storage pool is becoming depleted, or a large logical volume is created, it might be necessary to place the volume on more RAID group fragments.

Depending on the ability of the system to allocate sufficient contiguous storage blocks for the size of the logical volume, refer to the following number of RAID groups to configure your volumes for the best performance:

Table 7 Optimum number of RAID groups for best performance

Priority level	SATA standard redundancy	SATA double redundancy	FC standard redundancy	FC double redundancy
Archive	4	8	2	4
Low	4	8	2	4
Medium	6	12	3	6
High	8	16	4	8
Premium	8	16	4	8

Note: When the selected Storage Class is SSD, all available SSD drives are striped across, regardless of the priority level chosen.

For *performance testing purposes only*, create a logical volume using standard redundancy and the Performance Benchmark storage profile. This is *not* recommended for most applications. Before you configure normal volumes for applications, reset your system after you have created a Performance Benchmark volume.

About Access Bias

You can use the access bias Quality of Service (QoS) property (in conjunction with the I/O bias property) to help optimize the performance of a logical volume.

Access bias, as a QoS property, indicates to the system what type of access is the most common or expected for a particular volume. This bias can be one of the following:

- Sequential** Read and write requests from client applications tend to request operations on the data one record after the other.
- Random** Read and write requests from client applications tend to request operations on the data records in an arbitrary order.
- Mixed** Read and write requests from client applications tend to mix the request operations on the data sometimes in sequential and sometimes in random order.

Note: Access bias specifies an optimization bias; it is not a requirement that all data or data operations conform to the specified access method.

Related concepts

- [About I/O Bias](#)

Related references

- [Effects of Access Bias and I/O Bias](#)

About I/O Bias

You can use the I/O bias Quality of Service (QoS) property (in conjunction with the access bias property) to help optimize the performance of a logical volume.

I/O bias, as a QoS property, indicates to the system the type of I/O operation that is the most common or expected for a particular volume. This bias can be one of the following:

- Read** Most requests from client applications are for `read` operations.
- Write** Most requests from client applications are for `write` operations.
- Mixed** Requests from client applications are likely equal for `read` and `write` operations.

Important! If you choose **Random** as the access method and **Write** as the I/O Bias, the system creates the logical volume with a Distributed RAID geometry. This geometry provides enhanced write performance but uses twice the capacity.

The system stores all writes of user data and system metadata in mirrored copies of the journal.

One copy is maintained in non-volatile memory on one control unit (CU) of a Slammer. The mirror copy is maintained in one of the following locations:

- Battery-backed memory of the partner CU on the Slammer (preferred location). Writes to this copy are equivalent to write-back cache.
- Virtual LUN (VLUN) that is reserved on physical storage for the logical volume, if the partner CU is unavailable for the write operation. Writes to this copy are equivalent to write-through cache.

Writes from the journal to permanent physical storage are equivalent to write-through cache. The system flushes user data and the corresponding metadata as a unit to physical storage.

Related concepts

- [About Access Bias](#)
- [About Licensing Optional Premium Features](#)
- [About Enhanced Performance for Random Write Operations](#)

Related references

- [Effects of Access Bias and I/O Bias](#)

Effects of Access Bias and I/O Bias

The combination of the access bias and I/O bias QoS properties of a logical volume can have varying effects on certain performance characteristics of that volume.

These performance characteristics can be effected by the access and I/O biases:

- The amount of reading ahead performed by Slammers for the volume
- The RAID configuration of the volume in the Bricks

[Table 8](#) summarizes the effects that the access bias and the I/O bias of a logical volume can create for that volume.

Table 8 Effects of access and I/O bias

Access bias	I/O bias	Read-ahead in the Slammer	RAID configuration in the Brick
Sequential	Read	Aggressive	RAID 5 Reads large extents of the data into memory.
	Write	Conservative	RAID 5 Writes data in write-back mode to physical storage in full-stripe extents.
Mixed and random	Read	None	RAID 5 <ul style="list-style-type: none"> • Combines multiple block writes into a single-stripe write, when possible. • Retains data in the cache for a longer

Table 8 Effects of access and I/O bias (continued)

Access bias	I/O bias	Read-ahead in the Slammer	RAID configuration in the Brick
			period of time to allow for possible combining of writes, which minimizes the disk accesses needed to de-stage data.
Random	Write	None	Distributed RAID

Related concepts

- [About Access Bias](#)
- [About I/O Bias](#)
- [About Licensing Optional Premium Features](#)

About Enhanced Performance for Random Write Operations

You can enhance the performance of random write operations on a logical volume under certain circumstances.

Using the Quality of Service (QoS)-based management tools provided in the Pillar Axiom Storage Services Manager, you can improve the overall performance of random-write intensive applications by taking advantage of a nested RAID structure that replaces four I/O operations with a parallel mirrored-write operation.

The system utilizes this RAID geometry when you set the optimization settings for a logical volume to random access with a write I/O bias. In this case, the system allocates space on a Distributed RAID array on which it performs parallel mirrored-write operations (two writes).

Note: This Distributed RAID geometry applies only to newly created volumes and to volumes that are migrated by means of QoS migration that may occur when adding serial ATA (SATA) Bricks to a system containing Fibre Channel Bricks.

In addition, because the data resides on two independent drives, Distributed RAID arrays allow the system to optimize read operations as well. In this case, the system can select the least busy of the two drives.

Related concepts

- [About Licensing Optional Premium Features](#)

About Storage Profiles

When configuring a logical volume, you can select a collection of predefined properties to apply to that volume. This collection of properties is called a *Storage Profile*.

When using a specific Storage Profile, you can select a profile that you have previously created and saved or one of the pre-configured profiles.

After a volume is created using a Storage Profile, removal of the profile does not affect the performance characteristics of that volume.

The following properties define a Storage Profile:

Priority level	Determines the placement of the data relative to the drive spindles, the number of drives over which the data is striped, and the processing queue priority: Premium, high, medium, low, or archive.
Redundancy	Specifies the number of mirrors that are to be stored online: Standard or double.
Typical access	Specifies the type of access that is the most common or expected: Sequential, random, or mixed.
I/O bias	Specifies the type of I/O operation that is the most common or expected: Read, write, or mixed.
Strip size	<p>Specifies the number of contiguous bytes to be stored on a single drive. The default setting depends on the media type:</p> <ul style="list-style-type: none">64 KB for Fibre Channel (FC) media128 KB for serial ATA (SATA) media128 KB for solid state drive, single-level cell (SSD SLC) media <p>For Oracle Automatic Storage Management (ASM) applications, the strip size is 1 MB.</p>
Number of RAID groups	<p>Specifies the number of RAID groups across which the data is written (striped). The number of drives in a RAID group depends on the type of storage media within the group:</p> <ul style="list-style-type: none">○ For FC media, a RAID group consists of 11 drives.○ For SATA and SSD media, a RAID group consists of six drives.

	The number of drives is sometimes referred to as the <i>stripe width</i> .
Read ahead	Specifies normal (no read ahead), aggressive, or conservative. The default setting, by default, is based on the typical access and I/O bias of the volume: Sequential reads Aggressive. Sequential writes Conservative. Random access Normal.
Writes	Specifies the caching method for write operations: Write-back Writes to the cache are not immediately written to disk. Write-through Writes to the cache are immediately written to disk.
Disk protection	Specifies the type of data protection: Mirroring Data on a RAID drive is protected by means of an exact copy of that data (Distributed RAID). A mirror set is created for a volume that has a double redundancy setting. Parity Data on a RAID drive is protected through use of a special algorithm, the results of which are stored on a separate drive for fault tolerance (RAID 5).
Preferred Storage Classes	Specifies the type of storage media, which can be any combination of the following types: <ul style="list-style-type: none">○ FC○ SATA○ SSD SLC

Related concepts

- [About Managing Storage Profiles](#)

Related references

- [System Storage Profile Properties](#)

System Storage Profile Properties

A Storage Profile defines the Quality of Service (QoS) settings for an individual logical volume. To help the storage administrator configure a volume, Pillar Data Systems provides a collection of Storage Profiles, each of which is optimized for one of several common applications.

The following tables define the QoS settings that are associated with each of these collections:

- [Table 9: Backup Storage Profiles](#)
- [Table 10: MSSQL Storage Profiles](#)
- [Table 11: MSXchg Storage Profiles](#)
- [Table 12: OracleDB Storage Profiles](#)
- [Table 13: OracleUCM Storage Profiles](#)
- [Table 14: Xen Storage Profiles](#)
- [Table 15: Pillar Axiom MaxRep Storage Profiles](#)
- [Table 16: Other Storage Profiles](#)

Note: In all of the following tables, *stripe width* refers to the number of RAID groups across which the system writes data.

The table below lists the QoS settings for the Storage Profiles associated with the Backup and Virtual Tape Library (VTL) applications:

Table 9 Backup Storage Profiles

Profile	Priority level	Storage Class	Stripe width / Strip size	RAID type	Read ahead	Typical access / I/O bias
Disk to Disk	Archive	SATA	4 128 KB	RAID 5	Off	Mixed Write
SIR Data	Archive	SATA	4 128 KB	RAID 5	Off	Mixed Mixed
SIR Scratch	High	SATA	8 128 KB	Distributed RAID	Off	Random Write

Table 9 Backup Storage Profiles (continued)

Profile	Priority level	Storage Class	Stripe width / Strip size	RAID type	Read ahead	Typical access / I/O bias
VTL Data	Archive	SATA	4 128 KB	RAID 5	Off	Sequential Write

The table below lists the QoS settings for the Storage Profiles associated with the Microsoft SQL Server (MSSQL) application:

Table 10 MSSQL Storage Profiles

Profile	Priority level	Storage Class	Stripe width / Strip size	RAID type	Read ahead	Typical access / I/O bias
Backup Files	Low	SATA	4 128 KB	RAID 5	Off	Mixed Mixed
Quorum Disk	Low	SATA	4 128 KB	RAID 5	Off	Mixed Mixed
System DB	Low	SATA	4 128 KB	RAID 5	Off	Mixed Mixed
Temp DB	Medium	SATA	6 128 KB	Distributed RAID	Off	Random Write
TPCC Data	High	FC	4 64 KB	RAID 5	Aggressive	Sequential Write
TPCC Logs	Low	SATA	4 128 KB	RAID 5	Aggressive	Mixed Write

The table below lists the QoS settings for the Storage Profiles associated with the Microsoft Exchange Server (MSXchg) application:

Table 11 MSXchg Storage Profiles

Profile	Priority level	Storage Class	Stripe width / Strip size	RAID type	Read ahead	Typical access / I/O bias
Database	High	FC	4 64 KB	RAID 5	Off	Random Mixed

Table 11 MSXchg Storage Profiles (continued)

Profile	Priority level	Storage Class	Stripe width / Strip size	RAID type	Read ahead	Typical access / I/O bias
Transaction Logs	Low	SATA	4 128 KB	RAID 5	Aggressive	Sequential Write
SMTP/MTA Queue	High	FC	4 64 KB	RAID 5	Aggressive	Sequential Mixed

The table below lists the QoS settings for the Storage Profiles associated with the Oracle Database Platform (OracleDB) application:

Table 12 OracleDB Storage Profiles

Profile	Priority level	Storage Class	Stripe width / Strip size	RAID type	Read ahead	Typical access / I/O bias
Archive Logs	Low	SATA	4 128 KB	RAID 5	Off	Sequential Write
Control Files	Premium	SSD SLC	8 128 KB	RAID 5	Off	Mixed Mixed
DB Index	Medium	SATA	6 128 KB	RAID 5	Off	Mixed Mixed
DB Tables	Medium	SATA	6 128 KB	RAID 5	Off	Mixed Mixed
Online Redo Logs	High	FC	4 64 KB	RAID 5	Aggressive	Sequential Write
Temp Files	Medium	SATA	6 128 KB	RAID 5	Off	Mixed Mixed

The table below lists the QoS settings for the Storage Profiles associated with the Oracle Universal Content Management (OracleUCM) application:

Table 13 OracleUCM Storage Profiles

Profile	Priority level	Storage Class	Stripe width / Strip size	RAID type	Read ahead	Typical access / I/O bias
Backup & Recovery	Archive	SATA	4 128 KB	RAID 5	Conservative	Sequential Write
Native File Repository	Archive	SATA	4 128 KB	RAID 5	Off	Sequential Write
Redo Log Group	High	FC	4 64 KB	RAID 5	Aggressive	Sequential Write
Search Index Table Space	Medium	SATA	6 128 KB	RAID 5	Off	Random Mixed
Web Viewable Repository	Medium	SATA	6 128 KB	RAID 5	Off	Random Read

The table below lists the QoS settings for the Storage Profiles associated with the Citrix XenServer (Xen) application:

Table 14 Xen Storage Profiles

Profile	Priority level	Storage Class	Stripe width / Strip size	RAID type	Read ahead	Typical access / I/O bias
Application	Premium	FC	4 64 KB	RAID 5	Off	Mixed Mixed
Operating System	High	FC	4 64 KB	RAID 5	Off	Mixed Read
Swap Space	Medium	SATA	6 128 KB	RAID 5	Off	Mixed Mixed

The table below lists the QoS settings for the Storage Profiles associated with the Pillar Axiom MaxRep Replication for SAN application:

Table 15 Pillar Axiom MaxRep Storage Profiles

Profile	Priority level	Storage Class	Stripe width / Strip size	RAID type	Read ahead	Typical access / I/O bias
Home	Premium	SATA	8 64 KB	RAID 5	Aggressive	Sequential Mixed
Backup	Archive	SATA	4 64 KB	RAID 5	Off	Mixed Mixed
Retention	Premium	SATA	8 64 KB	RAID 5	Off	Mixed Mixed

The table below lists the QoS settings for all other Pillar Storage Profiles:

Table 16 Other Storage Profiles

Profile	Priority level	Storage Class	Stripe width / Strip size	RAID type	Read ahead	Typical access / I/O bias
General Purpose	Medium	SATA	6 128 KB	RAID 5	Off	Random Read
Generic Logs	Low	SATA	4 128 KB	RAID 5	Off	Mixed Mixed
Oracle ASM	High	FC	4 1 MB	RAID 5	Off	Sequential Mixed
Performance Benchmark ¹	Premium	FC	All 64 KB	RAID 5	Off	Random Mixed
Streaming Media	Low	SATA	4 128 KB	RAID 5	Aggressive	Sequential Read
Web Files	Low	SATA	4 128 KB	RAID 5	Off	Random Read

Related concepts

- [About Storage Profiles](#)

¹ Stripes data across all available drives in the corresponding Storage Class. This profile is intended for use in benchmarking or in environments having a small number of logical volumes to be configured.

Important! Striping data across all available drives in a Storage Class can lead to unexpected contention in larger configurations.

About RAID Array Stripes

Pillar Axiom systems support RAID 5 and Distributed RAID geometries within the same Brick array.

Strips are disk block addresses. A RAID array stripe consists of a set of consecutively addressed strips.

RAID 5 arrays support the following strip sizes:

- For wide stripes: 1 MB for each strip.
- For standard stripes:
 - Fibre Channel (FC) Bricks: 64 KB for each strip.
 - Serial ATA (SATA) and solid-state drive (SSD) Bricks: 128 KB for each strip.

Distributed RAID arrays are formed from pairs of standard strips (64 KB strips for FC and 128 KB strips for SATA and SSD) only.

For FC Bricks, a stripe is a collection of 10 data strips and one parity strip. Each strip (64 KB) is written to one of the drives in a FC Brick, which means the stripe is written across 11 drives. For FC Bricks, a stripe also contains 640 KB, but its width is 11. Each FC Brick contains one such array, plus a hot spare.

For SATA and SSD Bricks, a stripe is a collection of five data strips and one parity strip. Each strip (128 KB) is written to one of the drives in a RAID array, which means the stripe is written across six drives. For SATA and SSD Bricks, a stripe contains 640 KB, and its width is six. Each Brick contains two such arrays, plus a hot spare.

For an Oracle Automatic Storage Management (ASM) storage profile, strips contain 1024 KB (1 MB). The number of strips for each stripe remains the same, depending on the type of Brick. Also, the stripe width does not change, only the size of the strip does.

About Enhanced Performance for Oracle ASM

You might be able to enhance the I/O throughput of a logical volume by using a 1 MB strip (sometimes called *Wide Stripe*) RAID geometry in an Oracle Automatic Storage Management (ASM) environment.

Using the Quality of Service (QoS)-based management tools provided by the Pillar Axiom Storage Services Manager, you might improve the overall performance of logical volumes in an ASM environment by taking advantage of an alternative internal structure of the RAID array. This alternative geometry provides a wide stripe by increasing the stripe width to 1 MB.

The system utilizes this alternative RAID geometry when you select the Oracle ASM performance profile in the Configuration Wizard. Selecting that profile allows the system to optimize the internal structure of the stripe that the RAID array implements so that I/O chunks match those of Oracle 10g systems that utilize ASM. Because Oracle ASM performs 1 MB random I/O operations as its normal access pattern, matching the stripe size utilized in the Brick to the I/O size utilized by Oracle ASM minimizes the I/O required to support a given Oracle ASM workload. LUNs created without the Oracle ASM profile use standard striping.

Related concepts

- [About Licensing Optional Premium Features](#)

About Managing Storage Profiles

You can use a Storage Profile to configure the Quality of Service (QoS) properties automatically when you create a logical volume.

A Storage Profile is defined as follows:

A set of Quality of Service (QoS) attributes that can be used to configure a logical volume. Pillar Data Systems provides a collection of Storage Profiles that are optimized for specific uses within an application context. Administrators can select one of the available profiles, create a new profile, or modify an existing profile.

Related concepts

- [About Storage Profiles](#)

Related references

- [System Storage Profile Properties](#)

Related tasks

- [Create a Storage Profile](#)
- [Delete a Storage Profile](#)
- [View Storage Profiles](#)

View Storage Profiles

Before using a Storage Profile to create a logical volume, you can display the Quality of Service (QoS) properties of the profile to determine whether those properties are appropriate for your needs.

The GUI lists two types of Storage Profile:

Advanced A custom profile that was created by a storage administrator.

System A Pillar-provided profile.

- 1 From the **Configure** navigation tab, click **Storage > Storage Profiles**.

Result:

The system displays for each profile the name, priority level, and redundancy property.

- 2 (Optional) To view additional properties, click **Actions > Manage Storage Profiles**

Result:

The system displays a complete list of QoS properties for all available profiles.

- 3 (Optional) To view all properties, click **Manage Advanced Storage Profiles**.

Result:

The system displays two additional QoS properties for all available profiles: the strip size and the number of RAID groups.

Related concepts

- [About Storage Profiles](#)

Related tasks

- [Create a Storage Profile](#)
- [Delete a Storage Profile](#)

Create a Storage Profile

You can create a Storage Profile that defines a collection of Quality of Service (QoS) properties that differ in some way to the Storage Profiles that have been predefined in the system.

You can create a standard Storage Profile or an advanced Storage Profile.

- When selecting *Standard* as the type that you want to create, you can define the regular set of QoS properties. These profiles appear in the list with a type of Custom.
- When selecting *Advanced* as the type that you want to create, you can define two additional properties: strip size and the number of RAID groups over which the data should be striped. These profiles appear in the list with a type of Advanced.

Important! When creating a Storage Profile, you should be familiar with the interactions among the attributes and the potential effects on system performance.

Pillar-supplied profiles are displayed with a type of *System*.

- 1 From the **Configure** navigation tab, click **Storage > Storage Profiles**.
- 2 Click **Actions > Manage Storage Profiles**.
- 3 Choose whether you want the standard list of QoS properties or an extended list.
 - To define the standard QoS properties, select the **Manage Standard Storage Profiles** option.
 - To define the standard QoS properties and the striping properties, select the **Manage Advanced Storage Profiles** option.

Result:

The system adjusts the list of properties according to the option you select. Also, the system changes the label on the *Create* button accordingly.

- 4 Choose the method of creating a Storage Profile.
 - To create a profile by defining each property individually, depending on your choice in the preceding step, click **Create Standard Profile** or **Create Advanced Profile**.
 - To create a profile by starting with the properties already defined, which are based on another profile, highlight the source profile and then click **Duplicate**.

- 5 Set the QoS properties as needed.

For the name of the Standard Profile, enter an appropriate value. For all other properties, select the desired value from the drop-down list.

- 6 To save the new Standard Profile, click **OK**.

Result:

After saving a profile, you cannot make changes to it. You can only delete the profile.

Related concepts

- [About Storage Profiles](#)
- [About Quality of Service](#)

Related references

- [Effects of Access Bias and I/O Bias](#)

Related tasks

- [Delete a Storage Profile](#)
- [View Storage Profiles](#)

Delete a Storage Profile

When a custom Storage Profile is no longer needed, you can remove it from the system.

- 1 From the **Configure** navigation tab, click **Storage > Storage Profiles**.
- 2 Click **Actions > Manage Storage Profiles**.
- 3 In the Manage Storage Profiles dialog, select the custom Storage Profile that you want to delete.

Only those Storage Profiles that have a type of Advanced can be deleted.

- 4 Click **Remove**.
- 5 To save all changes, click **OK**.

Result:

All Storage Profiles that you have removed from the list are deleted from the system.

Related concepts

- [About Storage Profiles](#)

Related tasks

- [Create a Storage Profile](#)
- [View Storage Profiles](#)

CHAPTER 6

Manage SAN Volumes and Hosts

Manage SAN LUNs

The graphical user interface (GUI) component of the Pillar Axiom Storage Services Manager provides a collection of dialogs that allow you to create, modify, and otherwise manage LUNs.

A LUN is defined as:

A logical volume within a storage area network (SAN). Administrators assign storage resources and Quality of Service (QoS) attributes to each logical unit (LUN).

For example, using the GUI, you can perform the following actions:

- Create a LUN.
- Modify the properties of a LUN.
- Map a LUN to specific SAN hosts.
- Move a LUN from one storage array to another.
- Activate or deactivate a LUN to affect its accessibility on the data path.
- Provide clone operations on a LUN for various purposes, including data protection.

You assign the storage resources and QoS attributes when you create the LUN. As needs change, you can at a later time modify the QoS attributes of the LUN, the storage capacity that is assigned to the LUN, or both.

Additionally, circumstances might arise during which you might want to disable the data path to the LUN. The Pillar Axiom Storage Services Manager provides a mechanism that allows you to make the LUN inaccessible along the public data path when the need arises.

Lastly, you can provide data protection for a LUN by cloning the volume. You can clone a LUN manually or create a schedule by which the system automatically creates a Clone LUN on a predefined basis.

Related concepts

- [About Creating LUNs](#)
- [About Modifying LUNs](#)
- [About Moving Logical Volumes](#)
- [About Copying Logical Volumes](#)

Related tasks

- [Disable the Data Path of a LUN](#)
- [Delete a LUN](#)

Connection Status of Slammer Ports

The system displays icons to indicate the connection status of the ports in the network interface module (NIM). These icons are displayed on the host overview page and on the host and LUN mapping pages.

Table 17 NIM port status










This icon...	Indicates
	A connected FC switch.
	A disconnected switch.
	An iSCSI point-to-point connection.
	An FC point-to-point connection.
	A disconnected host.
	An iSCSI connector.
	An FC connector.

Table 17 NIM port status (continued)

This icon...	Indicates
	A fully masked Slammer port.
	An unmasked Slammer port.

Related references

- [LUN to Host Mapping Overview Page](#)
- [Host to LUN Mapping Overview Page](#)

About Creating LUNs

The Pillar Axiom system calculates whether enough storage resources are available to create a new logical volume. The graphical user interface (GUI) provides graphs that represent the storage capacity requirements for the volume and a second graph that represents the overall system capacity requirements. The system updates the graphs as you adjust the Quality of Service (QoS) values for Storage Class and redundancy.

Note: The capacity values displayed in the usage graphs represent the sizes of the largest volume that you can create in a particular Storage Class, given one of two performance configurations.

You can specify the Storage Domain in which the LUN should be created. In this case, the system uses only those Bricks that are assigned to that domain. If you do not specify a particular domain, the system creates the volume in the default domain.

Note: After you have assigned a Brick to a Storage Domain, it is possible to reassign that Brick to a different domain.

You create a LUN by entering the QoS attributes on the Pillar Axiom Storage Services Manager screen. The Create LUN screen contains three tabs for entering the QoS information, one of which is required while the other two are optional.

Quality of Service (Required) This tab is the main dialog for creating a LUN and is where you configure the QoS attributes for a LUN. Assign your LUN to a volume group and to an

administer-defined Storage Domain, if any have been defined. You can also create a new volume group from the Membership tab.

Note: If no specific Storage Domains have been defined, the Storage Domain option does not appear.

Enter the LUN volume name, select a Storage Profile that contains predefined QoS attributes or, if necessary, choose custom QoS attributes.

Mapping

(Optional) The Mapping tab allows you to specify which SAN hosts can access the LUN. This specification can allow access by all hosts (all of which use the same LUN number) or just certain hosts (each of which can use a different LUN number as specified by the map assigned to the host).

Data Protection

(Optional) The Data Protection tab allows you to allocate the storage capacity for Clone LUNs. You can also create a clone schedule to perform data protection at regular intervals.

Related concepts

- [About Redundancy](#)
- [About Storage Classes](#)
- [About Storage Domains](#)
- [About Logical Volumes and Storage Domains](#)
- [Volume Capacity and Provisioning Overview](#)
- [About Storage Profiles](#)
- [About Licensing Optional Premium Features](#)

Related tasks

- [Create LUN: Define Quality of Service](#)
- [Create LUN: Define Mapping by LUN Number](#)
- [Create LUN: Define Mapping by Selected Hosts](#)
- [Create LUN: Define Data Protection](#)
- [Create a Storage Domain](#)
- [Create Volume Groups](#)
- [Reassign a Brick to Another Storage Domain](#)

About Logical Volumes and Storage Domains

The impact of creating a logical volume depends on whether administrator defined Storage Domains exist.

Table 18 Effect of Storage Domains on storage availability

Do administrator defined Storage Domains exist?	Impact
No	<p>All storage is available. The entire storage pool comprises the default Storage Domain.</p> <p>No choice exists in placing the logical volume on a specific set of Bricks.</p>
Yes	<p>Because storage is segmented, you need to select a specific Storage Domain when creating a logical volume. This fact can cause storage space to be under utilized.</p> <p>The system allocates the new volume using only those Bricks that reside in the specified domain.</p> <p>Note: A clone repository resides in the same Storage Domain in which the source volume resides.</p>

Related concepts

- [About Storage Domains](#)
- [About Moving Logical Volumes](#)
- [About Creating LUNs](#)
- [About Licensing Optional Premium Features](#)

Create LUN: Define Quality of Service

Define the Quality of Service (QoS) attributes to allocate the storage resources necessary to create the LUN.

The Pillar Axiom Storage Services Manager provides a predefined list of Storage Profiles that contain QoS attributes. When you select a Storage Profile the system automatically fills in the QoS fields on the screen with the values defined for the profile. You can create your own Storage Profile if you want to define a custom collection of QoS settings. This custom profile can then be selected from the Storage Profile list.

Storage Domains allow storage administrators to assign logical volumes to a specific collection of Bricks. Such assignments can be made to reduce contention among volumes, to implement different levels of security for those volumes, or both.

Volume groups allow you to group logical volumes into one administrative unit. You can then treat this volume group as a single, large volume.

- 1 From the **Configure** tab, click **Storage > SAN > LUNs**.
- 2 Choose **Actions > Create LUN**.
- 3 From the Quality of Service tab, enter a **Volume Name** for the LUN.
- 4 (Optional) From the Storage Domain drop-down list, select the Storage Domain to which you want to assign the LUN.

If necessary, click [...] to display a list of available storage domains.

Note: The Storage Domain drop-down list displays only when administrator-defined domains exist. The system assigns your LUN to the default Storage Domain if no administrator-defined domains exist or you do not assign it to a specific domain.

- 5 (Optional) From the Volume Group drop-down list, select the volume group to which you want the LUN to belong.

Note: If necessary, click [...] to create a new volume group.

- 6 Select a **Storage Profile** from the drop-down list.

Result:

The system updates the QoS attributes as defined by the selected profile.

Note: You can use the predefined attributes or modify them as needed.

- 7 (Optional) Select the necessary QoS attributes, such as Storage Class and I/O Bias.
- 8 (Optional) Select the **Background Copy Priority** level at which the system performs background copies.
- 9 Specify the **Allocated** and **Addressable** logical capacities for this volume.

Note: Use the storage capacity usage graphs to determine the impact on the storage requirements for the LUN.

- 10 (Optional) To create the LUN now, click **OK**.

Clicking **OK** creates the LUN using the default settings on the remaining tabs. You may perform the tasks associated with the other tabs to fine tune the remaining LUN properties. The default properties include:

- LUN assigned to the default Volume Group and Storage Domain
- Host mapping the same as the most recent LUN mapping

- Clone repository capacity that is sized to 10 GB with no scheduled automatic cloning taking place

Related concepts

- [About Creating LUNs](#)
- [About Priority Levels](#)
- [About Redundancy](#)
- [About I/O Bias](#)
- [About Access Bias](#)
- [About Storage Classes](#)
- [About Storage Profiles](#)
- [About Volume Groups](#)
- [About Storage Domains](#)
- [About Managing Storage Domains](#)

Related references

- [Effects of Access Bias and I/O Bias](#)
- [Manage Volume Groups Dialog](#)

Related tasks

- [Create LUN: Define Mapping by LUN Number](#)
- [Create LUN: Define Mapping by Selected Hosts](#)
- [Create LUN: Define Data Protection](#)
- [Create a Storage Profile](#)
- [Create Volume Groups](#)

Create LUN: Define Mapping by Selected Hosts

Mapping allows you to specify which SAN hosts can access the LUN. You can grant access to the LUN in one of two ways: assign a specific LUN number that any SAN host can use, or map specific hosts with unique LUN numbers. This procedure describes the steps to map the LUN to specific hosts and a different LUN number.

- 1 From the **Configure** tab, click **Storage > SAN > LUNs**.
- 2 Choose **Actions > Create LUN**.
- 3 From the Mapping tab, click the appropriate **Access Protocol**: either Fibre Channel (FC), iSCSI, or both.

This selection determines the protocols that will be permitted for accessing the LUN.

Important! When you select both FC and iSCSI protocols, the system uses FC optimized and non-optimized paths as a preference over iSCSI paths. Also, the system does not mix load balancing between protocols.

- 4 Click the option **Only selected hosts (via maps)**.

Result:

The system displays the Hosts mapping table.

- 5 Select the Slammer that will own the LUN by selecting an option from the **Assigned Slammer CU** drop-down list.

Choose one of:

Auto-assign

Assigns your LUN to an available Slammer. This option allows the Pilot to move resources to the other control unit (CU) in the event of a failover and maximizes performance by balancing the system load with existing logical volumes. You can modify this field after the LUN has been created.

Note: If you select this option, you cannot set up port masking and port mapping until after the LUN is created.

Slammer CU

Select a Slammer CU from the drop-down list. Use this option when you want to access the data from a particular port (port masking).

- 6 Below the hosts mapping table, click **Create**.
- 7 From the Create LUN Map dialog, define the mapping for the LUN, then click **OK** or **Apply**.

Type

Select **All Hosts**, **Recognized Hosts**, or **Unassociated Hosts**. Selecting an option other than **All Hosts** filters the list of host names.

Host Name

Select the host name to map to LUN.

LUN Number

Select the LUN number for this LUN.

Tip: If network clients are running on Windows 2000 or 2003 platforms and you want those clients to be able to access the LUN, do not choose LUN number 255.

Note: Clicking **Apply** allows you to map additional hosts to this LUN.

- 8 (Optional) From the Ports Masked for this LUN table, select **Yes** for each Slammer CU port that you want to mask.

Mask a port so that the LUN cannot be accessed from the specified ports.

Note: If you use Pillar Axiom LUN masking or switch zoning and do not use LUN assignment, you might create a situation in which a LUN is not exposed on the ports through which you want the clients to be able to access the LUN. To avoid this situation, Pillar recommends that you assign the LUN to the Slammer CU on which you have the mapping set.

- 9 (Optional) To save your changes and create the LUN, click **OK**.

If the iSCSI host that you want to allow access to the LUN is not displayed in the list, you can add it by using the Associate Hosts option. See [Associate a SAN Host](#).

Clicking **OK** creates the LUN using the default settings on the remaining tabs. You may perform the tasks associated with the other tabs to fine tune the remaining LUN properties. The default properties include:

- LUN assigned to the default Volume Group and Storage Domain
- Host mapping the same as the most recent LUN mapping
- Clone repository capacity that is sized to 10 GB with no scheduled automatic cloning taking place

Related concepts

- [About Creating LUNs](#)
- [About Licensing Optional Premium Features](#)

Related references

- [Create SAN LUN, Mapping Tab](#)

Related tasks

- [Create LUN: Define Quality of Service](#)
- [Create LUN: Define Mapping by LUN Number](#)
- [Create LUN: Define Data Protection](#)

Create LUN: Define Mapping by LUN Number

Mapping allows you to specify which SAN hosts can access the LUN. You can grant access to the LUN in one of two ways: assign a specific LUN number that any SAN host can use, or map specific hosts with unique LUN numbers. This procedure describes the steps necessary to map the LUN to a LUN number that any SAN host can use.

Sometimes you might want all SAN hosts to be able to access a LUN using the same unique LUN number. This approach requires that you not map any host to this LUN.

- 1 From the **Configure** tab, click **Storage > SAN > LUNs**.

- 2 Choose **Actions > Create LUN**.

- 3 From the Mapping tab, click the appropriate **Access Protocol**: either Fibre Channel (FC), iSCSI, or both.

This selection determines the protocols that will be permitted for accessing the LUN.

Important! When you select both FC and iSCSI protocols, the system uses FC optimized and non-optimized paths as a preference over iSCSI paths. Also, the system does not mix load balancing between protocols.

- 4 Click the option **All hosts may access the LUN using LUN number**.

- 5 Choose a LUN number from the drop-down list to assign to the LUN.

Tip: If network clients are running on Windows 2000 or 2003 platforms and you want those clients to be able to access the LUN, do not choose LUN number 255.

- 6 Select the Slammer that will own the LUN by selecting an option from the **Assigned Slammer CU** drop-down list.

Choose one of:

Auto-assign

Assigns your LUN to an available Slammer. This option allows the Pilot to move resources to the other control unit (CU) in the event of a failover and maximizes performance by balancing the system load with existing logical volumes. You can modify this field after the LUN has been created.

Note: If you select this option, you cannot set up port masking and port mapping until after the LUN is created.

Slammer CU

Select a Slammer CU from the drop-down list. Use this option when you want to access the data from a particular port (port masking).

- 7 (Optional) From the Ports Masked for this LUN table, select **Yes** for each Slammer CU port that you want to mask.

Mask a port so that the LUN cannot be accessed from the specified ports.

Note: If you use Pillar Axiom LUN masking or switch zoning and do not use LUN assignment, you might create a situation in which a LUN is not exposed on the ports through which you want the clients to be able to access the LUN. To avoid this situation, Pillar recommends that you assign the LUN to the Slammer CU on which you have the mapping set.

- 8 (Optional) To save your changes and create the LUN, click **OK**.

Clicking **OK** creates the LUN using the default settings on the remaining tabs. You may perform the tasks associated with the other tabs to fine tune the remaining LUN properties. The default properties include:

- LUN assigned to the default Volume Group and Storage Domain
- Host mapping the same as the most recent LUN mapping
- Clone repository capacity that is sized to 10 GB with no scheduled automatic cloning taking place

Related concepts

- [About Creating LUNs](#)
- [About Licensing Optional Premium Features](#)

Related references

- [Create SAN LUN, Mapping Tab](#)

Related tasks

- [Create LUN: Define Quality of Service](#)
- [Create LUN: Define Mapping by Selected Hosts](#)
- [Create LUN: Define Data Protection](#)

Create LUN: Define Data Protection

You can allocate clone capacity for your LUN and create a schedule Clone LUN to perform clone operations on a regular basis.

After the clone is created, the system administrator can change the performance level and other properties of the clone. When creating a Clone LUN, make sure enough storage space exists for the clone. A Clone LUN consumes space from the repository that was allocated for clones when the source LUN was created. The system stores in the clone storage space only the changes that are made to the source volume or to the clone.

- 1 From the **Configure** tab, click **Storage > SAN > LUN**.
- 2 Choose **Actions > Create LUN**.
- 3 From the **Data Protection** tab, enter a value for the Clone LUN capacity.

**Caution**

Pillar strongly recommends that you allocate sufficient repository capacity to minimize the chances of running out of this space (which could lead to data inconsistency or loss). To set sufficient capacity, use a value equal to the source volume capacity times the number of replicas times the maximum rate of change. For example, for a 100 GB volume that is projected to have 20 active replicas at a time and no more than a 20% rate of change, use a value of 400 GB for the clone repository.

- 4 (Optional) Click **Create** to create a new data protection schedule.

See [Create a Clone LUN Schedule](#).

- 5 (Optional) To save your changes and create the LUN, click **OK**.

Clicking **OK** creates the LUN using the default settings on the remaining tabs. You may perform the tasks associated with the other tabs to fine tune the remaining LUN properties. The default properties include:

- LUN assigned to the default Volume Group and Storage Domain
- Host mapping the same as the most recent LUN mapping
- Clone repository capacity that is sized to 10 GB with no scheduled automatic cloning taking place

Related concepts

- [About Creating LUNs](#)

Related references

- [Create SAN LUN, Data Protection Tab](#)

Related tasks

- [Create a Clone LUN Schedule](#)
- [Create LUN: Define Quality of Service](#)
- [Create LUN: Define Mapping by LUN Number](#)
- [Create LUN: Define Mapping by Selected Hosts](#)
- [Create LUN Data Protection Schedules](#)

Create a Clone LUN Schedule

You can create a schedule that instructs the system to clone a logical volume at regular intervals.

Note: A schedule should be synchronized with the host applications that access the logical volume so that all data I/O is quieted before the replication operation starts.

- 1 From the **Configure** tab, click **Storage > SAN > LUNs**.
- 2 Choose **Actions > Create LUN**.
- 3 From the Data Protection tab, click **Create**.
- 4 From the Create Job Schedule dialog, enter a name for the clone schedule in the **Schedule Name** field.

Tip: Use a meaningful name that includes the type of protection and frequency to help you identify the schedule in case you need to modify it later.

- 5 Select the data protection type, **Clone**.
- 6 Determine whether your replication schedule should go into effect immediately.
 - To start your schedule as soon as it is created, select the **Enabled** option.
 - To enable your schedule at a later time, clear the **Enabled** option.
- 7 To select a day and time for your schedule to start, click the expansion button to the right of **Start Time**.
- 8 Choose a frequency for your schedule.

Available frequencies:

- **Run Once**
- **Hourly**
- **Daily**
- **Weekly**

- 9 Choose a recurrence value for your schedule.

If you chose a frequency of **Weekly**, choose the day of the week you would like your report to be generated.

- 10 To save your schedule, click **OK**.

Result:

Your schedule is listed on the Clone Schedules table and the Protection Schedules overview page.

Related references

- [Data Protection Overview Page](#)
- [Create Job Schedule Dialog](#)
- [Create SAN LUN, Data Protection Tab](#)
- [Scheduled Jobs Overview Page](#)

Related tasks

- [Modify a LUN Data Protection Schedule](#)
- [Delete a LUN Data Protection Schedule](#)

Display LUN Details

You can display details about a selected LUN.

The LUN details include:

- Quality of Service (QoS) attributes
- Allocated storage capacity
- Volume group and Storage Domain associations
- SAN host mapping details and Slammer port masking assignments
- Clone capacity and cloning schedules

- 1 From the **Configure** tab, click **Storage > SAN > LUNs**.
- 2 Select the LUN you want to view.
- 3 To view details about the LUN, choose **Actions > View LUN**.
- 4 Select any of the tabbed pages to view the LUN properties.
- 5 Click **Close** when you are done.

Related references

- [View SAN LUN, Quality of Service Tab](#)
- [Modify SAN LUN, Quality of Service Tab](#)
- [Create SAN LUN, Quality of Service Tab](#)

About Modifying LUNs

You may need to modify the current Quality of Service (QoS) attributes for a LUN, such as increase the capacity or allocate space for Clone LUNs. You can

also modify the mapping of a LUN as well as change the Slammer and control unit (CU) to which the LUN is assigned, called re-homing.

Note: When you change the Storage Class of a logical volume, the volume is migrated to the new Storage Class but any existing clones of that volume are not.

You modify a LUN by entering the QoS attributes on the Pillar Axiom Storage Services Manager screen. The Modify LUN screen contains three tabs: one tab for entering the required QoS information, while the other two are optional.

Quality of Service	(Required) Allows you to change the assigned volume group or Storage Domain. You can also create a new group if one does not already exist. This tab also allows you to customize QoS attributes, including selecting a storage profile, storage class, redundancy, and other properties. You can also set the capacity limits for the LUN and view the effects that the selected QoS attributes would have on the storage class and overall system storage capacities.
Mapping	(Optional) Allows you to specify which SAN hosts can access the LUN. This specification can allow access by all hosts (all of which use the same LUN number) or just certain hosts (each of which can use a different LUN number as specified by the map assigned to the host).
Data Protection	(Optional) Allows you to allocate the storage capacity for Clone LUNs. You can also create a clone schedule to perform data protection at regular intervals.

Related tasks

- [Modify a LUN: Define Quality of Service](#)
- [Modify LUN: Define Mapping by LUN Number](#)
- [Modify LUN: Define Mapping by Selected Hosts](#)
- [Modify LUN: Define Data Protection](#)

Modify a LUN: Define Quality of Service

You may need to modify the current Quality of Service (QoS) attributes for a LUN, such as increase the capacity or allocate space for Clone LUNs. You can also modify the mapping of a LUN as well as change the Slammer and control unit (CU) to which the LUN is assigned.

- 1 From the **Configure** tab, click **Storage > SAN > LUNs**.
- 2 Select the LUN that you want to modify.

- 3 Choose **Actions > Modify LUN**.
- 4 From the Quality of Service tab, modify the necessary QoS attributes.
- 5 (Optional) Select any of the tabbed pages to update the LUN properties.
- 6 When you are finished making your updates, click **OK**.

Related concepts

- [About Modifying LUNs](#)
- [About Moving Logical Volumes](#)

Related references

- [Modify SAN LUN, Quality of Service Tab](#)

About Re-Homing LUNs

You can move a LUN within a Slammer or to another Slammer, which is called re-homing.

If you re-home (move) a LUN from one Slammer to another, the system re-configures the volume at the new location while attempting to maintain the integrity of the data.

**Caution**

If a client attempts to modify that volume while it is being moved, the client will lose its connection and data may become corrupted or lost. We strongly recommend that, before you re-home a volume, clients unmount the volume to ensure data integrity during the move.

Important! If the LUN is a member of a SAN replication pair, you should isolate the pair before re-homing the LUN to a different Slammer. For more information, see the *Pillar Axiom MaxRep Replication for SAN User's Guide and Reference*.

When re-homing a LUN from one CU to another on the same Slammer the operation is non-disruptive to client connections and I/O, including operations being performed by Pillar Axiom MaxRep Replication for SAN.

Related tasks

- [Modify a LUN: Define Quality of Service](#)

Modify LUN: Define Mapping by Selected Hosts

Mapping allows you to specify which SAN hosts can access the LUN. You can grant access to the LUN in one of two ways: assign a specific LUN number that any SAN host can use, or map specific hosts with unique LUN numbers. This

procedure describes the steps to modify the LUN mapped to specific hosts and a different LUN number.

- 1 From the **Configure** tab, click **Storage > SAN > LUNs**.
- 2 Select a LUN to modify.
- 3 Choose **Actions > Modify LUN**.
- 4 From the Mapping tab, select the host mapping to modify, and then click **Modify**.
- 5 From the Modify LUN Map dialog, select a new LUN to map for this LUN, then click **OK**.

Tip: If network clients are running on Windows 2000 or 2003 platforms and you want those clients to be able to access the LUN, do not choose LUN number 255.

- 6 (Optional) From the Ports Masked for this LUN table, select **Yes** for each Slammer CU port that you want to mask.

Mask a port so that the LUN cannot be accessed from the specified ports.

Note: If you use Pillar Axiom LUN masking or switch zoning and do not use LUN assignment, you might create a situation in which a LUN is not exposed on the ports through which you want the clients to be able to access the LUN. To avoid this situation, Pillar recommends that you assign the LUN to the Slammer CU on which you have the mapping set.

- 7 To save your changes and modify the LUN, click **OK**.

If the iSCSI host that you want to allow access to the LUN is not displayed in the list, you can add it by using the Associate Hosts option. See [Associate a SAN Host](#).

Related concepts

- [About Modifying LUNs](#)
- [About Licensing Optional Premium Features](#)

Related references

- [Modify SAN LUN, Mapping Tab](#)

Related tasks

- [Modify a LUN: Define Quality of Service](#)
- [Modify LUN: Define Mapping by LUN Number](#)
- [Modify LUN: Define Data Protection](#)

Modify LUN: Define Mapping by LUN Number

Mapping allows you to specify which SAN hosts can access the LUN. You can grant access to the LUN in one of two ways: assign a specific LUN number that any SAN host can use, or map specific hosts with unique LUN numbers. This procedure describes the steps necessary to modify the LUN number used by a SAN host to access this LUN.

Sometimes you might want to modify the LUN number that all SAN hosts use to access the LUN.

- 1 From the **Configure** tab, click **Storage > SAN > LUNs**.
- 2 Select a LUN to modify.
- 3 Choose **Actions > Modify LUN**.
- 4 From the Mapping tab, choose a LUN number from the drop-down list to assign to the LUN.

Tip: If network clients are running on those platforms and you want those clients to be able to access the LUN, do not choose LUN number 255.

- 5 (Optional) From the Ports Masked for this LUN table, select **Yes** for each Slammer CU port that you want to mask.

Mask a port so that the LUN cannot be accessed from the specified ports.

Note: If you use Pillar Axiom LUN masking or switch zoning and do not use LUN assignment, you might create a situation in which a LUN is not exposed on the ports through which you want the clients to be able to access the LUN. To avoid this situation, Pillar recommends that you assign the LUN to the Slammer CU on which you have the mapping set.

- 6 To save your changes and modify the LUN, click **OK**.

Related concepts

- [About Modifying LUNs](#)
- [About Licensing Optional Premium Features](#)

Related references

- [Modify SAN LUN, Mapping Tab](#)


Related tasks

- [Modify a LUN: Define Quality of Service](#)
- [Modify LUN: Define Mapping by Selected Hosts](#)
- [Modify LUN: Define Data Protection](#)

Modify LUN: Define Data Protection

You can modify the allocated clone capacity for your LUN and create or modify a schedule Clone LUN to perform clone operations on a regular basis.

- 1 From the **Configure** tab, click **Storage > SAN > LUN**.
- 2 Select the LUN that you want to modify.
- 3 Choose **Actions > Modify LUN**.
- 4 From the **Data Protection** tab, enter a value for the Clone LUN capacity.

 Caution	Pillar strongly recommends that you allocate sufficient repository capacity to minimize the chances of running out of this space (which could lead to data inconsistency or loss). To set sufficient capacity, use a value equal to the source volume capacity times the number of replicas times the maximum rate of change. For example, for a 100 GB volume that is projected to have 20 active replicas at a time and no more than a 20% rate of change, use a value of 400 GB for the clone repository.
--	--

- 5 (Optional) Click **Create** to create a new data protection schedule.
See [Create a Clone LUN Schedule](#).
- 6 (Optional) Click **Modify** to modify an existing data protection schedule.
See [Modify a LUN Data Protection Schedule](#).
- 7 (Optional) Click **Delete** to immediately remove an existing data protection schedule.
Note: You are not prompted to confirm the removal of the data protection schedule.
- 8 To save your changes to the LUN, click **OK**.

Related concepts

- [About Modifying LUNs](#)

Related references

- [Modify SAN LUN, Data Protection Tab](#)

Related tasks

- [Create a Clone LUN Schedule](#)
- [Modify a LUN Data Protection Schedule](#)
- [Modify a LUN: Define Quality of Service](#)
- [Modify LUN: Define Mapping by LUN Number](#)
- [Modify LUN: Define Mapping by Selected Hosts](#)
- [Create LUN Data Protection Schedules](#)

About Moving Logical Volumes

Sometimes you might need to move a logical volume from one Storage Domain to another.

When you move a volume to a different Storage Domain, the system prompts you to choose a new Storage Domain for the volume. If sufficient free capacity to migrate the data to the selected domain exists, the move request succeeds; otherwise, the system returns an error.

When the system migrates a volume to another domain, if the volume has a clone repository, the system does not migrate the repository. In this case, you must delete all clones associated with the volume before attempting to move that volume.

If the clone repository is empty, the system creates a new one in the new domain after the migration is complete.

Related concepts

- [About Storage Domains](#)

Related tasks

- [Move a Volume to Another Storage Domain](#)

Move a Volume to Another Storage Domain

Move a logical volume to another Storage Domain when you want to remove the Bricks on which the volume resides or reassign those Bricks to another Storage Domain.

The Storage Domain to which you want to reassign the logical volume must contain sufficient free capacity of the appropriate Storage Class to hold the logical volume.

Note: Assigning logical volumes and Bricks to a Pillar Axiom Storage Domain must be performed as separate actions.

Tip: To avoid performance issues caused by Brick striping, move the Bricks to the Storage Domain before you move any volumes.

- 1 From the **Configure** tab, click **Groups > Storage Domains**.
- 2 Choose **Actions > Manage Storage Domains**.
- 3 On the **Volumes** tab, click the Storage Domain for the logical volume that you want to reassign.

Result:

A drop-down list appears in the Storage Domain column.

- 4 In the Storage Domain drop-down list, choose the Storage Domain to which you want to reassign the logical volume.
- 5 Click **OK**.

Result:

One of the following will occur:

- If the operation is successful, the system begins a background task to migrate the volume to the new Storage Domain. Also, the system releases and reconditions the storage in the previous domain.
- If the operation is unsuccessful, the system does not migrate the volume but instead displays an appropriate error dialog:
 - The target domain does not contain any Bricks in the appropriate Storage Class. To resolve, add to the target domain one or more Bricks of the appropriate Storage Class.
 - The target domain has insufficient free capacity in the corresponding Storage Class. To resolve, remove unneeded volumes that consume capacity on the Bricks of that Storage Class.

Related concepts

- [About Storage Domains](#)
- [About Moving Logical Volumes](#)
- [About Adding Bricks to a Storage Domain](#)
- [About Licensing Optional Premium Features](#)

About Copying Logical Volumes

When you copy a logical volume that exists in a Storage Domain, the system stores the copy in the same domain in which the source volume resides.

For full block copies, you can place the copy in a different domain.

When complete, these copies are independent volumes.

Copy a LUN

You can copy an existing LUN and give the new LUN different Quality of Service (QoS) properties. This copying allows system resources to be maximized for the task at hand. For example, for a volume copy that is to be used for reporting purposes, you might want to assign to the copy a lower performance priority and a higher read-centric access pattern than you would assign to the source volume.

- 1 From the **Configure** tab, click **Storage > SAN > LUNs**.
- 2 Select a LUN, and choose **Actions > Copy LUN**.
- 3 From the **Quality of Service** tab, enter a **Volume Name** for the LUN copy.
- 4 Update the QoS parameters and remaining fields, selecting the tabs as necessary.
- 5 To create the new LUN, click **OK**.

Related concepts

- [About Copying and Cloning LUNs](#)

Related references

- [Create SAN LUN, Quality of Service Tab](#)

Disable the Data Path of a LUN

Sometimes you might want to remove the ability of a SAN host to access a LUN or Clone LUN but not remove the host mappings to the logical volume.

Disabling the data path to the logical volume prevents I/O operations on the volume. However, SAN host mappings are retained.

- 1 From the **Configure** tab, click **Storage > SAN > LUNs**.
- 2 Select the volume for which you want to disable the data path.
- 3 Choose **Actions > Disable Data Path**.
- 4 Click **OK** in the confirmation dialog to disable the data path for the selected volume.

On the LUN overview page, the Host Access status of the volume changes to *Inactive*. The LUN is now unavailable for use until the data path is enabled.

Related references

- [SAN LUNs Overview Page](#)
- [SAN LUN Protection Overview Page](#)

Related tasks

- [Enable the Data Path of a LUN](#)

Enable the Data Path of a LUN

When the data path to a LUN has been disabled, you might want to provide the ability of a SAN host to access that LUN using the host mappings already established.

The LUN overview page identifies the Host Access status of a disabled LUN as *Inactive*. Enabling the data path to a volume restores the communication between the mapped SAN host and the volume.

- 1 From the **Configure** tab, click **Storage > SAN > LUNs**.
- 2 Select the volume that you want to enable from the data path.
- 3 Choose **Actions > Enable Data Path**.
- 4 Click **OK** in the confirmation dialog to enable the data path for the selected volume.

On the LUN overview page, the Host Access status of the volume changes from *Inactive* to the original status.

Related references

- [SAN LUNs Overview Page](#)
- [SAN LUN Protection Overview Page](#)

Related tasks

- [Disable the Data Path of a LUN](#)

Delete a LUN

Sometimes you might not need a LUN any longer, such as one that is no longer in use. You can delete an existing volume if the volume is not being accessed.

Note: When you delete a LUN that is a parent or source for Clone LUNs, all child clones are deleted as well.

- 1 From the **Configure** tab, click **Storage > SAN > LUNs**.
- 2 Select the LUN you want to delete.
- 3 Choose **Actions > Delete LUN**.

Result:

The system displays the Delete LUN dialog with a list of the LUN and affected clones that will be deleted.

- 4 Select the option **Delete LUNs and existing host mappings**.

Note: The system displays this option when the LUN you are deleting contains host mappings. Deleting a LUN that has host mappings causes each of those hosts to lose access to the LUN.

- 5 When prompted to confirm the deletion, click **OK**.

Related concepts

- [About Copying and Cloning LUNs](#)

Related references

- [SAN LUNs Overview Page](#)

Related tasks

- [Delete a Clone LUN](#)
- [Delete All Clone LUNs](#)

About SAN Host Management

The graphical user interface (GUI) component of the Pillar Axiom Storage Services Manager provides a collection of dialogs that allow you to configure a SAN Slammer storage controller so that it can connect successfully to hosts in the storage area network (SAN).

The configuration of a SAN Slammer includes the following tasks:

- Configure the Fibre Channel (FC) or iSCSI ports in the Slammer for network access. When these ports are configured properly, a successful connection can be made from the initiator ports on the SAN host to the target ports on the Slammer.
- Optionally provide an alias for the initiator ports on the SAN host.
- Specify the secret for the Challenge Handshake Authentication Protocol (CHAP), if applicable. This setting enables the Slammer iSCSI ports to communicate successfully with a SAN host.
- Optionally map selected SAN hosts to a LUN. Mapping is the mechanism that enables these hosts to identify and access the LUN.
- Optionally mask a Slammer port so that the LUN cannot be accessed through that port.

You can install the Pillar Axiom Path Manager (APM) application on a SAN host to manage the initiator ports on the host and the data paths between the host and the Pillar Axiom system. When the APM application is installed on a host, all of the initiator ports are automatically associated with the host. Such a host is referred to as an *associated host*.

An *associated host* is one that is associated with one or more of its initiator ports. An *unassociated host* is one that is not associated with any initiator ports.

The APM application also automatically provides a variety of information to the system on a continuous basis. For a SAN host that is managed by APM, the GUI shows the host as an associated host and its status as Registered.

Note: For a SAN host that is not running the APM application, you can manually associate a Slammer port with a SAN host.

If APM is installed on the SAN host, you can perform the following actions:

- Use APM to manage the multiple access paths to the Pillar Axiom system.
- Use the Pillar Axiom Storage Services Manager to verify the connection status of each initiator port on the host.

For more information about APM, refer to the *Pillar Axiom Path Manager Installation Guide and Release Notes* for the appropriate SAN host platform.

To enable a SAN host that is not running APM so it can access Pillar Axiom LUNs, you need only perform the following actions on the host:

- Configure the authentication method that is to be used when the SAN host connects to the Pillar Axiom system.
- Discover and connect to the configured Slammer ports.

Related concepts

- [About Modifying SAN Hosts](#)

Related tasks

- [Display SAN Host Settings](#)
- [Delete a SAN Host Entry](#)
- [Associate a SAN Host](#)

Display SAN Host Settings

You can display details about the Pillar Axiom Path Manager SAN host driver settings and LUN connection status as well as configure iSCSI settings.

- 1 From the **Configure** tab, click **Storage > SAN > Hosts**.
- 2 From the Hosts overview page, select a SAN host to view.
- 3 Choose **Actions > View Host**.
- 4 Select any of the tabbed pages to view the host properties.
- 5 Click **Close** when done.

Related concepts

- [About Modifying SAN Hosts](#)

Related references

- [View Host, Ports Tab](#)
- [Modify Host, iSCSI Access Tab](#)

About Modifying SAN Hosts

You can modify information about a SAN Host including adding an alias name for a host, adjusting the Pillar Axiom Path Manager (APM) load balancing setting,

enabling the iSCSI host Challenge Handshake Authentication Protocol (CHAP) authentication and setting the HP-UX compatibility mode.

You can change the LUN settings of the SAN host drivers only when the drivers are installed and can communicate with the Pillar Axiom system.

Also, if you have SAN hosts that access the LUNs using HP-UX initiator ports and HP HBAs, you can enable the HP-UX option. When this option is enabled, the system determines LUN numbers using the HP-UX addressing scheme, allowing up to 255 LUNs. Also when enabled, the host cannot have a visible LUN using ID 0.

Modify the host by using the following tabbed dialogs as necessary:

- **Ports:** Allows you to create or modify a host alias and view Fibre Channel (FC) and iSCSI port information.
- **Pillar Axiom Path Manager:** Allows you to view the installed APM version and path manager settings. From this page you can modify the load balancing settings, and view the number of optimized and non-optimized data paths.
- **iSCSI Access:** If you select a host with an iSCSI connection you can manage the CHAP authorization and grant access to the Pillar Axiom system.
- **Advanced:** If your configuration accesses LUNs that have HP initiator ports and HP host-bus adapters (HBAs), you can set the HP-UX compatibility mode option from this dialog.

Related tasks

- [Modify a Host: Reconfigure Port Settings](#)
- [Modify a Host: Reconfigure APM Settings](#)
- [Modify a Host: Reconfigure iSCSI Access Settings](#)
- [Modify a Host: Reconfigure Advanced Settings](#)

Modify a Host: Reconfigure Advanced Settings

If you have SAN hosts that access the LUNs using HP-UX initiator ports and HP HBAs, you can enable the HP-UX compatibility option.

When the HP-UX compatibility option is enabled, the system determines the LUN numbers by using the HP-UX addressing scheme, allowing up to 255 LUNs.

Note: When enabled, the host cannot have a visible LUN using ID 0.

- 1 From the **Configure** tab, click **Storage > SAN > Hosts**.
- 2 Select a host from the list to modify.

- 3 Choose **Actions > Modify Host**.
- 4 From the **Advanced** tab, select **HP-UX Compatibility Mode** to enable HP HBA and LUN addressing scheme.
- 5 To save your changes, click **OK**.

Related concepts

- [About Modifying SAN Hosts](#)

Related references

- [Modify Host, Advanced Tab](#)

Modify a Host: Reconfigure APM Settings

You can change the load balancing method that the Pillar Axiom Path Manager (APM) uses to access LUNs.

- 1 From the **Configure** tab, click **Storage > SAN > Hosts**.
- 2 Select a host from the list to modify.
- 3 Choose **Actions > Modify Host**.
- 4 From the **Pillar Axiom Path Manager** tab, select a LUN, then choose a **Load Balancing** method from the drop-down list.
- 5 To save your changes, click **OK**.

Related concepts

- [About Modifying SAN Hosts](#)

Related references

- [Modify Host, Pillar Axiom Path Manager Tab](#)

Modify a Host: Reconfigure iSCSI Access Settings

If you need to allow iSCSI initiator access to the Pillar Axiom system, enable the Challenge Handshake Authentication Protocol (CHAP) option and grant access to the system.

- 1 From the **Configure** tab, click **Storage > SAN > Hosts**.
- 2 Select an iSCSI host from the list to modify.
- 3 Choose **Actions > Modify Host**.

- 4 From the iSCSI Access tab, select **Enable Authentication** to allow CHAP authentication credentials.
- 5 Enter the necessary CHAP credentials in the fields provided.
- 6 (Optional) Select **Grant Access to Axiom** to allow iSCSI initiator login attempts to the Pillar Axiom system.
- 7 To save your changes, click **OK**.

Related concepts

- [About Modifying SAN Hosts](#)

Related references

- [Modify Host, iSCSI Access Tab](#)

Modify a Host: Reconfigure Port Settings

You can provide an alias as part of the host port information to make the host easier to identify.

- 1 From the **Configure** tab, click **Storage > SAN > Hosts**.
- 2 Select a host from the list to modify.
- 3 Choose **Actions > Modify Host**.
- 4 From the **Ports** tab, select a host from the list.
- 5 Enter an **Alias** name for the port you wish to modify.
- 6 To save your changes, click **OK**.

Related concepts

- [About Modifying SAN Hosts](#)

Related references

- [Modify Host, Ports Tab](#)

Modify iSCSI Port Settings

You can change the default values of the iSCSI port settings. For example, you may need to change the maximum transmission unit (MTU) of a port in one of the Slammer control units.

The default for all iSCSI ports is to receive the IP address, subnet mask, and gateway using Dynamic Host Configuration Protocol (DHCP). If you want to

manually assign these values, modify each port with the values that you want to use.

- 1 From the **Configure** tab, click **Storage > SAN > Slammer Ports**.
- 2 From the Slammer Ports overview page, select a Slammer that contains iSCSI ports that you want to modify.
- 3 Choose **Actions > Modify iSCSI Port Settings**.
- 4 Make any necessary changes and click **OK**.

Related references

- [Modify iSCSI Port Settings Dialog](#)

Delete a SAN Host Entry

If you need to delete an existing SAN host, you can do so regardless whether the host is connected to the network.

- 1 From the **Configure** tab, click **Storage > SAN > Hosts**.
- 2 From the Hosts overview page, select the host that you want to delete.
- 3 Choose **Actions > Delete Host**.
- 4 When prompted to confirm the deletion, click **OK**.

Related references

- [SAN Hosts Overview Page](#)
- [Modify Host, Ports Tab](#)

Associate a SAN Host

You can create a host-to-HBA association when you do not have the Pillar Axiom Path Manager driver installed on the SAN host.

You can do this for hosts that are listed as *unknown* and are referenced by the World Wide Name (WWN) for Fibre Channel hosts or iSCSI Qualified Name (IQN) for iSCSI hosts of their HBA.

- 1 From the **Configure** tab, click **Storage > SAN > Hosts**.
- 2 Click **Actions > Associate Hosts**.

- 3 Enter a name for the host or select a host to associate from the drop-down list.
- 4 From the Create Association dialog box, select or add an HBA to use from the WWNs or iSCSI list that is not yet detected by the system.
- 5 (Optional) Enter the authentication settings for the specific host.
- 6 (Optional) Click **Remove** to delete the current associations.
- 7 Click **OK** to save your changes.

Related references

- [Associate Hosts Dialog](#)

About Host Groups

You can easily manage the mapping of a LUN to SAN hosts by assigning the hosts to a specific group. This group is a named, logical collection of SAN hosts.

You might have SAN hosts that have been registered by the Pillar Axiom Path Manager (APM) application or might have created a host association for various initiators. You can create additional host associations by using existing APM registered or manually created hosts. This activity is useful if you have host clusters, each of which contains many hosts and each host contains a few initiators.

If this host cluster is not defined in the GUI as a host group, when you want to map a LUN to the cluster, you need to map each SAN host to the LUN one at a time. Furthermore, if you need to move a host to a different cluster, you must manually update each LUN mapping, also one at a time.

A more efficient method, however, is to define the cluster as a host group and then assign the SAN hosts to the host group. When you subsequently move a host from one host group to another, all the initiators associated with that host inherit the LUN mappings associated with that host group.

Note: The Pilot automatically manages the deletion of the old mappings and the creation of the new initiator mappings.

Host groups have the following properties:

- A host can belong to only one host group.
- You can map unlimited hosts to a host group.
- A host group can have zero or more mappings.
- You can map a LUN to either a host or a host group.

- If a host group has mappings, then all hosts in the host group will have all of the mappings of the host group, but any given host may also have other mappings. No mappings may conflict.
- When assigning a host with mappings to a host group without mappings, you will have the option to migrate mappings on the host to the host group, making those mappings available to all hosts in the group, not just the single host.

For example, consider the following host group (cluster) configuration:

Host group Alpha LUN1 is mapped to this host group as LUN number 0.

Host A Initiators A1 and A2 are mapped to LUN1. The LUN number is 0.

Host B Initiators B1 and B2 are mapped to **LUN1**. The LUN number is 0.

Host group Omega LUN2 is mapped to this host group as LUN number 0.

Host C Initiators C1 and C2 are mapped to LUN2. The LUN number is 0.

If you move Host B from host group Alpha to host group Omega, the LUN mappings for Host B are automatically adjusted, as shown below:

Host group Alpha LUN1 is mapped to this host group as LUN number 0.

Host A Initiators A1 and A2 mapped to LUN1. The LUN number is 0.

Host group Omega LUN2 is mapped to this host group as LUN number 0.

Host B Initiators B1 and B2 are mapped to **LUN2**. The LUN number is 0.

Host C Initiators C1 and C2 are mapped to LUN2. The LUN number is 0.

Related concepts

- [About SAN Host Management](#)

Related tasks

- [Create a SAN Host Group](#)
- [Modify a SAN Host Group](#)

About Managing Host Groups

Managing host groups involves understanding the host mappings to the hosts groups and host access to the LUNs.

To use the host group feature, first create the host group, then assign your hosts to the group. After the host group is created and the hosts assigned to the group, you can map your LUNs to the host group. A host that is assigned to a host group is still available for mapping by way of the host or the host group to which it is assigned.

When deleting a host group, remove the host members first. Ideally, you would delete an empty host group that contains no host memberships. Emptying a host group involves mapping each host to another group or removing the host from the group. This action might affect the current host-to-LUN mapping. After moving a mapped host to another host group, you will receive a confirmation to unassociate the host from the host group.

The system displays the confirmation to unassociate a host from a host group when there are LUNs mapped to a group. You can decide how you want the system to process the residual mappings. You are presented with two options:

- **Retain Host Mappings:** Allows you to copy all mappings for the deleted host group to the hosts to which the LUN was a member. The hosts that belonged to the deleted host group will retain access to any LUNs to which they had access while a member of their host group.
- **Delete Mappings:** Allows you to remove all mappings for the deleted host group. The hosts that belonged to the deleted host group will lose access to any LUNs to which they had access while a member of the host group. Choosing this option causes the message *No Mappings* to appear in the LUNs overview page if the LUN is not assigned to a host or host group. Any LUNs that are mapped to the host (and not to the host group) are not affected by Delete Mappings option.

Related concepts

- [About Host Groups](#)

Related tasks

- [Create a SAN Host Group](#)
- [Delete a SAN Host Group](#)

Create a SAN Host Group

You can create a host group that allows you to associate registered SAN hosts into logical organizational units.

- 1 From the **Configure** tab, click **Storage > SAN > Hosts**.
- 2 Choose **Actions > Manage SAN Host Groups**.
- 3 From the Manage SAN Host Groups dialog, click **Create**.
- 4 Enter a name for the host group.
- 5 (Optional) From the Hosts tab, assign the host to an available host group.
- 6 To save your changes, click **OK**.

Related concepts

- [About Host Groups](#)
- [About SAN Host Management](#)

Related references

- [Manage SAN Host Groups, Groups Tab](#)
- [Manage SAN Host Groups, Hosts Tab](#)

Modify a SAN Host Group

You can modify a host group by changing its name, assigning new hosts to the group, or removing existing hosts from the group.

- 1 From the **Configure** tab, click **Storage > SAN > Hosts**.
- 2 Choose **Actions > Manage SAN Host Groups**.
- 3 From the Manage SAN Host Groups dialog, modify the host group.

Valid modifications:

Change the host group name

From the **Group** tab, select a host group and update the name.

Reassign a host to a new host group

From the **Hosts** tab, select a host and choose a new host group from the **Host Group** drop-down list.

Remove a host from a host group

From the Hosts tab, select a host and choose [--] from the Host Group drop-down list.

Delete a host group

Follow the instructions in *Delete a SAN Host Group*.

- 4 To save your changes, click **OK**.

Related concepts

- [About Host Groups](#)

Related references

- [Manage SAN Host Groups, Groups Tab](#)
- [Manage SAN Host Groups, Hosts Tab](#)

Related tasks

- [Create a SAN Host Group](#)
- [Delete a SAN Host Group](#)

Delete a SAN Host Group

Delete a host group when the group is no longer needed.

When possible, delete a host group that contains no hosts. If you delete a host group that contains hosts, the system prompts you for more action on how to map the hosts.

- 1 From the **Configure** tab, click **Storage > SAN > Hosts**.
- 2 Choose **Actions > Manage SAN Host Groups**.
- 3 From the Manage SAN Host Groups, Groups tab, select a host group from the available list.
- 4 Click **Delete**.

Result:

The host group is removed from the list.

- 5 To save your changes, click **OK**.

Result:

If the host group was empty when you deleted it, the system deletes the host group from the system. However, if the host group contains mapped hosts, additional information is required about how to map the LUNs that were mapped to the host group that you just deleted.

- 6 (Optional) From the Confirm SAN Host Group Unassociation of Hosts dialog, specify how the LUN mappings are processed for the mapped hosts.

Valid options:

- Retain Host Mappings
- Delete Mappings

7 To save your changes, click **OK**.

We recommend that you review the *Host Access* status from the LUNs overview page for the affected LUNs.

Related concepts

- [About Host Groups](#)
- [About SAN Host Management](#)

Related references

- [Manage SAN Host Groups, Groups Tab](#)
- [Manage SAN Host Groups, Hosts Tab](#)

Related tasks

- [Create a SAN Host Group](#)

Download and Install the Pillar Axiom VDS Provider

The Pillar Axiom Virtual Disk Service (VDS) Provider plug-in allows you to use the Disk Administrator on a Windows 2003 server to configure and manage LUNs on a Pillar Axiom system.

Prerequisites:

- System serial number
- Login account: username
- Login account: password

The plug-in installer allows the configuration of a single Pillar Axiom system at the time of installation. Additional systems may be configured from a command line tool. A default location for the installation is presented on the installation screen, which you can change during installation.

- 1 From the **Support** tab, click **Utilities**.
- 2 In the Utilities content pane, click **Pillar Axiom VDS Provider** link for your operating system type.
- 3 Save the file to a client workstation.
- 4 Double-click the file to begin the installation.
- 5 Follow the instructions to install the VDS Provider plug-in on your SAN host.
- 6 Click Close at the Installation Complete page to close the VDS Provider Installer wizard.
- 7 Restart the Windows server.

Restarting permits the `diskraid` utility to see the VDS providers.

Once the installation completes, you can verify it by running `diskraid.exe` at a command prompt and issuing the command `ListProviders` within `diskraid`.

For the Pillar Axiom VDS Provider to be able to manage a Pillar Axiom system, it must be connected using Fibre Channel. Be sure to register it by using the `registerAxiom.exe` tool available in the `bin` folder in the installation directory.

This registration tool has two functions, add and remove registry entries. Running `registerAxiom.exe` prints the usage directions.

To add a registry entry:

```
registerAxiom.exe sample-serial user-password
```

To remove a registry entry:

```
registerAxiom.exe sample-serial
```

Related references

- [Virtual Disk Service \(VDS\) Page](#)

CHAPTER 7

Manage Data Protection

About Data Replicas and System Capacity

You can create online data replicas in different ways. Each method consumes the capacity in the storage array differently.

The Pillar Axiom system ensures that all logical volumes that are associated with a particular replica tree reside on² the same Slammer control unit (CU).³ If you change the home of any of these logical volumes, the system changes all of them. This feature applies to all of the following objects:

- Clone LUNs
- Volume Copies
- Active data migrations because of Quality of Service (QoS) changes

Volume Copies and logical volumes that are being migrated due to QoS changes continue to reside in the original replica tree until the data operations are complete. Once the Volume Copy or the migration completes, the volume is removed from the original replica tree and becomes the root of a new replica tree.

However, after you start a Volume Copy operation or the system starts a data migration operation, if you re-home anything in the replica tree, the mechanics are a little different. If the system has not yet detached the copy from its source volume, the copy will be re-homed. If, however, the system has already detached the copy, the copy is no longer in the original replica tree and, so, is not re-homed.

Table 19 Capacity usage by online data replicas

Method	Description	Capacity usage
Clone LUN	Creates a readable and writable point-in-time snapshot of a LUN.	Consumes system space allocated for clones. Only changes

² Sometimes the term *homed on* or *owned by* is used instead of *reside on*.

³ This discussion of replica trees on a Slammer CU does not apply to replicated objects created by the Pillar Axiom MaxRep Replication for SAN utilities.

Table 19 Capacity usage by online data replicas (continued)

Method	Description	Capacity usage
		to the source or clone are stored.
Volume Copy	Creates a block-level, full-image, read-write copy of a logical volume. QoS attributes for a Volume Copy can differ from the QoS attributes of the original.	Consumes free space from system capacity that is equal to the current size of the volume.

The online data replicas identified in the preceding table have the following characteristics:

- They require no prior configuration (other than the initial allocation).
- They are created by explicit one-time operations.
- They are created on the same Pillar Axiom system as the source volume.
- Updates to the source volume are not reflected in the replica. When data changes in the source volume, that change *is not* reflected in the replica.

Note: A Pillar Axiom system uses binary units to calculate and display the capacity of physical storage and the size of logical volumes:

1 MB = 1024^2 (1,048,576) bytes

1 GB = 1024^3 (1,073,741,824) bytes

1 TB = 1024^4 (1,099,511,627,776) bytes

About Copying and Cloning LUNs

You can copy an existing LUN and give the new LUN different Quality of Service (QoS) properties. This copying allows system resources to be maximized for the task at hand. For example, for a volume copy that is to be used for reporting purposes, you might want to assign to the copy a lower performance priority and a higher read-centric access pattern than you would assign to the source volume.

Copy a Clone LUN when you want to test a new application on an exact copy instead of on the original LUN. A Clone LUN is a point-in-time, read-write copy of a LUN that you can immediately use. A Clone LUN retains the same Quality of Service (QoS) parameters as the source LUN and consumes storage capacity from the Clone LUN storage space created for the source LUN. A Clone LUN is available immediately after creation. Clone LUNs provide a convenient method to branch from the source data without the need to do a full block-level copy.

Copy a LUN when you need a new LUN with the same starting data as an existing LUN.

Another reason to create a clone or a copy is to preserve a point-in-time view of the data. If you create a clone for this purpose, at a later time you can restore the data to the source LUN.

Unlike a clone, the new blocks for the copy may be on a different set or even a different type of Brick. In other words, a volume copy of a Fibre Channel or solid state drive (SSD) based, premium priority LUN may be created in the low-priority band on SATA Bricks.

Related concepts

- [About Creating LUNs](#)

Related tasks

- [Copy a LUN](#)
- [Create an Immediate Clone LUN](#)
- [Create LUN Data Protection Schedules](#)

View Protection Schedules

You can display a complete list of schedules for the Pillar Axiom system. The schedules overview page displays the schedule name, the start time, the name of the protected volume, and whether the schedule is enabled. This page provides options to view, modify, and delete selected scheduled jobs.

- 1 From the **Protect** tab, click **Data Protection > Protection Schedules**.
- 2 Ensure that the overview page for protection schedules contains the information that you expect.

Result:

You can create, modify, delete, and view data protection schedules from the overview page.

Related references

- [Scheduled Jobs Overview Page](#)
- [Protection Schedules Overview Page](#)

Related tasks

- [Create LUN Data Protection Schedules](#)
- [Modify a LUN Data Protection Schedule](#)
- [View a LUN Data Protection Schedule](#)
- [Delete a LUN Data Protection Schedule](#)

About Managing Clone LUNs

Clone LUNs are writable snapshots of a LUN using partial-block snapshot technology. You can create an immediate Clone LUN at any time.

A Clone LUN is defined as:

A point-in-time, read-write, partial-block snapshot of a LUN that can be accessed immediately. A Clone LUN retains the same QoS parameters as the source LUN and consumes storage capacity from the Clone LUN repository that was allocated for the source LUN.

Important! Make sure that the clone space does not fill up, consuming the maximum amount of space allocated. We strongly recommend that you monitor the amount of space available and modify the volume to allocate more clone space as needed.

Related concepts

- [About Copying and Cloning LUNs](#)

Related references

- [System Components That Can Be Monitored](#)
- [Create SAN Clone LUN, Quality of Service Tab](#)

Related tasks

- [Create an Immediate Clone LUN](#)

Create an Immediate Clone LUN

You can create Clone LUNs from an existing LUN or Clone LUN.

When creating a Clone LUN, make sure enough storage space exists for the clone. A Clone LUN consumes space from the repository that was allocated for clones when the source LUN was created.

- 1 From the **Configure** tab, click **Storage > SAN > LUNs**.
- 2 Select the volume from which you want to create an immediate clone.
- 3 Choose **Actions > Clone LUN**.
- 4 From the Quality of Service tab, enter a new **Volume Name** for the Clone LUN.
- 5 (Optional) Set the **Priority Level** and **Maximum Logical Capacity** for the Clone LUN.

- 6 (Optional) Click the Mapping tab and set the mapping and host connections for the Clone LUN.
- 7 To create the Clone LUN, click **OK**.

The name of the new Clone LUN will appear on the SAN LUNs overview page, indented beneath the source volume.

Related concepts

- [About Managing Clone LUNs](#)
- [About Copying and Cloning LUNs](#)

Related references

- [Create SAN Clone LUN, Quality of Service Tab](#)

Related tasks

- [Create LUN: Define Data Protection](#)

Delete a Clone LUN

You can delete a single Clone LUN.

When you delete a Clone LUN, only the target clone is deleted. In other words, if the target clone is the parent or source for other clones, the child clones *are not deleted*. Instead, the child clones become children of the next higher parent in the hierarchy.

- 1 From the **Configure** tab, click **Storage > SAN > LUNs**.
- 2 Select the Clone LUN that you want to delete.
- 3 Choose **Actions > Delete LUN**.

Note: The system displays the Delete LUN dialog. This dialog indicates that, if this clone is a parent or source of additional clones, those other clones will not be deleted.

- 4 Select the option **Delete LUNs and existing host mappings**.

Note: The system displays this option when the LUN you are deleting contains host mappings. Deleting a LUN that has host mappings causes each of those hosts to lose access to the LUN.

- 5 To delete the highlighted Clone LUN, click **OK**.

If this Clone LUN has child clones, those child clones move up one level in the hierarchy of clones.

Related concepts

- [About Copying and Cloning LUNs](#)

Related references

- [SAN LUNs Overview Page](#)

Related tasks

- [Delete All Clone LUNs](#)

Delete All Clone LUNs

When a collection of Clone LUNs that are derived from a common source LUN are no longer needed, you can delete the entire collection.

When you delete a collection of clones that have a common parent LUN, the system determines the most efficient and quickest order of deletion.

- 1 From the **Configure** tab, click **Storage > SAN > LUNs**.
- 2 Select the parent LUN of all of the Clone LUNs that you want to delete.
- 3 Choose **Actions > Delete Clones**.

Result:

The system displays the Delete Clones dialog with a list of all the clones that will be deleted.

- 4 When prompted to confirm the deletion, click **OK**.

Related concepts

- [About Copying and Cloning LUNs](#)

Related references

- [SAN LUNs Overview Page](#)

Related tasks

- [Delete a Clone LUN](#)
- [Delete a LUN](#)

Display Clone LUN Details

Occasionally, you might want to view specific information about a Clone LUN, such as the host mappings for the clone.

The details of a Clone LUN include the following:

- Quality of Service (QoS) attributes

- Allocated storage capacity
 - Volume group and Storage Domain memberships
 - SAN host mapping details and Slammer port masking assignments
 - Clone capacity and cloning schedules
- 1 From the **Configure** tab, click **Storage > SAN > LUNs**.
 - 2 Select the Clone LUN that you want to view.
 - 3 To view details about the LUN, choose **Actions > View LUN**.
 - 4 Select any of the tabbed pages to view the LUN properties.
 - 5 Click **Close** when you are done.

Related concepts

- [About Copying and Cloning LUNs](#)
- [About Managing Clone LUNs](#)

Related references

- [View SAN LUN, Quality of Service Tab](#)
- [Modify SAN LUN, Quality of Service Tab](#)
- [Create SAN LUN, Quality of Service Tab](#)

Related tasks

- [Create an Immediate Clone LUN](#)

Restore a LUN from a Clone LUN

You can restore a particular LUN back to its state that you previously captured through a Clone LUN.

Restoring a LUN from a Clone LUN uses partial block snapshot technology, which allows the LUN to keep its same identity and to come back online in a short amount of time, especially when compared to copying the entire data set back from a tape backup. This restoration process copies only that data that was modified after the snapshot was taken. Furthermore, this process allows access to the data while the background copy is in progress.

Such restoration is often used to restore a LUN to a known good image in various scenarios, including:

- Some undesirable changes were made.
- An external client application or virus corrupted the LUN.

- 1 From the **Configure** tab, click **Storage > SAN > LUNs**.
- 2 From the SAN LUNs overview page, select the Clone LUN from which you want to restore the LUN.
Note: The restoration process resets the creation date of the LUN to that of the selected Clone LUN.
- 3 Choose **Actions > Restore from Clone**.
- 4 In the Restore from Clone dialog, click **OK**.

The system restores the LUN, during which time system performance may be slightly degraded. The system starts a task in the background to perform the copy operation. When the background task completes, the system writes an event to the event log.

Related concepts

- [About Creating LUNs](#)
- [About Copying and Cloning LUNs](#)

Related references

- [SAN LUNs Overview Page](#)

Related tasks

- [Display LUN Details](#)
- [Enable the Data Path of a LUN](#)
- [Disable the Data Path of a LUN](#)

About Data Protection Schedules

A data protection schedule defines the following parameters:

- The time units in which the data protection event occurs, such as hourly, daily, or weekly.
- The time intervals at which a replica is created, such as every hour, every 2 hours, and so on.
- If you need to perform a data protection job only one time, use the *Run Once* option when you create or modify your job schedule. After the system runs this job, the system deletes the schedule. Check the event log for the completion status of your job.

You can modify an existing data protection schedule or delete a schedule when it is no longer needed.

Create LUN Data Protection Schedules

You can create replication schedules that in turn create a clone of a protected volume (LUN or Clone LUN) at regular intervals.

- 1 From the **Protect** tab, click the **Data Protection > Protection Schedules**.
- 2 Choose **Actions > Create Schedule**.
- 3 From the Create Data Protection Schedule dialog, enter a name for the schedule in the **Schedule Name** field.

Tip: Use a meaningful name that includes the type of protection and frequency to help you identify the schedule in case you need to modify it later.
- 4 Select the data protection type, **Clone**.
- 5 (Optional) From the **Volume Group** drop-down list, choose the name of the volume group to which the clone volume will be assigned.
- 6 Select **Enabled** if you would like your schedule to start as soon as it is created.

If you do not enable your schedule now, you can do so at a later time by modifying the schedule.

- 7 Select the volumes to replicate from the list.

- 8 Click the expansion button to the right of **Start Time** to select the day and time for your schedule to start.
- 9 Use the controls in the **Modify Date/Time** dialog to select the date and time.
- 10 Click **OK** to close the scheduler dialog.
- 11 Choose a frequency for your schedule:
 - Run Once
 - Hourly
 - Daily
 - Weekly
- 12 Choose a recurrence value for your schedule.

If you chose a frequency of **Weekly**, choose the day of the week you would like your report to be generated.
- 13 To save the schedule, click **OK**.

Result:

Your schedule is listed on the Data Protection Schedules overview page.

Related references

- [Create Data Protection Schedule Dialog](#)
- [Data Protection Overview Page](#)
- [Pillar Axiom System Limits](#)

Related tasks

- [Modify a LUN Data Protection Schedule](#)

Modify a LUN Data Protection Schedule

You might want to modify certain characteristics of a data protection schedule, such as its frequency to reduce the number of clones.

- 1 From the **Protect** tab, click **Data Protection > Protection Schedules**.
- 2 Select a data protection schedule that you want to modify from the available list.
- 3 Choose **Actions > Modify Schedule**.
- 4 (Optional) From the Modify Data Protection Schedule dialog, enter a new name for the notification in the **Schedule Name** field.

- 5 (Optional) From the **Volume Group** drop-down list, choose the name of the volume group to which the clone volume will be assigned.
- 6 (Optional) Set the **Enabled** check-box as necessary to enable or disable the data protection schedule.

You can disable the data protection schedule to stop replication operations temporarily.
- 7 (Optional) Click the expansion button to the right of **Start Time** to select a revised day and time for your schedule to start.

To close the Start Time dialog, click **OK**.
- 8 (Optional) Choose a new time basis for your schedule, as necessary.
- 9 (Optional) Choose a **Recurrence** value for your schedule, as necessary.
- 10 To save your changes, click **OK**.

Related references

- [Scheduled Jobs Overview Page](#)
- [Protection Schedules Overview Page](#)
- [Modify Data Protection Schedule Dialog \(Protect tab\)](#)
- [Modify Scheduled Job Dialog](#)

Related tasks

- [Create LUN Data Protection Schedules](#)

Delete a LUN Data Protection Schedule

You can delete a data protection schedule when your data replication requirements change. After deleting the schedule no automatic data protection will occur.

- 1 From the **Protect** tab, click **Data Protection > Protection Schedules**.
- 2 Select the data protection schedule that you want to delete from the available list.
- 3 Click **Actions > Delete Schedule**.
- 4 When prompted to confirm the deletion, click **OK**.

Related references

- [Scheduled Jobs Overview Page](#)
- [Protection Schedules Overview Page](#)
- [Modify Data Protection Schedule Dialog \(Protect tab\)](#)
- [Modify Scheduled Job Dialog](#)

Related tasks

- [Create LUN Data Protection Schedules](#)

View a LUN Data Protection Schedule

You can display the details of a LUN data protection schedule. For example, you can view the name of the logical volume associated with the schedule or review the schedule details.

- 1 From the **Protect** tab, click **Data Protection > Protection Schedules**.
- 2 Select a data protection schedule from the available list.
- 3 Choose **Actions > View Schedule**.
- 4 Review the displayed information to ensure that the data protection schedule details are what you expect.
- 5 Click **Close** when finished reviewing the schedule.

Related references

- [Scheduled Jobs Overview Page](#)
- [Protection Schedules Overview Page](#)
- [View Data Protection Schedule Dialog](#)
- [View Scheduled Job Dialog](#)

Related tasks

- [Modify a LUN Data Protection Schedule](#)
- [Create LUN Data Protection Schedules](#)

Manage a Replication Engine

You can manage any Replication Engine that is registered with the Pillar Axiom system.

Managing the Replication Engine opens a web browser that provides administrative access to the device.

- 1 From the **Protect** tab, click **Replication Engines**.
- 2 Select a Replication Engine that you want to manage from the available list.
- 3 Choose **Actions > Manage**.

Result:

A web browser opens with the Pillar Axiom MaxRep login page for the Replication Engine displayed. Refer to the *Pillar Axiom MaxRep for SAN User's Guide*.

Related references

- [Replication Engines Overview Page](#)

About the Pillar Axiom VSS Provider Plug-In

The Microsoft Volume Shadow Copy Service (VSS) Provider plug-in enables the use of VSS-enabled backup applications with the Pillar Axiom 600 system.

VSS enables data protection and management services through a standard set of configuration and monitoring capabilities. These capabilities include creating, manipulating, and restoring snapshots without shutting down applications or essential services.

For more information about VSS, refer to the following documentation:

- The [Volume Shadow Copy Service Technical Reference](http://technet.microsoft.com/en-us/library/cc738819(WS.10).aspx) ([http://technet.microsoft.com/en-us/library/cc738819\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc738819(WS.10).aspx)) provided by Microsoft.
- The Microsoft Developers Network (MSDN) article [The VSS Model \(Windows\)](http://msdn.microsoft.com/en-us/library/aa384625.aspx) (<http://msdn.microsoft.com/en-us/library/aa384625.aspx>).

The Pillar Axiom VSS Provider is a VSS hardware provider that allows VSS-enabled applications to make volume shadow copies of data on Pillar Axiom systems without interrupting normal operations. The Pillar Axiom technology partners FalconStor and InMage offer data replication solutions featuring VSS implementations that do not require the VSS Provider plug-in.

Refer to your VSS-enabled backup application documentation for instructions on configuring and using VSS with your backup application.

Download and Install the VSS Provider Plug-In

Download the Pillar Axiom VSS Provider plug-in from the Pillar Axiom Storage Services Manager for installation on your SAN host.

Prerequisites:

- The SAN host must have TCP/IP connectivity, over Ethernet, to the Pilot management controller.
- For the VSS Provider to create volume shadow copies, the SAN host must have Fibre Channel connectivity to the Slammer storage controller.
- During the installation, you need the system serial number, user name, and password.

- 1 From the **Support** tab, click **Utilities**.
- 2 In the Utilities content pane, click **Pillar Axiom VSS Provider** link for your operating system type.
- 3 Save the file to a client workstation.
- 4 Double-click the file to begin the installation.
- 5 Follow the instructions to install the VSS Provider plug-in on your SAN host.
- 6 Click Close at the Installation Complete page to close the VSS Provider Installer wizard.
- 7 Verify installation by running the following command at a command prompt:

```
vssadmin List Providers
```

Result:

This command should return the name of the Pillar VSS Provider, as follows:

```
Provider name: 'PDS VSS HW Provider'
```

If it does, installation was successful and your SAN host can use the VSS Provider to create shadow copies.

The VSS Provider installer allows you to configure a single Pillar Axiom system. To configure additional systems or remove systems, use the `registerAxiom.exe` command line tool:

- To configure additional systems, run this command at a command prompt:

```
registerAxiom.exe serial_number user_name password
```

- To remove a configured system, run this command:

```
registerAxiom.exe serial_number
```

- Running `registerAxiom.exe` without parameters prints the usage instructions.

Related concepts

- [About the Pillar Axiom VSS Provider Plug-In](#)

Related references

- [Utilities Overview Page](#)
- [Volume Shadow Copy Service \(VSS\) Page](#)

CHAPTER 8

Manage Software Components

Display Software Versions

You can display the versions of all software modules in your Pillar Axiom system.

The version information includes:

- Drive and Enclosure Services (ES) firmware in the Brick storage enclosures.
- Application software and operating system in the Pilot management controller.
- Software (SAN) and programmable ROM (PROM) in Slammer storage controllers.

- 1 From the **Support** tab, click **Software Modules**.
- 2 Review the displayed information to ensure that the versions are what you expect.

Related references

- [Software Modules Page](#)

About Updating the Pillar Axiom Software

An update operation installs a new version of software or firmware onto a Pillar Axiom system. An update affects one or more of the following components.

- Brick storage enclosures:
 - Drive firmware
 - Enclosure Services (ES) firmware
- Pilot management controller:
 - Software
 - Operating system
- Slammer storage controllers:
 - Software for storage area network (SAN) configurations
 - Programmable ROM (PROM)

Note: Updating a Brick requires a system restart.

Note: Updating the PROM requires a system restart.

Download Firmware and Software Updates

You can download from the Customer Support portal the latest software and firmware updates.

Prerequisites:

- Contact the Oracle Pillar Customer Support to request the firmware or software update.
- Be sure you are registered on the Customer Support portal.
- Have available the serial number for the Pillar Axiom system for which you want the software update.

- 1 Using your registered username and password, log in to the Customer Support portal.

Choose one of the following:

- Click this link: [Customer Support portal](#).

- Add this URL to the address field in your browser: <http://support-portal.pillardata.com/csportal/login.seam>.

- 2 In the menu bar, select **My Downloads > My Software Releases**.
- 3 If you have more than one Pillar Axiom system, click the **System** drop-down list and select the serial number of the system for which you want the software update.
- 4 Under Folders for All Software, navigate to the software type you want and click the release you want to download.

If the software release is not displayed for your system, contact the Oracle Pillar Customer Support.

- 5 In the **Available Software** content pane, click the title of the software package that you want to download.
- 6 In the **Software Download Information** content pane, review the details of the download package to verify your selection.

Note: Check the file size of the download and be sure your workstation has sufficient space.

- 7 To download the software package, click the **Download** link.

The system displays a dialog box to inform you that the software package is being read. This operation can take a few minutes, depending on the size of the package.

Tip: If your browser window displays an information bar that states that the download is blocked, click the appropriate options to allow the download to proceed.

- 8 To begin the download, click **Save**.

Browse to the location on your workstation where you want to save the software update package.

- 9 To save the software package on your workstation, click **Save**.

After you successfully download the software update package, in the original dialog box, click the **Close When Finished** link.

Upload (stage) the software or firmware package to the Pillar Axiom system.

Related concepts

- [About Updating the Pillar Axiom Software](#)

Related tasks

- [Update the Pillar Axiom Software](#)
- [Upload the Drive Firmware Package](#)

Upload the Software Package

After downloading a software update package, you can stage it on the Pilot management controller to prepare the system for the software update. You can perform the update immediately or schedule the update for a later time.

Prerequisites:

- We recommend that you use a faster internal network connection (10 Mb/s, or greater) to upload a software update package from a client to your Pillar Axiom system. You should avoid using a slow connection, such as a wide area network (WAN) connection.
- Have the software download package available on a reachable host machine (preferably on your local host).

- 1 From the **Support** tab, click **Software Modules**.
- 2 From the Software Modules page, click **Upload Software Package**.
- 3 In the **Upload Software Package** dialog, navigate to the software package you downloaded, highlight it, and click **Open**.

Result:

The software package is placed onto the Pilot management controller. When the upload is complete, the update package displays in the **Staged Software** panel.

- 4 From the Software Modules page, click **OK**.

Related references

- [Software Modules Page](#)
- [Update Software, Details Tab](#)

Confirm the Upgrade Paths

You can review the software packages from which you can upgrade the Pillar Axiom system.

- 1 From the **Support** tab, click **Software Modules**.
- 2 Choose **Actions > View Upgrade Paths to Staged Package**.
- 3 Review the upgrade path information provided on the screen.

Note: If the list shows more than one upgrade version, install the earliest software version first, followed by the subsequent versions.

Related references

- [Upgrade Paths to Staged Package Dialog](#)
- [Upgrade Paths from Installed Package Dialog](#)

Related tasks

- [Download Firmware and Software Updates](#)
- [Upload the Software Package](#)
- [Update the Pillar Axiom Software](#)

Update the Pillar Axiom Software

After uploading a software package for staging on the Pilot management controller you can update the system software. You can perform the update immediately or schedule the update for a later time.

Note: Pillar recommends that you perform the update operation as the Primary administrator and in an Administrator 1 role.

Important! When logged into the system as a support administrator you can select individual components to upgrade or downgrade from the software module package. Such action is not recommended and may affect system performance. Contact the Oracle Pillar Customer Support before installing individual software components.

- 1 From the **Support** tab, click **Software Modules**.
- 2 From the Software Modules page, choose **Actions > Update Software**.
- 3 (Optional --*support role only*) If you are logged in as a support administrator select the individual software module you wish to update.

Valid options are:

- Do not install
- Install if newer version
- Force Install

Important! Updating individual software modules is **NOT** recommended and should only be performed under the direction of Oracle Pillar Customer Support.

- 4 Select the option **Update software without restarting system**.
- 5 (Optional) Select any of the other options available on the Details page.
Note: Some options will cause data access disruptions. Be sure to read each option carefully.
- 6 (Optional) To schedule your software update for a later time, select the **Schedule** tab and enter the time on which the system should perform the operation. You can schedule updates to occur within 72 hours.
- 7 From the Software Modules page, click **OK**.
- 8 To confirm the software update, click **OK**.

Related references

- [Software Modules Page](#)
- [Update Software, Details Tab](#)

Related tasks

- [Upload the Software Package](#)
- [Schedule the Software Update](#)

Schedule the Software Update

You can schedule software updates to occur at a specified time. For example, you can schedule an update to occur during off-peak hours.

You can schedule updates to occur within 72 hours.

- 1 From the **Support** tab, click **Software Modules**.
- 2 From the Software Modules page, choose **Actions > Update Software**.
- 3 From the Schedule tab, click the **Schedule software update to occur at a later time** option.
- 4 Select the expansion button to the right of **Time to Perform Software Update** to select day and time that you want the software update to start.
Note: The system limits your date selection to the next 72 hours.
- 5 To set the time, click **OK**.
- 6 To update the software at your prescribed schedule, click **OK**.

Result:

After clicking OK, the Software Modules overview page displays the scheduled software update.

Related references

- [Update Software, Schedule Tab](#)

Related tasks

- [Update the Pillar Axiom Software](#)
- [Cancel a Scheduled Software Update](#)

Cancel a Scheduled Software Update

You can delete a scheduled software update. Cancelling a scheduled software update may be necessary to reschedule the update for a later time.

- 1 From the **Support** tab, click **Software Modules**.

Result:

If a scheduled software update is active, a notice appears on the page.

- 2 Click **Cancel Scheduled Update**.
- 3 Confirm that you want to cancel the update and click **OK**.

Result:

The system deletes the scheduled task and removes the software update notice from the Software Modules page.

Related references

- [Scheduled Jobs Overview Page](#)

Related tasks

- [Schedule the Software Update](#)

About the Drive Firmware Update

The drive firmware contains programming updates that improve the performance and reliability of the drive. Updating the drive firmware ensures that the device runs at optimum levels in the Pillar Axiom system.

The Oracle Pillar Customer Support might request that you update the drive firmware in the Pillar Axiom system. You update the firmware in three phases:

- Download the firmware package from the Oracle Pillar Customer Support.
- Upload the firmware package to the Pillar Axiom system.
- Update the drive firmware.

Uploading (staging) the firmware package overwrites any existing version on the Pillar Axiom system. Each package contains the firmware updates for the drive manufacturers and types in your system. If you have multiple firmware packages, install each one separately.

Updating the drive firmware disrupts data access to the Pillar Axiom system. Perform the update during a time that does not impact access to the system. When you initiate the update, the system updates the firmware on all of the recognized drives, and then the system restarts the Slammers. During startup, the system updates any new drives that contain outdated firmware versions.

Related tasks

- [Upload the Drive Firmware Package](#)
- [Update the Drive Firmware](#)
- [Download Firmware and Software Updates](#)

Upload the Drive Firmware Package

Upload (stage) the drive firmware package to make the firmware available so that the drives can be updated right away or at a later time.

Prerequisite:

Before performing the drive firmware upload, ensure that the Pillar Axiom system state is *Normal*. If your system requires attention, contact the Oracle Pillar Customer Support.

Ensure that the firmware package file that you downloaded from the Customer Support portal is available for upload to the Pillar Axiom system.

- 1 From the **Support** tab, click **Tools > Drive Firmware**.

- 2 Choose **Action > Upload Drive Firmware Package**.
- 3 From the Upload Drive Firmware Package dialog, click the browse button [...], select the firmware package file, and then click **Open**.
- 4 To upload the package to the system, click **OK**.

Result:

When the upload is complete, the system displays the staged firmware package version number and provides a list of drives whose firmware is eligible for update.

After staging the firmware package, update the firmware to the eligible drives in the Pillar Axiom system.

Related concepts

- [About the Drive Firmware Update](#)

Related references

- [Drive Firmware Overview Page](#)

Related tasks

- [Update the Drive Firmware](#)
- [Remove the Drive Firmware Package](#)
- [Download Firmware and Software Updates](#)

Update the Drive Firmware

Update the drive firmware so that the drive performs at an optimum level as specified by the manufacturer.

- 1 From the **Support** tab, click **Tools > Drive Firmware**.

Result:

The Drive Firmware overview page provides the staged firmware version number and a list of drives that contain outdated firmware.

- 2 Confirm that the correct firmware version is staged on the Pillar Axiom system.
- 3 Choose **Action > Update Drive Firmware**.
- 4 Read the information provided in the confirmation dialog and select the option, **Disrupt data access**.
- 5 When you are ready to update the drive firmware and disrupt data access to the system, click **OK**.

The system updates the firmware of the drives that match the criteria specified in the firmware package. When the update completes, the Pillar Axiom system restarts. During restart, the system updates any drives that contain outdated firmware.

If the update fails, the Pillar Axiom system records a system alert. To resolve the issue, you can try the update process again or replace the affected drive. If the problem continues, contact Oracle Pillar Customer Support.

Related concepts

- [About the Drive Firmware Update](#)

Related references

- [Drive Firmware Overview Page](#)

Related tasks

- [Upload the Drive Firmware Package](#)
- [Remove the Drive Firmware Package](#)

Remove the Drive Firmware Package

Remove the uploaded firmware package when it is no longer needed to update the drive firmware. Removing the firmware package does not delete the firmware version from the drives, but prevents the administrator from using this package to update the drive firmware in the Pillar Axiom system.

- 1 From the **Support** tab, click **Tools > Drive Firmware**.
- 2 From the Pending Drive Firmware Updates table, verify that the installed drive firmware version is the package to remove.
- 3 Choose **Action > Remove Drive Firmware Package**.
- 4 From the confirmation dialog, click **OK**.

Related concepts

- [About the Drive Firmware Update](#)

Related references

- [Drive Firmware Overview Page](#)

CHAPTER 9

Manage Hardware Components

Display Hardware Component Status

At any time, you can review the status of the Pillar Axiom hardware components and their field replaceable units (FRUs).

- 1 From the **Monitor** tab, click **Hardware**.
- 2 Click the component type for which you want to display the statuses of the individual FRUs.

Available component types:

- Pilot
- Slammers
- Bricks
- UPS

Result:

The corresponding hardware overview page displays some basic information about the components and the status of their FRUs.

Related references

- [Hardware Overview Page](#)
- [Pilot Overview Page](#)
- [Slammers Overview Page](#)
- [Bricks Overview Page](#)
- [Uninterruptible Power Supplies Overview Page](#)

Display Additional Details for the FRUs

At any time, you can review the full details of the field replaceable units (FRUs) contained within a Brick or Slammer.

- 1 From the **Monitor** tab, click **Hardware**.
- 2 Click the component type for which you want to view FRU details.

Available component types with FRUs:

- **Slammers**
- **Bricks**

- 3 Select the specific hardware component for which you want to view FRU details.
- 4 For that component, choose **Actions > View Details**.
- 5 In the View dialog, click the **Components** and **I/O Ports** tabs to review the details of the hardware FRUs.

Result:

Different details appear depending on the component type and specific FRU that you selected.

Related references

- [Hardware Overview Page](#)
- [View Brick, Components Tab](#)
- [View Brick, I/O Ports Tab](#)
- [View Slammer, Components Tab](#)
- [View Slammer, I/O Ports Tab](#)

Modify a Hardware Component Name

You may want to change the names of Slammers and Bricks that are displayed in the Pillar Axiom Storage Services Manager.

- 1 From the **Monitor** tab, click **Hardware**.
- 2 Click the component type of the hardware for which you want to modify the name.

Available component types:

- **Slammers**
- **Bricks**

- 3 Select the specific hardware component that you want to rename.
- 4 Choose **Actions > Modify Name**.
- 5 In the Modify dialog, enter a new name for the component.
- 6 Click **OK**.

About Hardware Replacement

Your Support Services contract provides guidelines to replace a hardware field replaceable unit (FRU) in your Pillar Axiom system. Based on the terms of your contract, you can:

- Replace the FRU yourself.
- Place a service request so that a Service Technician comes to your site to replace the FRU.

Important! Replacement of most FRUs requires Guided Maintenance to perform the following actions:

- Prepare the system for the FRU replacement.
- Integrate the new FRU into the system.

Consult the *Pillar Axiom Service Guide* for details.

We recommend that you check the power supplies annually for accumulated dust. If needed, vacuum the power supplies, even if no component replacement or repair is required. This type of maintenance does not require Guided Maintenance.

Identify the Hardware Component

Sometimes you might want to locate a specific Slammer or Brick in the Pillar Axiom system. For example, when replacing a field replaceable unit in a particular Slammer, it would be useful to be able to identify the target Slammer.

The Guided Maintenance feature identifies hardware components by blinking the light-emitting diodes (LEDs) on the front and back of the Slammers and Bricks. To locate a particular Slammer or Brick, you can request that the system blink the LEDs on the target hardware or blink the LEDs on all hardware *except* for the target.

Note: For more information on identifying hardware components, refer to the *Pillar Axiom Service Guide*.

- 1 From the **Monitor** tab, click **Hardware**.
- 2 Click the link in the left navigation pane for the type of component to identify.

Available component types that can be identified:

- Slammers
- Bricks

- 3 In the content pane, select the specific component that you want to identify.
- 4 Choose **Actions > Identify**.
- 5 In the Identify dialog, follow the instructions to identify the hardware component.

Options:

Identify Blinks the LEDs on the front and back of the target Slammer or Brick.

Reverse Identify Blinks the LEDs on all Slammers and Bricks *except* those on the target component.

- 6 Click **Finish**.

Related references

- [Hardware Overview Page](#)

Related tasks

- [Display Hardware Component Status](#)
- [Display Additional Details for the FRUs](#)

Replace a FRU

To maintain or restore reliability to a Pillar Axiom system, you sometimes need to replace a field replaceable unit (FRU).

Pillar Data Systems supports only Pillar-supplied parts on a Pillar Axiom system.



Caution

Hardware that does not conform to Pillar Axiom specifications or is not a Pillar-supplied part voids the warranty and may compromise data integrity. For Pillar Axiom hardware specifications, refer to the *Pillar Axiom 600 Service Guide* for your system.

- 1 From the **Monitor** tab, click **Hardware**.
- 2 Click the link in the left navigation pane for the chassis type that contains the FRU to be replaced.

Available chassis types:

- Slammers
- Bricks

- 3 In the content pane, click the Slammer or Brick that contains the FRU you want to replace.
- 4 Choose **Actions > View Details**.
- 5 On the Components tab in the View dialog, select the FRU that you want to replace and click **Replace Component**.

Note: Although the chassis is listed as a replaceable unit, Pillar does not currently support chassis replacement.

- 6 Follow the instructions provided by the Guided Maintenance wizard to repair the hardware component.

Refer as well to the appropriate *Pillar Axiom Service Guide* for detailed instructions.

- 7 When you have completed the FRU replacement, click **Finish**.

Related references

- [Hardware Overview Page](#)

Related tasks

- [Display Hardware Component Status](#)
- [Display Additional Details for the FRUs](#)
- [Identify the Hardware Component](#)

About Brick Drive Insertion

Drive insertion is a part of the overall drive replacement procedure performed using Guided Maintenance. The replacement drive can be from a spares kit or from another Brick storage enclosure.

Important! Pillar Axiom storage systems accept only Pillar-supplied drives.

All Pillar-supplied drives are specially branded to indicate that they have been manufactured by Pillar. Drives that currently reside in or once upon a time resided in a Brick enclosure have been branded by the Pillar Axiom system with a unique identifier called a *system serial number (SSN)*. Drives that have never been accepted into a Brick, such as those from a spares kit, are branded at the factory with a string of 9s.

A drive that has already been branded with an SSN and is re-inserted into a Brick enclosure is known as a *foreign drive*. Foreign drives require your intervention for them to be accepted into a Pillar Axiom Brick enclosure.

Important! The capacity of a replacement drive must be equal to or greater than that of the other drives in the Brick enclosure.

Using Guided Maintenance, after you have inserted a replacement drive into a Brick enclosure, continue using Guided Maintenance to complete the replacement procedure.

If the replacement drive came from a spares kit, the drive acceptance task should begin automatically within a few minutes. If, however, the replacement drive came from a Brick enclosure, Guided Maintenance displays a system alert that prompts you to confirm the acceptance of the foreign drive.

Acceptance The system binds the drive to the Brick and destroys any data that might have existed on the drive.

Rejection The system terminates the drive insertion procedure and does not integrate the drive into the RAID array. Any previous data on the foreign drive remains intact. The system alert remains in the list of alerts. If the alert is then deleted and the drive is removed, the drive can be inserted again at another time. In this case, the drive will be seen as a Foreign Drive.

When Guided Maintenance successfully validates the drive replacement, the drive is bound to the Brick into which it was added. Any and all data that existed on the drive will have been erased.

When the drive replacement process is complete, the Pillar Axiom system reports the status of the drive.

Related tasks

- [Accept a Foreign Drive](#)

Accept a Foreign Drive

Accepting a foreign drive into a Brick storage enclosure binds that drive to that Brick and adds the appropriate capacity of the drive to the total capacity of the RAID array in which the drive participates.

Prerequisites:

- The inserted drive came from one of the following sources:
 - A Pillar-supplied spares kit
 - A Pillar Axiom Brick
- The capacity of the inserted drive is equal to or greater than that of the other drives in the Brick enclosure.

- The drive has been inserted into the Brick enclosure by following the instructions in the *Pillar Axiom Service Guide*.

A system alert is displayed when a drive that is not factory-fresh from Pillar is inserted into the Brick. In such a case, if you want to bind this drive to this Brick, you must accept the drive.

- 1 (Optional) To accept the foreign drive, select **Accept Foreign Drive** and click **OK**.



Result:

The system clears the alert and starts a copyback task in the background. Other tasks might run as well, depending on whether Guided Maintenance was used to control the drive replacement steps. Similarly, the status of the replacement drive and spare drive might vary depending on whether Guided Maintenance was used.

The system binds the drive to the Brick and destroys any data that might have existed on the drive.

When the copyback process completes, confirm that the status of the replacement drive is Normal.

- 2 (Optional) To reject the foreign drive, click **Cancel**.

Result:

The system terminates the drive insertion procedure and does not integrate the drive into the RAID array. Any previous data on the foreign drive remains intact. The system alert remains in the list of alerts. If the alert is then deleted and the drive is removed, the drive can be inserted again at another time. In this case, the drive will be seen as a Foreign Drive.

Related concepts

- [*About Responding to System Alerts*](#)
- [*About Brick Drive Insertion*](#)

About Managing Bricks

The storage pool available to a Pillar Axiom system can be expanded to accommodate increased storage demands by adding additional Bricks to the system. Similarly, you can balance the storage requirements across several Storage Domains by reassigning a Brick to a different domain.

About Adding Bricks to a Storage Domain

The impact of adding a Brick to a Pillar Axiom system depends on whether administrator defined Storage Domains exist.

Table 20 Effect of Storage Domains on Brick additions

Do administrator defined Storage Domains exist?	Impact
No	<p>The system checks the system serial number (SSN) of the Brick to verify whether the SSN is applicable to this Pillar Axiom system. How the system responds to this check depends on the applicability of the SSN:</p> <ul style="list-style-type: none"> • Applicable. The Brick is a new one from the factory. The system automatically adds the new Brick to the default Storage Domain. • Not applicable. The Brick is from some other Pillar Axiom system. The system prompts you to accept the <i>foreign</i> Brick.
Yes	<p>The system prompts you to perform one of the following actions:</p> <ul style="list-style-type: none"> • Add the Brick to one of the listed Storage Domains. • Create a new Storage Domain with this Brick as the initial member. <p>Note: Under certain circumstances, the system might automatically add this Brick to the primary domain, which can happen if the system has been unable to migrate the system data into the primary Storage Domain.</p> <p>Based on the current Quality of Service (QoS) settings of the various logical volumes and their associated clone repositories,</p>

Table 20 Effect of Storage Domains on Brick additions (continued)

Do administrator defined Storage Domains exist?	Impact
	the system might notify you of any recommended data migrations.

For best performance, you should add Bricks to Storage Domains in quantities that are sufficient to support the default number of RAID groups for each Storage Class and QoS.

For information about how to add Bricks to a system, refer to the *Pillar Axiom Hardware Installation Guide* for your system.

Related concepts

- [About Storage Domains](#)
- [About Reassigning Bricks](#)
- [About Licensing Optional Premium Features](#)

Related tasks

- [Accept a Brick](#)

Accept a Brick

When you add a Brick storage enclosure to an existing Pillar Axiom system, your acceptance of the Brick allows the system to add the storage provided by the Brick to the existing storage pool.

Prerequisites:

- The Pillar Axiom system is in a Normal state.
- The Brick has been cabled correctly according to the wiring diagrams in the *Pillar Axiom 600 SSF Cabling Reference*.
- Both RAID controllers of the Brick have been powered on.
Note: After you power on a Brick, the system updates the Brick firmware. This update can take up to 15 minutes.
- A system alert exists that states that a Brick has been added to the system.

Typically, you respond to the system alert by either accepting or rejecting the newly added Brick. If you delete the system alert and, as a consequence, do not

accept the Brick, you can perform the **Accept Brick** action at a later time. This action mirrors the functionality of the Accept Brick alert.

The Brick to be accepted can be a new one from Pillar Manufacturing or an existing one from a different Pillar Axiom system. A Brick from a different system is referred to as a *foreign* Brick.

- 1 From the **Monitor** tab, click **Hardware > Bricks**.
- 2 Choose **Actions > Accept Brick**.
- 3 (Optional) Select a domain from **Storage Domain** drop-down list.
This list is active only when additional Storage Domains exist.
- 4 (Optional) Replace the default logical name for this newly added Brick with a name of your own choosing.
- 5 To accept the Brick into the system, click **OK**.

Result:

While the Brick is being integrated into the system, the status of the Brick changes from red to yellow to green. Also, the overall status of a foreign Brick is displayed as Foreign.

When the system completes the integration process, the system performs the following additional actions:

- Generates a “Brick Accepted” event.
- Changes the health status of the Brick from Warning to Normal.
- Removes all system alerts that are related to the Brick addition.

Note: If any system alerts remain, contact the Oracle Pillar Customer Support.

The Brick is now fully integrated into the Pillar Axiom system.

You can now begin utilizing the additional capacity provided by the newly added Brick. The **Monitor > Hardware > Bricks** overview screen shows this capacity and the Storage Domain to which the Brick is assigned.

Related concepts

- [About Reassigning Bricks](#)
- [About Adding Bricks to a Storage Domain](#)

Related references

- [Accept Brick Dialog](#)

Related tasks

- [Reassign a Brick to Another Storage Domain](#)

About Reassigning Bricks

Sometimes you might need to reassign a Brick to another Storage Domain.

Important! If the Brick contains any logical volumes or a portion of one or more volumes, you must first move those volumes to other Bricks before reassigning the Brick.

Note: For a given Storage Domain, only one Brick can be reassigned at a time. Wait for the current background task to complete before reassigning additional Bricks.

Related tasks

- [Create a Storage Domain](#)
- [Modify a LUN: Define Quality of Service](#)

Reassign a Brick to Another Storage Domain

Reassign a Brick to another Storage Domain when you want to provide initial storage capacity to a newly created domain or to provide additional capacity to an existing domain.

If one or more logical volumes exist on the Brick to be reassigned, the Storage Domain to which the Brick is currently assigned must have sufficient free capacity to hold those volumes after the Brick is reassigned.

Note: Assigning logical volumes and Bricks to a Pillar Axiom Storage Domain must be performed as separate actions.

Important! Reassigning a Brick to another Storage Domain can cause data migration. Such migration occurs when data associated with one or more logical volumes resides on that Brick.

- 1 From the **Configure** tab, click **Groups > Storage Domains**.
- 2 Choose **Actions > Manage Storage Domains**.
- 3 On the **Bricks** tab, click the name of the Brick you want to reassign.
Result:
A drop-down list appears in the Storage Domain field.
- 4 In the Storage Domain field, click the drop-down list and choose the Storage Domain to which you want to reassign the Brick.

- 5 Click **OK**.

After the background task that reassigns the Brick completes, you can reassign another Brick.

Related concepts

- [About Storage Domains](#)
- [About Reassigning Bricks](#)
- [About Adding Bricks to a Storage Domain](#)
- [About Licensing Optional Premium Features](#)

Remove a Brick

Remove a Brick after you have migrated all of its data and system configuration to a new storage location.

Before you can remove a Brick, all user and system resources must be migrated off that Brick. There are a variety of options for doing this, depending on the specific configuration and the reasons for removing the Brick. For technical assistance, contact the Oracle Pillar Customer Support. For obtaining new storage, contact your account representative.

Important! Before you attempt to remove any Bricks, contact the Oracle Pillar Customer Support for assistance with identifying and moving your data.

Prerequisites:

- The Pillar Axiom system is in a Normal state.
- No logical volume has any part of its allocation residing on this Brick.
- No system configuration information resides on this Brick.
- Identify the physical location of the Brick in the system.

- 1 From the **Monitor** tab, click **Hardware > Bricks**.
- 2 From the Bricks overview page, select a Brick to remove.
- 3 Choose **Actions > Remove Brick**.
- 4 From the confirmation dialog, click **OK**.

Result:

The system removes the Brick from the system configuration and records a system event. Consult customer support for information about physically removing the Brick from the system.

If data is associated with the Brick the system displays an error message. Resolve the error and try again.

You can safely remove the physical Brick after meeting the following conditions:

- The system no longer displays an error message when trying to remove the Brick.
- The Bricks overview page no longer displays the Brick.

Related concepts

- [*About Managing Bricks*](#)

Related tasks

- [*Identify the Hardware Component*](#)
- [*Reassign a Brick to Another Storage Domain*](#)

About the UPS Device

The uninterruptible power supply (UPS) device provides backup power to the Pillar Axiom system in the event of a power failure. The system monitors the UPS activities and reports the health of the device.

The system uses Simple Network Management Protocol (SNMP) traps to obtain information about the UPS device. Up to four devices can be monitored by the system. The information gathered from the UPS includes:

- Communication status
- Power source
- Battery status

In the event of a power failure, the UPS device switches from AC (alternating current) to battery power and the Pillar Axiom system switches to a conservative operating state. In the conservative state, the Slammer switches to write-through mode, which causes the Slammer to write data immediately to disk.

Related references

- [Uninterruptible Power Supplies Overview Page](#)
- [Create SNMP Host Dialog](#)

Related tasks

- [Create a UPS Device](#)
- [Modify a UPS Device](#)

Create a UPS Device

You can create a connection to an uninterruptible power supply (UPS) device connected to the Pillar Axiom system. Up to four UPS devices can be configured to the system.

- 1 From the **Monitor** tab, click **Hardware > UPS**.
- 2 Choose **Actions > Create UPS**.
- 3 From the Create UPS dialog, enter the **Name** for the UPS device.
- 4 Enter the **IP Address** of the UPS device.
- 5 Enter the **SNMP Community** name.
- 6 To save your changes, click **OK**.

Related concepts

- [About the UPS Device](#)

Related references

- [Create UPS Dialog](#)
- [Uninterruptible Power Supplies Overview Page](#)
- [SNMP Hosts Overview Page](#)

View a UPS Device

You can review the properties and connection status of an uninterruptible power supply (UPS) device connected to the Pillar Axiom system.

- 1 From the **Monitor** tab, click **Hardware > UPS**.
- 2 From the Uninterruptible Power Supply overview page, select a UPS device from the list.
- 3 Choose **Actions > View UPS**.
- 4 Review the properties of the UPS device to ensure that the information is what you expect.

Related references

- [Modify UPS Dialog](#)
- [Uninterruptible Power Supplies Overview Page](#)
- [SNMP Hosts Overview Page](#)

Modify a UPS Device

You can modify the properties of an uninterruptible power supply (UPS) device. For example, you can update the name of the UPS device or change the name of the community string used to receive traps that monitor the device activities.

- 1 From the **Monitor** tab, click **Hardware > UPS**.
- 2 From the Uninterruptible Power Supply overview page, select a UPS device from the list.
- 3 Choose **Actions > Modify UPS**.
- 4 From the Modify UPS dialog, update the properties for the UPS connection.
- 5 To save your changes, click **OK**.

Related references

- [View UPS Dialog](#)
- [Uninterruptible Power Supplies Overview Page](#)
- [SNMP Hosts Overview Page](#)

Delete a UPS Device

You can remove an uninterruptible power supply (UPS) device from the Pillar Axiom system. After you delete the UPS device you will no longer be able to monitor the device activities.

- 1 From the **Monitor** tab, click **Hardware > UPS**.
- 2 From the Uninterruptible Power Supply overview page, select a UPS device from the list.
- 3 Choose **Actions > Delete UPS**.
- 4 From the confirmation dialog, click **OK**.

Related references

- [Uninterruptible Power Supplies Overview Page](#)

CHAPTER 10

Manage Event Logs, Notifications, Alerts, and Jobs

About Event Logs

Event logs display the system events of a Pillar Axiom system. Events include management actions such as the creation or deletion of LUNs and any problems encountered by the Pillar Axiom system, such as hardware issues or other problems detected in the Slammer or the Pillar Axiom management software. You can set filters for severity and category types.

When you encounter an issue that you cannot resolve, you can bundle a collection of the logs and send the bundle to your Call-Home server. From there, the Oracle Pillar Customer Support can analyze the logs to help you resolve the issue.

Event severities:

Informational	Requires no action for events that are information only.
Warning	Requires no immediate action for minor conditions that you can address at your convenience.
Critical	Requires prompt action to prevent system failures or offline conditions.

Event categories:

Security	Events to notify of a security problem such as unauthorized request.
Audit	Events that keep track of what users are doing, such as the operations that they performed.
System	Events to notify of system problems, such as a missing Brick or Slammer.

Display the Event Log

Review the event log to monitor events that have occurred in the Pillar Axiom system. If too many events display on the screen, you can apply filters to the list.

- 1 From the **Monitor** tab, click **Event Log**.
- 2 Review the event log details to ensure that the information is what you expect.
- 3 (Optional) Select the **Events per page** drop-down list to select the number of events to display on each page.
- 4 (Optional) Click the page number on the upper right side of the page to navigate quickly to a desired page.
- 5 (Optional) Choose **Actions > Set Event Log Filter** to specify items to display in the list.
- 6 (Optional) Click the **Refresh** icon (the round green arrow) on the upper right side of the page to update the current data.

Related references

- [Event Log Overview Page](#)

Related tasks

- [Create an Event Notification](#)
- [Filter Event Log Entries](#)

Delete an Event Log

You can remove all of the entries in an event log. If the number of events becomes too large, you can remove all of the events in one operation.

Note: This task requires Support login privileges.

- 1 From the **Monitor** tab, click **Event Log**.
- 2 Choose **Actions > Delete Event Log**.
- 3 When prompted to confirm the deletion, click **OK**.

Related references

- [Event Log Overview Page](#)

Display the Event Properties

You can review the event properties from the Pillar Axiom system and copy them to the clipboard. This allows you to capture the event details and send them to Technical Support for example.

- 1 From the **Monitor** tab, click **Event Log**.
- 2 Select an event from the list.
- 3 Choose **Actions > Event Properties**.
- 4 (Optional) To copy the event properties to the clipboard, click **Copy to Clipboard**.
- 5 When you are finished reviewing the event properties, click **Close**.

Related references

- [Event Log Overview Page](#)
- [Events Properties Dialog](#)

Filter Event Log Entries

You may not want to see all entries in the event log as you work. Filter the events to limit the type of events that appear.

- 1 From the **Monitor** tab, click **Event Log**.
- 2 Choose **Actions > Set Event Log Filter**.
- 3 Set the following filters that you want to apply. Choose from:
 - **Event Categories:** Select all that apply.
 - **Event Severities:** Select all that apply.
 - **Event Date Range:** Select the **Display Events that occur in a date range** option, and then select the **Beginning date** and **Ending date**.
- 4 (Optional) To reset the dialog to its default state, click **Reset to Defaults**.
- 5 Click **OK**.
- 6 From the Event Log overview page, click the **Refresh** icon (the round green arrow) in the upper right corner of the page.

Result:

The Event Log overview page displays the **(filtered)** label at the top of the list, indicating that the events match your filtered criteria.

Related references

- [*Set Event Log Filter Dialog*](#)
- [*Event Log Overview Page*](#)
- [*Event Notification Overview Page*](#)

About Managing Event Notifications

Create event notifications so that you are notified when specific Pillar Axiom system events occur. You may want to display the details of an event and make changes as needed. You can also test notifications to make sure that the specified email addresses are correct.

An event notification, when enabled, is defined as follows:

A Simple Mail Transfer Protocol (SMTP) email message that notifies recipients of specified system events. System events include informational, warning, or critical events such as the creation of a logical volume or the occurrence of a hardware or software problem. Event notifications are optional and supplement normal event logging and Call-Home notification. (Formerly called an *alert*).

You must designate one or more recipients to receive an event notification and define an email server to receive the notifications.

Note: This email server is also used to send Call-Home notifications to the Oracle Pillar Customer Support.

Related tasks

- [Configure Email Notification Settings](#)

Display Event Notifications

You can view a list of existing event notifications and determine if any changes are needed. Use the Event Notification overview page to create, modify, delete, or view the event notifications.

- 1 From the **Monitor** tab, click **Event Notification**.
- 2 Review the event notification details to ensure that the information is what you expect.

Related references

- [Event Notification Overview Page](#)

Related tasks

- [Create an Event Notification](#)
- [Modify an Event Notification](#)
- [View Event Notification Details](#)
- [Delete an Event Notification](#)

Event Notification Selection

Use the following aids to sort and select individual events or groups for your event notification:

Table 21 Event severity and category selection

To ...	Perform this action ...
Sort the list of events	Valid sort orders: <ul style="list-style-type: none"> • By severity, then category • By category, then severity
Open or close a group of events	Click the expand (►) or collapse (▼) symbols as needed.
Move items between the Events Not Monitored column and the Monitored Events column	Select the event you want to move and click the right and left arrows in the center column.
Select groups of events	Select an event severity or category type. For example, to monitor all Critical events, select Critical and move it to the Monitored Events column.

Related references

- [Create Event Notification Dialog](#)

Related tasks

- [Create an Event Notification](#)

Create an Event Notification

Create event notifications so that you are notified when specific events occur in the Pillar Axiom system. You can specify the types of system events that trigger alerts as well as designate the recipients who receive the notices.

If you do not set up notices, you can still monitor system events using the event log. Call-Home notifications are also independent of email notifications and will be sent to Pillar Data Systems about issues in the Pillar Axiom system.

- 1 From the **Monitor** tab, click **Event Notification**.

- 2 Choose **Actions > Create Event Notification**.
- 3 Enter a name for the event notification in the **Name** field.
- 4 Enter a description in the **Description** field.
- 5 To enable the notification, select **Enable Event Notification**.
- 6 From the Monitored Events list, select the events for which you want to trigger the notification.

Example:

To be notified of any login failures, in the event tree, navigate down to the **Informational > Audit** list. Select the **Login Failed** item and then click the right-facing arrow to move the item to the **Monitored Events** column.

- 7 To add one or more event notification recipients, click **Add**.
 - 8 Enter the email address of each notification recipient.
 - 9 (Optional) Click **Test Email** to make sure that the alert is sent to the correct email addresses and that the SMTP server is properly configured.
- Note:** Allow at least 10 minutes between email tests.
- 10 (Optional) To remove an email address from the list, select the address and click **Remove**.
 - 11 To save the new notification, click **OK**.

Related concepts

- [About Managing Event Notifications](#)

Related references

- [Create Event Notification Dialog](#)
- [Event Notification Selection](#)
- [System Event Severities](#)

Related tasks

- [Configure Email Notification Settings](#)

View Event Notification Details

You can view the details of an event notification and determine if any changes are needed.

- 1 From the **Monitor** tab, click **Event Notification**.
- 2 Select the name of the event notification you want to view.

- 3 Choose **Actions > View Event Notification**.
- 4 When you are finished, click **Close**.

Related references

- [View Event Notification Dialog](#)
- [Create Event Notification Dialog](#)
- [System Event Severities](#)

Modify an Event Notification

You can modify the properties of an event notification. For example, for a given notification, you can change the events that are monitored or the email address to which the notification is sent.

- 1 From the **Monitor** tab, click **Event Notification**.
- 2 Select the name of the event notification you want to modify.
- 3 Select **Actions > Modify Event Notification**.
- 4 Enter a new name for the notification in the **Name** field.
- 5 Enter a new description in the **Description** field.
- 6 Use the **Add** and **Remove** buttons to update the **Event Notification Recipient Email Addresses** list.
- 7 Select new event categories or severities to monitor, as necessary.
- 8 Click **OK** when you are finished.

Related references

- [Modify Event Notification Dialog](#)
- [Create Event Notification Dialog](#)

Delete an Event Notification

You can delete an existing event notification. For example, you can do this if someone leaves the company and you no longer want event notifications to be sent to an inactive email account.

- 1 From the **Monitor** tab, click **Event Notification**.
- 2 Select the name of the event notification you want to delete.

- 3 Select **Actions > Delete Event Notification**.
- 4 When prompted to confirm the deletion, click **OK**.

Related references

- [*Create Event Notification Dialog*](#)

About Responding to System Alerts

Some configuration events in a Pillar Axiom system require administrator intervention to resolve the underlying issue.

The system notifies you of a system alert by displaying an exclamation-point (!) icon at the bottom of pages in the GUI. When you click the exclamation-point icon, the GUI displays:

- Information about the event and the time that it occurred.
- A recommended action to resolve the issue.
- A status field that identifies whether the action has been performed.

To resolve the issue, perform the recommended action.

Manage System Alerts

You can view the details of a system alert generated by the Pillar Axiom system. You can also copy the alert information to the workstation clipboard.

- 1 From the **Monitor** tab, click **System Alerts**.
- 2 Select an alert from the list.
- 3 Click **Actions > Manage System Alert**.

Result:

The Manage Alert dialog appears.

- 4 Read the information about the system alert.
- 5 (Optional) Click **Copy to Clipboard** button to save the alert information to your workstation clipboard.
- 6 When finished, click **OK**.

Related references

- [Manage System Alert Dialog](#)

Related tasks

- [Display System Alerts](#)
- [Delete a System Alert](#)

Display System Alerts

You can view an overview of the system alerts generated by the Pillar Axiom system.

- 1 From the **Monitor** tab, click **System Alerts**.

Result:

The System Alerts overview page displays.

- 2 Review the system alert list to ensure that the information is what you expect.

Related tasks

- [Delete a System Alert](#)
- [Manage System Alerts](#)

Delete a System Alert

You can delete an alert generated by the Pillar Axiom system. However, before deleting the alert, ensure that you address the source of the alert first.

- 1 From the **Monitor** tab, click **System Alerts**.

- 2 Select an alert from the list.

- 3 Click **Actions > Delete System Alert**.

Result:

The Delete Alert dialog displays.

- 4 Read the information about the system alert.

- 5 Click **OK**.

Related tasks

- [Display System Alerts](#)

About Clearing Pinned Data

Pinned data can occur when issues arise regarding the Brick storage array. In such a case, data to be written to that array remains in the battery-backed memory of the Slammer storage controller.

Each logical volume maintains a time-ordered record of committed transactions (set of modified blocks). These records are kept within a dedicated area of the battery-backed memory that belongs to the owning Slammer control unit (CU). The system continuously (but asynchronously) flushes these records to the appropriate Bricks in the background. For SAN LUNs, these records are managed within what are called a *write cache*.

Note: These records reside on the same Slammer CU as the volume itself. A mirror of the cache is kept on the partner CU. The mirror allows the system to recover from a failure of the owner CU.

An administrator-initiated shutdown request will fail if any user data is still cached and has not yet been written to physical storage. If the Slammers cannot communicate with the Bricks to flush the cached data, the Pillar Axiom system retains, or *pins*, the data in cache.

If you receive a system alert about pinned data when you initiate a shutdown request, check the **Monitor > Hardware > Bricks** overview page for details about the Bricks. Resolve any hardware issues that may exist. Hardware issues can prevent communication between Slammers and Bricks and can prevent the system from flushing the cached data to storage.

Note: If you need additional help, contact the Oracle Pillar Customer Support for more information on clearing the pinned data.

About Scheduled Jobs

You can use job schedules to generate Clone LUNs on a regular basis. The Pillar Axiom system generates these clones at the desired time and frequency based on the job options.

You can create, modify, view, or delete a job schedule from the following pages:

- Data Protection tab when you are create or modify a LUN.
- Protection Schedules page located in the Protect tab.
- Scheduled Jobs page located in the Monitor tab, which provides limited job functions.

You can create a job schedule and enable it to start generating clones immediately at the specified start time. Or, if you prefer, you can store the schedule on the Scheduled Jobs page and enable it later. You can also disable a schedule temporarily (if, for example, you want to keep it from interfering with scheduled maintenance) and then enable it again. Deleting a schedule removes it from the system, but disabling a schedule leaves it available for enabling later on.

Scheduled jobs will continue create Clone LUNs until you disable or delete the schedule.

View a Job Schedule

You can review the details of a scheduled job. For example, you can check the start time and recurrence interval for the protection of a particular volume.

- 1 From the **Monitor** tab, click **Scheduled Jobs**.
- 2 Select a scheduled job that you want to review from the available list.
- 3 Choose **Actions > View Schedule**.
- 4 Verify the schedule details are what you expected.
- 5 When you are finished, click **Close**.

Related references

- [Scheduled Jobs Overview Page](#)
- [Modify Scheduled Job Dialog](#)

Related tasks

- [Create LUN Data Protection Schedules](#)

Modify a Job Schedule

You can modify the details of a scheduled job. Modifying a schedule may be necessary when you want, for example, to change from a daily to a weekly schedule.

Note: If you are updating a Software Update schedule, use the Cancel a Scheduled Software Update procedure.

- 1 From the **Monitor** tab, click **Scheduled Jobs**.
- 2 Select a scheduled job that you want to modify from the available list.
- 3 Choose **Actions > Modify Schedule**.
- 4 From the Modify Scheduled Job dialog, enter a new name for the notification in the **Schedule Name** field.
- 5 Set the **Enabled** check-box as necessary to enable or disable the job.
- 6 Click the arrow to the right of **Start Time** to select a revised day and time for your schedule to start.
- 7 Choose a new frequency for your schedule, as necessary.
- 8 Choose a **Recurrence** value for your schedule, as necessary.
- 9 To save your changes, click **OK**.

Related references

- [Scheduled Jobs Overview Page](#)
- [Modify Scheduled Job Dialog](#)

Related tasks

- [Create LUN Data Protection Schedules](#)
- [Schedule the Software Update](#)
- [Cancel a Scheduled Software Update](#)

Delete a Job Schedule

You can delete a scheduled job. For example, you can cancel a logical volume clone schedule or a scheduled software update.

- 1 From the **Monitor** tab, click **Scheduled Jobs**.
- 2 Select a scheduled job that you want to delete from the available list.
- 3 Choose **Actions > Delete Schedule**.

Note: Deleting a job schedule stops all scheduled activity.

- 4 To delete the job schedule, click **OK**.

Related references

- [Scheduled Jobs Overview Page](#)
- [Modify Scheduled Job Dialog](#)

Related tasks

- [Create LUN Data Protection Schedules](#)
- [Schedule the Software Update](#)

CHAPTER 11

Perform Diagnostic Operations

About Pillar Axiom Diagnostics

Someone from the Oracle Pillar Customer Support may request that you run one or more of the support tools and send the diagnostic output to Pillar Data Systems.

A Pillar Axiom system is fault tolerant. The system detects anomalies and automatically fails over to a partner component to maintain data availability. No intervention is required, unless a technician is needed to replace a hardware component.

Even fault-tolerant systems with a long mean time between failure (MTBF) rate cannot avoid component failure forever. If a component failure results in system instability, support tools are available to diagnose and fix the issue.

To support a Pillar Axiom system, you can perform any of the following actions:

- Collect system information and download the system log bundle from the Pilot or send the bundle to the Call-Home server.
- Diagnose Slammer hardware and software issues.
- Resolve connectivity trouble.
- Troubleshoot and isolate errors in the Storage System Fabric (SSF).
- Shut down and restart a Pillar Axiom system.
- Set halt points that pause the system startup process.
- Reset the system to its factory configuration.

Related concepts

- [*About System Log Bundles*](#)
- [*About Slammer Diagnostics and Connectivity Testing*](#)
- [*About System Halt Points*](#)

Related tasks

- [*Reset Pillar Axiom System*](#)
- [*Run PITMAN Diagnostics*](#)
- [*Shut Down the Pillar Axiom System Software*](#)
- [*Restart the Pillar Axiom System Software*](#)

Display the System Status Summary

Sometimes a high-level view of the status of a Pillar Axiom system is needed.

This summary includes the status of all the hardware components in the system and a brief list of the events and notifications that have occurred.

Tip: You can also obtain a list of current system alerts, event information, and system status information by pointing your browser to the Pillar Axiom web server. Simply specify the IP address of the Pilot management controller or the name of the Pillar Axiom system as the address to open. This facility is convenient when you want to download this information to a mobile device.

- 1 From the **Monitor** tab, click **Status Summary**.
- 2 Verify that the displayed information is what you expect.
 - The Pilot section indicates the operational mode and status of each control unit.
 - The Slammer section indicates the type of each Slammer in the system and the status of each of their control units.
 - The Brick section indicates the status of each Brick in the system.
 - The UPS section indicates the type of power source for each uninterruptible power supply (UPS) and the status of their batteries.
 - The event log section indicates by severity level the number of events that exist for each level.
 - The event notification section indicates the number of notification recipients and monitored events, plus other information.
- 3 (Optional) To retrieve the most current information, click **Refresh**.

If you detect a situation that needs to be addressed, you can perform the following actions:

- To view additional details about a hardware component and to perform other diagnostic tasks, navigate to **Monitor > Hardware**.
- To view additional details about system alerts or events, navigate to **Monitor > System Alerts** or to **Monitor > Event Log**, respectively.

Related concepts

- [About Accessing Pillar Axiom 600 Applications](#)

About Data Consistency

Data consistency refers to the integrity of the parity data, which is maintained by the RAID controller, not to the integrity of user-created data.

You might want to run the data consistency test after replacing a drive or a RAID controller in a Brick. Also, Oracle Pillar Customer Support might request that you run a data consistency test for diagnostic purposes.

Running the test, which executes within the RAID controllers, impacts Pillar Axiom system performance. You have two options to choose from when performing this test:

- **High Priority:** Permits the verification check to affect I/O performance by up to 30%.
- **Low Priority:** Permits the verification check to affect I/O performance by up to 10%.

The High priority option yields faster results, but has a greater impact on system performance. A Low priority option is recommended if you want to check the Brick after replacing a drive or a RAID controller.

Data consistency failures are typically isolated to the drive or RAID controller error handling. The RAID controller compensates for some of the errors that are encountered during the tests. However, if an error persists that cannot be fixed, the system displays *Fail* on the Data Consistency overview page. In this case, collect the Pillar Axiom data logs and contact Oracle Pillar Customer Support.

Related references

- [Data Consistency Overview Page](#)
- [Create Log Bundle Dialog](#)

Related tasks

- [Verify Data Consistency](#)

Verify Data Consistency

You can verify the integrity of the parity data, which is maintained by the RAID controller, by running the data consistency test on a selected Brick. The RAID controller writes and otherwise maintains the parity data (which corresponds to the user data) on various drives within a certain Brick. After replacing a drive or a RAID controller in one of those Bricks, you might want to confirm that this parity data is consistent on that Brick.

- 1 From the **Support** tab, click **Tools > Data Consistency**.
- 2 On the Data Consistency page, select a Brick that you want to verify.
- 3 Choose **Actions > Data Consistency**.
- 4 From the Verify Data Consistency dialog, specify how much I/O time to give to this operation. Valid priority options:
 - **High Priority**
 - **Low Priority**

For example, if you specify High Priority, this operation could impact Brick performance by up to 30%.

- 5 To start the data verification, click **OK**.

After the completion of the data verification, the results appear on the Data Consistency page. Use the refresh button to update the page, if necessary.

Related concepts

- [About Pillar Axiom Diagnostics](#)

About System Log Bundles

To help diagnose a situation that might exist, the Oracle Pillar Customer Support might request that you collect into a single bundle certain logs and other diagnostic information and then send the bundle to Pillar Customer Support for analysis.

System information can be collected from the following sources and placed into the system log bundle:

- Pilot hardware component
- Slammer hardware components
- Brick hardware components
- Client hosts

When you create a system log bundle, you can indicate the extent of information coverage for each of the above selected sources. You can specify that all logs are to be included or just the more recent logs. For the recent logs, you can specify the number of hours back in time for which information is to be collected.

You can also include in the log bundle the statistics and the existing configuration of the Pillar Axiom system. All log bundles contain the time and date at which the bundle was collected.

After you create a log bundle, you can have the system send the bundle to the Call-Home server, or you can download the bundle and then send it to Pillar manually. In either case, the logs are transferred securely using encryption.

Related concepts

- [About the Network Interfaces](#)

Related tasks

- [Collect Statistics](#)
- [Create a Log Bundle](#)
- [Delete Log Bundles](#)
- [Download Log Bundles](#)
- [Send Logs to Call-Home Server](#)
- [View UI Client Logs](#)

View UI Client Logs

You can display a folder of client logs, which contain a history of the graphical user interface (GUI) activities that have been performed on the Pillar Axiom system.

- 1 From the **Support** tab, click **Tools > System Logs**.
- 2 Choose **Actions > View UI Client Logs**.

Result:

Depending on your operating system, the following actions occur:

- Windows: The system opens an explorer window to the client logs location.
- Linux: The system changes the directory to the client logs location.

Use a text editor or reader to view the contents of the client logs.

Related concepts

- [About System Log Bundles](#)

Related references

- [System Logs Overview Page](#)

Create a Log Bundle

If a Pillar Axiom hardware component fails, the system writes log bundles so that the issue can be investigated. The Oracle Pillar Customer Support might request that you collect the logs and send them to Pillar Data Systems for analysis.

- 1 From the **Support** tab, click **Tools > System Logs**.
- 2 Choose **Actions > Create Log Bundle**.

Result:

The Create Log Bundle dialog box displays with all of the components selected for data collection.

- 3 (Optional) Enter a short description for the log collection in the **Collection Reason** field.
- 4 Use the buttons to select groups of components or select individual components from the list, as necessary:

- **Select All**
 - **Deselect All**
 - **Select All Slammers**
 - **Select All Bricks**
- 5 (Optional) Click the **Automatically send log bundle to Call-Home server** checkbox to send the log files to the Call-Home server.
 - 6 Choose the **Collection Period** for the log collection:
 - **Most Recent Logs:** Choose the extent of the collection period in hours or days.
 - **All Logs:** Collects all available logs regardless of time constraints.
 - 7 Click **Select Host**
 - 8 From the **SAN Host Log Selection** dialog, select the host from which to collect logs.
 - 9 When finished selecting the hosts, click **OK**.
 - 10 To create the log bundle, click **OK**.

Result:

The system begins collecting the data logs and displays the log bundle in the System Logs overview page.

Related references

- [Create Log Bundle Dialog](#)
- [System Logs Overview Page](#)

Related tasks

- [Download Log Bundles](#)
- [Delete Log Bundles](#)

Collect Statistics

The Pillar Axiom system generates performance statistics for logical volumes and storage area network (SAN) protocols. The statistics also include capacity usage and system health information. The Oracle Pillar Customer Support might request that you collect the system performance statistics and transmit the data to Pillar Data Systems for analysis.

- 1 Log in to the Pillar Axiom Storage Services Manager (GUI).

- 2 From the **Support** tab, click **Tools > System Logs**.
- 3 Choose **Create Log Bundle** from the **Actions** menu.
Result:
The Create Log Bundle dialog box displays with all of the components selected for data collection.
- 4 Click **Deselect All**.
- 5 In the Collect column, select **Yes** beside **Statistics**.
- 6 Select a collection period.
 - **Most Recent Logs**: Choose the extent of the collection period in hours or days.
 - **All Logs**: Collects all available logs regardless of time constraints.
- 7 Click **OK**.
- 8 Select the collection when it appears in the System Logs list.
- 9 Choose **Download Log Bundle** from the **Actions** menu.
- 10 Select a directory on a local drive as the **Target Download Location**, and click **OK**.

Related concepts

- [About System Log Bundles](#)

Related references

- [System Logs Overview Page](#)

Download Log Bundles

When a Pillar Axiom hardware component fails, the system writes logs that contain information about the incident. These logs are useful when troubleshooting.

A log bundle contains a number of system logs and is formatted as a TAR file, which you can download to your workstation. The Oracle Pillar Customer Support might request that you collect the logs and send them to Pillar Data Systems for analysis.

- 1 From the **Support** tab, click **Tools > System Logs**.
- 2 Select a log bundle to download from the System Logs list.
- 3 Choose **Actions > Download Log Bundle**.

- 4 Click the browse button (...) to select the target file location on your workstation.
- 5 To save the log files, click OK.

Related references

- [System Logs Overview Page](#)
- [Create Log Bundle Dialog](#)

Send Logs to Call-Home Server

In the event of a Pillar Axiom hardware component failure, the system writes logs that contain information about the incident. You can send the system log bundles to the Call-Home server as necessary.

The Oracle Pillar Customer Support may request that you collect the logs and send them to Pillar Data Systems for analysis. If you want to automatically send the logs to the Call-Home server select the Automatically send log bundle to Call-Home server option in the Collect Log Bundles action.

- 1 From the **Support** tab, click **Tools > System Logs**.
- 2 Select a log bundle to send from the System Logs list.
- 3 Choose **Actions > Send Log Bundle to Call-Home Server**.

Result:

The system displays the Send Logs to Call-Home Server dialog box.

- 4 To send the file to the Call-Home server, click OK.

Related references

- [Create Log Bundle Dialog](#)

Related tasks

- [Configure Call-Home Settings](#)
- [Create a Log Bundle](#)

Delete Log Bundles

Deleting the logs allows you to remove from the system those log bundles that you no longer need.

Note: Only the Pillar Support and Support roles can delete log bundles. After a log bundle is deleted, all information within the bundle about past system behavior is permanently gone.

- 1 From the **Support** tab, click **Tools > System Logs**.
- 2 Choose **Actions > Delete Log Bundles**.
- 3 Choose the types of log bundles to delete.

Available bundle types:

- **Slammer Logs.** Removes all of the Slammer log bundle files.
 - **Brick Logs.** Removes all of the Brick log bundle files.
 - **Log Collections.** Removes all of the log collections.
- 4 (Optional) To remove the logs associated with a specific Brick RAID controller, click **Add**.

The Add Raid Controller To Clear History For dialog box appears. Specify the RAID controller:

- First, choose the **Brick** name from the drop-down list.
 - Then, choose the **RAID group** from the drop-down list.
 - Then, click **OK**.
- 5 (Optional) To remove a selected item from the list, click **Remove**.
 - 6 (Optional) To remove the RAID controller history files that are displayed in the list, click **Clear**.
 - 7 To delete the logs from the system, click **OK**.

Related references

- [Add RAID Controller to Clear History Dialog](#)
- [Create Log Bundle Dialog](#)

About Slammer Diagnostics and Connectivity Testing

Administrators can use two features of the Pillar Axiom Storage Services Manager to help characterize and isolate the source of Slammer issues. These issues can be related to Slammer hardware or software or to the connections between the Slammer and the public data network.

The Slammer diagnostics feature performs a suite of diagnostic tests on the hardware components and software modules in a Slammer control unit (CU). The hardware that is tested includes, for example, the motherboard, network interface cards, fans, and power supplies contained within the CU.

Note: During startup, the Pillar Axiom system always performs diagnostics on Slammer CUs.

The diagnostic tests on the hardware and software return detailed information to help a support administrator to characterize and isolate specific faults in the system. With this information, the support administrator can more easily determine which FRU needs to be replaced.

Important! Before running diagnostics on a Slammer CU, all applications using the control unit that will be tested should be closed. Then, the CU can be physically disconnected from the public data path.

A small form factor (SFP) loopback, which can be as simple as one side of an optical cable, is inserted into each port in the network interface module of the CU being tested. A loopback carries the electrical signal from the transmit side of an optical port to the receive side of the port.

This SFP loopback allows the diagnostic tests to run successfully.

While the diagnostic tests are being run, the status of the Slammer control unit appears as Failed Over. When the tests are complete, the status changes to Normal.

Slammer connectivity can be tested to isolate possible issues with its connections to the public data network. Administrators can request certain commands to be executed within the Slammer, such as `perf`, which checks CPU utilization within the Slammer.

Related concepts

- [About PITMAN Diagnostic Tool](#)
- [About System Startup](#)

Related references

- [Slammer Connectivity Commands](#)

Related tasks

- [Run Slammer Diagnostics](#)
- [View Slammer Diagnostics](#)
- [Test System Connectivity](#)

Run Slammer Diagnostics

The Oracle Pillar Customer Support might request that you run Slammer diagnostics on a selected control unit (CU) to test its hardware components. The results of these tests can help you take the appropriate steps to ensure data integrity and to reduce downtime.

Prerequisites:

- Only Pillar Support and Support roles can run Slammer diagnostics.
- Ensure that all clients that are accessing the target Slammer CU are idle. Alternatively, ensure that the zoning and client configuration are set up to handle the condition of the CU going offline.

Hardware diagnostics can be run in response to various conditions such as certain hardware faults, the crossing of critical statistics thresholds, and certain generated events. The goal of these diagnostics is to isolate the cause of that condition. Once invoked, a hardware diagnostic performs a particular test and returns a Pass or Fail status and, in the case of failure, detailed information about the failure.

**Caution**

Do not initiate Slammer diagnostics on a CU that is currently serving data; otherwise, data loss might occur.

To run diagnostics on a Slammer CU, the system disables the write cache in the target CU, moves all the resources of the CU to its partner CU, and takes the target CU offline. All LUNs that are assigned to the Slammer are put into Conservative mode. During this period, the performance of the Slammer is diminished.

- 1 Disconnect the target CU from the public network by removing the cables from the network interface module (NIM).
- 2 Attach a loopback connector to each port on the NIM of the target CU.

- 3 Log in to the Pillar Axiom Storage Services Manager using one of the support roles.
- 4 From the **Monitor** tab, click **Hardware > Slammers**.
- 5 Choose **Actions > Run Diagnostics**.
- 6 Using the **Slammer Control Unit** drop-down list, select the CU for which you want to run diagnostics.
- 7 Read the warning on the **Slammer Control Unit Diagnostics** dialog box, then click **Next**.

Result:

After the diagnostics is completed, the **Success** dialog appears.

- 8 To display the diagnostics test results, click **Next**.
- 9 Review the results of the diagnostics test.
- 10 To close the diagnostics dialog, click **Finished**.
- 11 Remove the loopback connector from the target CU NIM and reconnect the NIM to the public data network.

Related concepts

- [About Slammer Diagnostics and Connectivity Testing](#)

Related tasks

- [View Slammer Diagnostics](#)

View Slammer Diagnostics

Administrators logged in with one of the support roles can review the results of the latest Slammer diagnostics.

Only Pillar Support and Support roles can view the Slammer diagnostics results.

- 1 From the **Monitor** tab, click **Hardware > Slammers**.
- 2 Choose **Actions > View Diagnostics**.
- 3 From the **Slammer Control Unit** drop-down list, select the CU for which to view diagnostics test results.
- 4 To display the diagnostics test results, click **Next**.
- 5 Review the results of the diagnostics test.

- 6 To close the diagnostics dialog, click **Finished**.

Related concepts

- [About Slammer Diagnostics and Connectivity Testing](#)

Related tasks

- [Run Slammer Diagnostics](#)

Slammer Connectivity Commands

Commands can be executed on a Slammer control unit (CU) to help with the diagnosis of issues related to the data path connections.

Table 22 SAN Slammer commands

Command	Syntax	Description
<code>perf</code>	<code>perf [-c]</code> -c Reset the counters after returning the statistics. Environment variables: None	<p>Checks CPU utilization of the specified Slammer CU. This command returns the CPU statistics for the following categories:</p> <ul style="list-style-type: none"> • The idle process • The kernel time • All process IDs that are running <p>When you use the <code>-c</code> option, the next invocation of <code>perf</code> will return data accumulated from that point.</p> <p>Example:</p> <p>The following command displays the utilization statistics for all threads running on the selected Slammer and then clears the counters for that Slammer.</p> <p><code>perf -c</code></p>

Related references

- [Test Connectivity Dialog](#)

Test System Connectivity

Use the Test Connectivity page to identify any communication issues between a Slammer storage controller and the customer data network.

- 1 From the **Support** tab, click **Tools > System Trouble**.
- 2 Choose **Actions > Test Connectivity**.
- 3 Choose the Slammer from the drop-down list.
- 4 Choose the control unit from the drop-down list.
- 5 Enter the command in the **Command Line** field.
- 6 Enter any necessary variables in the **Environment Variables** field.

Enter the variables in the form of *variablename=va1ue*. Where *variablename* is the environment variable and *va1ue* is the text passed to the system.

- 7 Click **Execute**.

Result:

The **Command Output** displays the results from the Pillar Axiom system.

Related references

- [Test Connectivity Dialog](#)
- [Slammer Connectivity Commands](#)

About PITMAN Diagnostic Tool

The Private Interconnect Topology Manager (PITMAN) in the Automatic mode is a statistics generator tool that runs by default on the Pillar Axiom system to collect high-level statistical and error information on the private interconnect (PI) (also known as the Storage System Fabric (SSF)) without disabling customer access to data.

In the Manual mode, PITMAN is a diagnostic tool used to troubleshoot or isolate errors within a specific domain of the SSF. It enables you to selectively disable the components within the SSF network and identify malfunctioning hardware.

Each Slammer control unit (CU) runs a PITMAN instance that guides you to take appropriate action in response to errors.

A warmstart of the Slammer CU that is running PITMAN terminates its operation in the manual diagnostic mode and returns PITMAN to a monitoring state where it acts as a statistics generator.

PITMAN commands perform the following tasks on the Slammer CU:

- Checks the status of PITMAN instances
- Collects statistical information on the SSF network in the Master Analytic Record Keeping System (MARKS) database
- Generates traffic on the SSF network between the specified fabric ports
- Identifies the SSF ports or the specified link device to be disabled or enabled in the SSF network



Caution

Care must be taken when disabling Slammer ports since it can have unwarranted consequences and result in emergency shutdowns or cause data corruption.

Note: The MARKS database keeps a record of the problems that PITMAN has detected in the SSF network and the subsequent actions that have been taken.

Note: Contact Oracle Pillar Customer Support to manually isolate errors on a system that encounters repeated warm starts.

Related references

- [Run PITMAN Diagnostics Dialog](#)

Run PITMAN Diagnostics

You can troubleshoot and isolate errors within the Storage System Fabric (SSF) of the Pillar Axiom system.

- 1 From the **Support** tab, click **Tools > System Trouble**.
- 2 Choose **Actions > Run Pitman Diagnostics**.
- 3 Enter the PITMAN command in the **Command Line** field.

Example:

```
TrafficGenOn mode=auto peer=all
```

- 4 Click **Execute**.

Result:

The **Command Output** displays the results from the Pillar Axiom system.

```
TrafficGenOn:  
peer=0x2008000b080459a2 OK  
peer=0x2009000b0804593a OK  
peer=0x2008000b080459aa OK  
peer=0x2008000b08045932 OK
```

Related concepts

- [About PITMAN Diagnostic Tool](#)

Related references

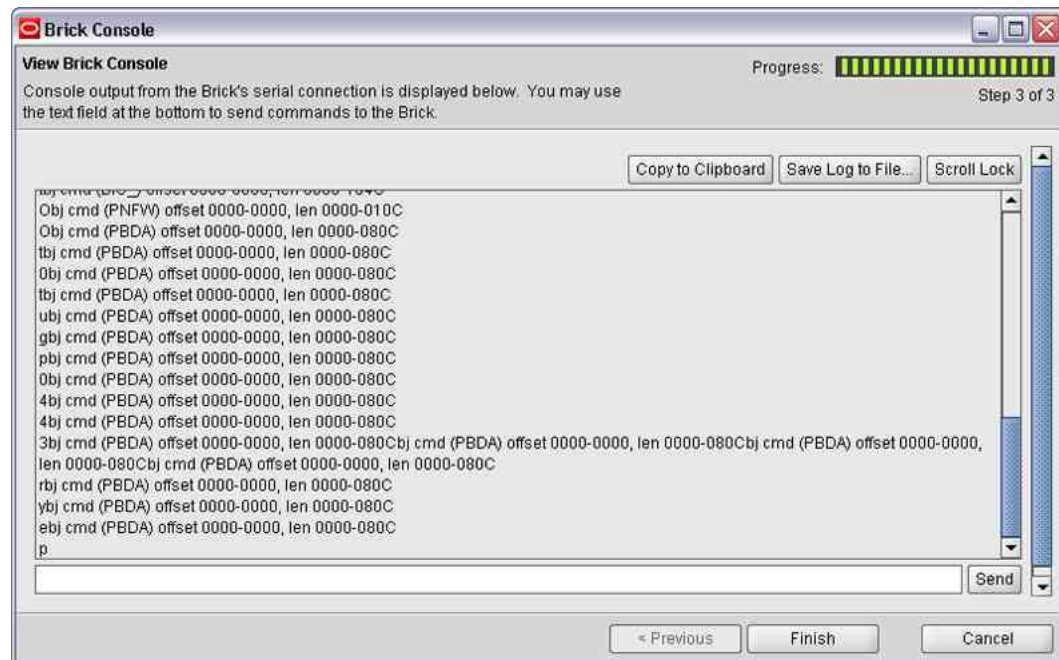
- [Run PITMAN Diagnostics Dialog](#)

About the Brick Console

On occasion, a support administrator might want to access the Brick console to issue commands to a particular Brick control unit (CU) and to view the responses to those commands.

When the support administrator uses the Brick console to access a Brick CU, the output being generated by that CU appears in the console.

Figure 8 Brick console



Note: The Brick console can be used by only one login session at a time. When launching the console, the administrator has the option of forcing other sessions to disconnect.

During a debug session, the support administrator has the option of capturing all generated output at any time and copying that output to the clipboard or saving it to a file.

This log contains the World Wide Name of the Brick and a timestamp, which can help in a review of the debug session.

When a situation occurs within a Brick CU, sometimes the recovery of that CU requires access to a number of password protected commands that are available on the CU. The Brick console provides access to those commands.

**Caution**

Brick console commands are to be used for recovery purposes only. They are used to gather information or to clear conditions that cannot otherwise be accomplished. Brick console commands should never be executed without assistance from the Oracle Pillar Customer Support. Execution of these commands can be performed only by the support administrator.

The support administrator can execute a variety of Fibre Channel (FC) and SCSI Brick commands, which are provided by Pillar Customer Support. Each of these commands allows the administrator to test or debug the Brick RAID controller in some way. Before executing any of these commands, the support administrator must enter a password. This password is embedded in the RAID firmware and is not changeable.

Related tasks

- [View Brick Console](#)
- [Run Brick Commands](#)

View Brick Console

In most circumstances, you might want to capture the output that is being generated by a Brick RAID controller and, if requested, to send that output to the Oracle Pillar Customer Support.

Important! When you execute a Brick command, we recommend that you always capture the output before and after command execution.

- 1 From the **Monitor** tab, click **Hardware > Bricks**.
- 2 Choose **Actions > View Brick Console**.

Result:

The Brick Console dialog appears and an informational warning is displayed.

Note: This warning is to inform you that, in order for you to execute Brick commands, you must be using the support administrator account.

- 3 Click **Next**.
- 4 In the **Brick** drop-down list, select the Brick that contains the RAID controller that you want monitor.
- 5 In the **Raid Controller** drop-down list, select the control unit (CU) to be monitored.

- 6 (Optional) To ensure that no other **Brick** console session is running, select the **Disconnect other users from the Brick console** option.
- 7 Click **Next**.
Result:
Output from the RAID controller that is associated with the CU that you selected appears in the console.
- 8 (Optional) To control the display, click **Scroll Lock**.
The first time you click this control, the display temporarily stops. To restart the display, click the control again.
- 9 (Optional) Capture the output from the RAID CU.
Valid options:
 - **Copy to Clipboard:** Transfers the displayed output to a temporary memory buffer in your client host so you can copy (paste) that output to another, permanent location.
 - **Save Log to File:** Transfers the displayed output directly to a file at any location on your network.
- 10 To terminate the **Brick** console session, click **Finish**.

Related concepts

- [About the Brick Console](#)

Run Brick Commands

To help in the recovery from a Brick error, a support administrator can access the Brick console and issue commands to the Brick RAID controller.

Prerequisite:

You have logged in to the Pillar Axiom Storage Services Manager using the support administrator account.



Brick console commands are to be used for recovery purposes only. They are used to gather information or to clear conditions that cannot otherwise be accomplished. Brick console commands should never be executed without assistance from the Oracle Pillar Customer Support. Execution of these commands can be performed only by the support administrator.

- 1 From the **Monitor** tab, click **Hardware > Bricks**.

- 2 Choose **Actions > View Brick Console**.

Result:

The Brick Console dialog appears and an informational warning is displayed.

Note: This warning is to inform you that, in order for you to execute Brick commands, you must be using the support administrator account.

- 3 Click **Next**.
- 4 In the **Brick** drop-down list, select the Brick that contains the RAID controller that you want monitor.
- 5 In the **Raid Controller** drop-down list, select the control unit (CU) to be monitored.
- 6 (Optional) To ensure that no other **Brick** console session is running, select the **Disconnect other users from the Brick console** option.
- 7 Click **Next**.

Result:

Output from the RAID controller begins to appear in the console.

- 8 In the text field at the bottom of the console, enter the string `login` and then click **Send**.

Result:

When prompted for a password, enter the required password.

Note: Contact the Oracle Pillar Customer Support for the password.

- 9 In the text field at the bottom of the console, enter a Brick command and then click **Send**.

Result:

The RAID controller attempts to execute the command and displays the results in the console.

- 10 (Optional) Capture the output from the RAID CU.

Valid options:

- **Copy to Clipboard:** Transfers the displayed output to a temporary memory buffer in your client host so you can copy (paste) that output to another, permanent location.
- **Save Log to File:** Transfers the displayed output directly to a file at any location on your network.

- 11 To terminate the **Brick** console session, click **Finish**.

Related concepts

- [*About the Brick Console*](#)

Shut Down the Pillar Axiom System Software

The Pillar Axiom Storage Services Manager systematically shuts down all of the software running on the system. Once the software is shut down, you can safely power down the hardware.

The Pillar Axiom system is composed of many hardware components and software processes that have dependencies on other components and processes. To ensure that all dependencies are satisfied and that the Pillar Axiom system is shut down in an orderly fashion, use the **Shutdown** option.

While the system is in a shutdown state, the only actions you can perform are to display system status and to restart the system.

Important! If you need to power off the system for more than 48 hours, remove the batteries.

- 1 From the menu bar, click **Axiom > Shut Down**.
- 2 Read the information on the confirmation dialog, then perform one of the following:
 - To shut down the system, click **OK**.
 - To cancel the shutdown request, click **Cancel**.

Result:

The system status icon changes to a yellow triangle with the message: *Prepare for Shutdown*. The system continues to shut down all of the software, however the Pillar Axiom Storage Services Manager remains running. After the software is shutdown, the Asset Information page (**Configure > Summary > System**) displays *Status: Shutdown*.

When you are ready to restart the software, use the **Axiom > Restart** action.

Related concepts

- [About System Startup](#)

Related tasks

- [Restart the Pillar Axiom System Software](#)

Restart the Pillar Axiom System Software

You can restart the Pillar Axiom system software, which is necessary after powering up the system hardware.

The Pillar Axiom Storage Services Manager restarts the system software by first shutting down the software running on the hardware components, and then starts the software again.



Caution

Performing a system restart may cause data loss.

You may want to send a message to the system users that a system restart is about to begin. You cannot schedule a system restart.

- 1 From the menu bar, click **Axiom > Restart**.
- 2 Read the information on the confirmation dialog, then click **OK**.

If the Pillar Axiom Storage Services Manager cannot safely shutdown the system to begin the restart, a second dialog appears. Read the message, then do one of the following:

- To close the dialog so you can resolve the problem, click **Cancel**.
- To ignore the problem and continue with the system restart, click **Force Restart**.

Result:

The system starts up and the Asset Information page (**Configure > Summary > System**) displays *Status: Normal*.

Related concepts

- [About System Startup](#)

Related tasks

- [Shut Down the Pillar Axiom System Software](#)

About System Startup

The Pillar Axiom system starts up when the system is powered on, when the system undergoes a disruptive software update, or when a system administrator explicitly requests a restart.

Controlled by the Pilot management software, the startup process proceeds in an orderly way.

Note: When a system starts, the data paths are not available until the Slammers enter a Ready state.

During a system startup, the management software obtains heartbeats from the Slammers and verifies the configuration of the Pillar Axiom system.

When a system starts, the Slammer CU progresses through two stages. The first stage is controlled by the programmable read only memory (PROM) that resides in the Slammer CU. The second stage is controlled by the Configuration Server in the Pilot management controller.

A Slammer CU starts by executing a page that resides in its PROM. You can watch the Slammer LEDs to monitor the progress of this stage. (Refer to the *Pillar Axiom Hardware Installation Guide* for an explanation of these startup codes.)

During the first stage, the Slammer PROM performs many actions, including the following sequence:

- 1 Runs a set of power-on tests
- 2 Starts hardware temperature monitoring
- 3 Initializes the private management interface (PMI) on the Slammer CU
- 4 Starts an application called *netboot*, which downloads the Slammer software from the Pilot
- 5 Initializes the Slammer software

If this stage fails, the Slammer LEDs signal which software module was executing when the startup process failed. The names of these modules all have a prefix of `EEL_`, as described in the *Hardware Installation Guide*.

Note: These LED signals are progress codes that you can use to determine how far the PROM progressed before a failure occurred, causing the Slammer CU to halt. These codes, however, do not necessarily imply why the startup failed.

If this stage succeeds, the second stage begins, in which the Slammer software components are initialized.

Related concepts

- [*About Updating the Pillar Axiom Software*](#)
- [*About System Halt Points*](#)

Related tasks

- [*Shut Down the Pillar Axiom System Software*](#)

About System Halt Points

By enabling system halt points, you can more easily diagnose those situations in which you cannot get a Slammer control unit (CU) to start successfully because of some software condition.



Caution

System halt points are to be used for recovery purposes only. They are used to gather information or to clear conditions that cannot otherwise be accomplished. Halt points should never be set or cleared without assistance from the Oracle Pillar Customer Support. Management of system halt points can only be performed by the Primary administrator and the Support administrator.

When a system starts, the Slammer CU progresses through two stages. The first stage is controlled by the programmable read only memory (PROM) that resides in the Slammer CU. The second stage is controlled by the Configuration Server in the Pilot management controller.

In this second stage, the Pilot performs several checks on each Slammer CU and, if all is well, puts the CU into a Ready state. The Pilot then, by sending one command at a time to each CU in a defined sequence, starts the software components that were downloaded to the Slammer.

The Pillar Axiom Storage Services Manager and Pillar Axiom Command Line Interface (CLI) products both identify the names of these Slammer software components with a prefix of `PDS_`. Support administrators can selectively control the execution of these software components by enabling and disabling halt points on those PDS components.

If the Support administrator has previously enabled a halt point on one of these software components, when the time comes for the Pilot to send to each Slammer the command to start the software component, the Pilot instead pauses and does not send the command.

When the startup process stops, the Support administrator can take various diagnostic actions, such as dumping a log file or reading an internal table.

After completing those actions, the Support administrator can instruct the startup process to continue. At this point, the Pilot now sends to each Slammer the command on which the Pilot paused.

Related concepts

- [About Clearing Pinned Data](#)
- [About System Startup](#)

Related tasks

- [Create a Log Bundle](#)
- [Continue System Startup](#)
- [Manage System Halt Points](#)

Manage System Halt Points

You can enable halt points for diagnostic purposes. Halt points pause the Pillar Axiom startup sequence at the specified component step, allowing you to perform various diagnostics tasks.

**Caution**

System halt points are to be used for recovery purposes only. They are used to gather information or to clear conditions that cannot otherwise be accomplished. Halt points should never be set or cleared without assistance from the Oracle Pillar Customer Support. Management of system halt points can only be performed by the Primary administrator and the Support administrator.

- 1 From the **Support** tab, click the **Tools > System Halt Points**.
- 2 Choose **Actions > Manage Halt Points**.
- 3 (Optional) To enable a halt point for a component step, highlight the step and choose **Yes** in the **Active** column.

You can enable up to eight halt points on your system.

- 4 (Optional) To disable all active halt points in the list, click **Clear**.

Clearing all active halt points enables the system, when you instruct it to continue, to resume the startup process without any additional system halts.

- 5 Click **OK**.

After the system starts and the startup process subsequently pauses at an enabled halt point, you can perform diagnostic tasks such as collecting logs, reviewing the contents of system tables, and so forth. After you complete these tasks, you can direct the system to continue the startup process.

Related concepts

- [About System Halt Points](#)

Related references

- [Manage Halt Points Dialog](#)
- [System Halt Points Overview Page](#)

Related tasks

- [Continue System Startup](#)

Continue System Startup

After using system halt points to stop the Pillar Axiom startup sequence at a specified component step, you can easily resume system startup.

Important! System halt points are to be used for recovery purposes only. They are used to gather information or to clear conditions that cannot otherwise be accomplished. Halt points should never be set or cleared without assistance from the Oracle Pillar Customer Support. Management of system halt points can only be performed by the Primary administrator and the Support administrator.

- 1 From the **Support** tab, click **Tools > System Halt Points**.
- 2 Choose **Actions > Continue**.

Result:

The system continues the startup process and proceeds to the next halt point, if any.

- 3 Click **OK**.

Related concepts

- [About System Halt Points](#)

Related references

- [Manage Halt Points Dialog](#)

Related tasks

- [Manage System Halt Points](#)

Reset Pillar Axiom System

In extremely rare circumstances, you might need to reset your system serial number and system configuration.

Prerequisites:

A special encryption file from the Oracle Pillar Customer Support.

The encryption file performs the following actions:

- Deletes all data stored on the Pillar Axiom system.
- Resets the configuration to an initial state.
- Resets the system serial number.



Caution

Because this action deletes all user data along with the system configuration, the system prompts you to confirm the operation. Be absolutely sure you want to reset your system, because *all data in your system will be lost*.

- 1 From the **Support** tab, **Tools > System Trouble**.
- 2 Choose **Actions > Reset System**.
Result:
The Reset System dialog box displays.
- 3 Read the WARNING text, and when you are ready, click the browse button (...) to proceed.
- 4 Navigate to and select the encrypted configuration file that you received from the Oracle Pillar Customer Support.
- 5 Click **OK**.
- 6 When prompted to confirm the deletion of all data and system configuration, click **OK** to reset your system.

Related references

- [Reset System Dialog](#)

CHAPTER 12

Manage Reports

About Generated Reports

Generated reports provide listings of configuration details and statistical information about your system that you can download to your client from the Pillar Axiom system in various formats.

You can generate a statistical report immediately at the Generated Reports page, or you can schedule a report to be generated at a specified time at the Scheduled Reports page.

You can generate the following types of reports:

SAN Hosts	Provides statistical information on the host servers and configured components currently included in your storage area network (SAN).
Storage Performance	Provides performance information about the LUNs on the Pillar Axiom system. Includes operations/second, read MB/s, and write MB/s.
Storage Use	Provides storage capacity information on the storage currently available on the Pillar Axiom system. Includes total capacity, allocated, free, and unavailable capacity, and storage use by Storage Class.
Storage Use per Volume	Provides capacity information for each logical volume on the Pillar Axiom system.
System Configuration	Provides detailed information on the configuration and status of the current Pillar Axiom system and all of its components, such as serial numbers, firmware versions, ports, and status, for the Pilot, Slammers, and Bricks.
System Configuration Summary	Provides a summary of the Pilot, Slammer, and Brick information included in the detailed System Configuration report.

You can download reports in the following formats:

Table 23 Report download formats

Format	Usage
CSV	Comma-separated values. Import into any spreadsheet or database.
Excel	Import directly into an Excel spreadsheet.
HTML	Display in a browser.
PDF	Printer-friendly online document.
XML	XML tagged document.

Related references

- [Generated Reports Overview Page](#)

Related tasks

- [Generate a Report](#)
- [Download a Report](#)

Generate a Report

You can generate one of a set of predefined reports to view statistical information about Pillar Axiom systems.

- 1 From the **Monitor** tab, click **Reporting > Generated Reports**.
- 2 Choose **Actions > Generate Report**.
- 3 From the **Type** drop-down menu in the Generate Report dialog, choose one of:

SAN Hosts	Provides statistical information on the host servers and configured components currently included in your storage area network (SAN).
Storage Performance	Provides performance information about the LUNs on the Pillar Axiom system. Includes operations/second, read MB/s, and write MB/s.
Storage Use	Provides storage capacity information on the storage currently available on the Pillar Axiom system. Includes total capacity, allocated, free, and unavailable capacity, and storage use by Storage Class.

Storage Use per Volume	Provides capacity information for each logical volume on the Pillar Axiom system.
System Configuration	Provides detailed information on the configuration and status of the current Pillar Axiom system and all of its components, such as serial numbers, firmware versions, ports, and status, for the Pilot, Slammers, and Bricks.
System Configuration Summary	Provides a summary of the Pilot, Slammer, and Brick information included in the detailed System Configuration report.

- 4 Click OK.

When the report is complete, the Generated Reports page displays the name of the report, the time the report was created, and the size of the report.

To see the contents of the report, select the name of the report in the Generated Reports Overview Page and download it in your preferred format.

Related concepts

- [About Generated Reports](#)

Related references

- [Generate Report Dialog](#)

Related tasks

- [Download a Report](#)

Download a Report

You can download generated reports to your client workstation in a variety of formats.

Only reports listed on the Generated Reports page can be downloaded.

Download reports to see their contents.

- 1 From the **Monitor** tab, click **Reporting > Generated Reports**.
- 2 Select the name of the report you want to download on the Generated Reports page.
- 3 Choose **Actions > Download Report**.
- 4 Choose a format from the **Format** drop-down menu in the Download Report dialog.

Choose one of:

- CSV
- Excel
- HTML
- PDF
- XML

5 Click the browse button (...) and choose the desired destination for the report.

6 Enter a filename in the File Name field, and click **Save**.

Result:

The path, filename, and extension appear in the Target Download Path field in the Download Report dialog.

7 Click **OK**.

The report is downloaded in the specified format to the target location.

You must have the appropriate viewer to view the downloaded report. For example, Adobe Reader is required to view PDF reports.

Related concepts

- [About Generated Reports](#)

Related references

- [Download Report Dialog](#)

Related tasks

- [Generate a Report](#)

Delete a Report

You can delete any generated report. Deleting a report removes it from the Pillar Axiom system.

Only reports listed on the Generated Reports page can be deleted.

Delete a report to make room for additional reports, or to remove older reports that are no longer valid.

- 1 From the **Monitor** tab, click **Reporting > Generated Reports**.
- 2 Select the name of the report you want to delete in the Generated Reports page.
- 3 Choose **Delete Report** from the Actions menu.

4 Click **OK**.

About Scheduled Reports

You can schedule a report to be generated at a time and frequency that you specify.

You can use reporting schedules to generate different types of reports whenever you need them. The Pillar Axiom system generates these scheduled reports at the desired time and lists them on the Generated Reports page for you to download in the format of your choice.

All schedules for generating reports are listed on the Reporting Schedules page. You can create new reporting schedules, or view, modify, or delete existing schedules, from the Reporting Schedules page.

You can create a reporting schedule and enable it to start generating reports immediately at the specified start time. Or, if you prefer, you can store the schedule on the Reporting Schedules page and enable it later. You can also disable a schedule temporarily (if, for example, you want to keep it from interfering with scheduled maintenance) and then enable it again. Deleting a schedule removes it from the system, but disabling a schedule leaves it available for enabling later on.

Scheduled reports will continue to be generated until you disable or delete the reporting schedule.

Related references

- [Reporting Schedules Overview Page](#)

Related tasks

- [Create a Reporting Schedule](#)
- [Modify a Reporting Schedule](#)
- [View a Reporting Schedule](#)
- [Delete a Reporting Schedule](#)

Create a Reporting Schedule

You can schedule a report to be generated at a time and frequency that you specify.

To generate a particular report on a regular basis, create a schedule for generating that report on the Reporting Schedules page.

- 1 From the **Monitor** tab, click **Reporting > Reporting Schedules**.
- 2 Choose **Actions > Create Reporting Schedule**.
- 3 Enter a name for your schedule in the **Schedule Name** field.

If you do not provide a name, the system uses the default name `untitled`.

Tip: Use a meaningful name that includes the type of report and frequency to help you identify the schedule in case you need to modify it later.

- 4 Select the type of report you want to generate from the **Report Type** menu.

Choose one of:

- SAN Hosts
- Storage Performance
- Storage Use
- Storage Use per Volume
- System Configuration
- System Configuration Summary

- 5 (Optional) Select **Enabled** if you would like your schedule to start as soon as it is created.

If you do not enable your schedule now, you can do so at a later time by modifying the schedule.

- 6 Click the expansion button to the right of **Start Time** to select the day and time for your schedule to start.

- 7 Use the controls in the **Modify Date/Time** dialog to select the date and time.

- 8 Choose a frequency for your schedule:

- Run Once
- Hourly
- Daily
- Weekly

- 9 Choose a recurrence value for your schedule.

If the schedule frequency is **Weekly**, specify if you want to generate the report every one, two, three, or four weeks, and on which day of the week to generate the report. Select multiple days if you want to generate the report on more than one day during each week.

- 10 Click **OK**.

Your schedule is listed on the Reporting Schedules page and, if you enabled the schedule, the scheduled report is listed on the Generated Reports page when it is generated.

Related concepts

- [About Scheduled Reports](#)

Related references

- [Create Reporting Schedule Dialog](#)

Related tasks

- [Modify a Reporting Schedule](#)

View a Reporting Schedule

View a reporting schedule to see the name, report type, enabled status, start time, frequency, and recurrence of the reporting schedule.

View reporting schedules from the Reporting Schedules page.

- 1 From the **Monitor** tab, click **Reporting > Reporting Schedules**.
- 2 Select the name of the reporting schedule you want to view on the Reporting Schedules page.
- 3 Choose **Actions > View Schedule**.

The View Reporting Schedule dialog lists the parameters of the selected schedule.

Modify a Reporting Schedule

Modify a reporting schedule to change the name, report type, enabled status, start time, frequency, or recurrence of the reporting schedule.

- 1 From the **Monitor** tab, click **Reporting > Generated Reports**.
- 2 Choose **Actions > Modify Schedule**.
- 3 Enter a new name for the reporting schedule, if desired, in the **Schedule Name** field.
- 4 Select a new type of report to generate, if desired, from the **Report Types** menu.
- 5 Click the expansion button to the right of **Start Time** to select a new start date and time, if desired.
- 6 Select a new frequency, if desired.

- 7 Select a new **Recurrence** value, if desired.

If the schedule frequency is **Weekly**, specify if you want to generate the report every one, two, three, or four weeks, and on which day of the week to generate the report. Select multiple days if you want to generate the report on more than one day during each week.

- 8 Click **OK** to save your modifications.

Your modified schedule is listed on the Reporting Schedules page and, if you enabled the schedule, the scheduled report is listed on the Generated Reports page when it is generated.

Related references

- [Modify Reporting Schedule Dialog](#)

Delete a Reporting Schedule

Delete a reporting schedule when you no longer need to generate a report of this type on a regular basis.

- 1 From the **Monitor** tab, click **Reporting > Reporting Schedules**.
- 2 Select the name of the reporting schedule you want to delete on the Reporting Schedules page.
- 3 Choose **Actions > Delete Schedule**.
- 4 Click **OK** in the Confirm Delete Reporting Schedule dialog.

This removes the schedule name from the Reporting Schedules page, and no further reports will be generated from this schedule. Reports that have already been generated from this schedule will remain on the Generated Reports page until you delete them.

CHAPTER 13

Manage Statistics Trending

About LUN Statistics and Trending

The Pillar Axiom system collects statistics that can keep you informed about the storage network status and performance of the LUNs on your system.

LUN statistics can be displayed for reference in a static table, or they can be displayed dynamically in a graphical trending chart. The chart represents information about the LUN during I/O activity. A system restart might reset this information to zero, which will affect the results of your chart.

Statistics are arranged by LUN name in the LUN statistics table. The following statistics collected over the specified collection period are included in the table:

- Capacity
- Priority level
- Average I/O
- Average throughput
- Average I/O latency
- Average I/O size

To view the interplay of LUN statistics in a graphical format, display them in a trending chart. Build your own trending chart by selecting specific LUNs associated with specific Slammers, and select from a range of statistics to include in the chart. Customize the chart by specifying threshold lines to display, and use data filters to restrict the age of the data used in the chart. The following types of statistics are available to use in a LUN statistics trending chart:

- Allocated capacity
- Read and write data
- Optimized data access
- Non-optimized data access
- Read and Write bandwidth

- Read and Write throughput
- Average I/O operation size
- Average I/O response time
- Repository allocated capacity

About LUN Statistics

LUN statistics provide an overview of all LUNs present on your Pillar Axiom system.

You can review the status of the following for each LUN:

Name	Identifies the name that is assigned to a LUN for administrative purposes.
Physical Allotted Capacity	Identifies the maximum capacity limit, in gigabytes (GB), that is assigned to the object.
Priority Level	Identifies the priority level assigned to the specified LUN. Valid levels: <ul style="list-style-type: none">○ Archive○ Low○ Medium○ High○ Premium
Average IOPs	Identifies the current performance for input (read) and output (write) operations for the LUN.
Average Throughput	Identifies the data transfer rate for inputs (reads) and outputs (writes) of the specified LUN.
Average I/O Latency	Identifies the average time to complete the read or write operations.
Average I/O Size	Identifies the average size of the read and write operations.

Collection Period Identifies the start and end time at which information was last collected from the Pillar Axiom system.

You can use this information to monitor the LUNs in your Pillar Axiom system or to compare LUN performance and capacity for planning improvements to your system.

Related references

- [LUN Statistics and Trending Overview Page](#)

Related tasks

- [View LUN Statistics](#)

View LUN Statistics

You can view statistical information about all LUNs configured on the Pillar Axiom system on the LUN Statistics and Trending Overview page.

- 1 From the **Monitor** tab, click **Statistics and Trending > SAN > LUNs**.

Result:

All LUNs are listed in the LUN Statistics and Trending table.

- 2 Click a column heading to sort the list by the contents of that column.
- 3 Select a LUN from the list.
- 4 To view detailed information about the selected LUN, choose **Actions > View Details**.

Related concepts

- [About LUN Statistics](#)

Related references

- [LUN Statistics and Trending Overview Page](#)
- [View Details Dialog \(LUNs\)](#)

About LUN Statistics Trending Charts

You can create charts of statistics collected from the LUNs in your Pillar Axiom system to show trends in the statistics.

Statistics collected from LUNs that can be used to produce trending charts include:

- The number and rates of data access commands handled over non-optimized paths.
- The number and rates of data access commands handled over optimized paths.
- Allocated capacity.

From the LUN Statistics and Trending Overview Page, you can view a default trending chart , or you can configure your own trending chart.

- To view a default trending chart, select one of the LUNs listed on the LUN Statistics and Trending Overview page, and choose LUN Statistics Trending from the Actions menu. A default trending chart appears in the LUN Statistics Trending dialog, showing data from the selected LUN using a configuration of all available Slammer control units (CUs) and a pre-defined selection of statistics.
- To configure your own trending chart, choose LUN Statistics Trending from the Actions menu without selecting a LUN. The Configure Trending Chart dialog appears, and you will need to select at minimum one or more LUNs, one or more Slammer CUs, and one or more statistics to include in the trending chart, and then click OK to display the trending chart in the LUN Statistics Trending dialog.

Default trending charts provide a quick overview of the most commonly referred to characteristics of the selected LUN over the last few hours. To add more LUNs, or to look at different characteristics of the LUN, you can modify the default configuration of the trending chart.

Configuring your own trending chart gives you the ability to specify only those LUNs, Slammer CUs, and statistics in which you are interested. In addition, you can add threshold lines to your chart and filter the data by specifying time constraints.

A chart threshold line establishes a visual benchmark against which you can compare other charted values. Having a named chart threshold line on the chart makes it easy to see when the lines representing other charted values exceed or drop below the threshold value. Threshold lines can be color coded to distinguish them from each other, and from the trending lines in the chart. Available colors are:

- Black
- Blue
- Cyan
- Green

- Magenta
- Orange
- Pink
- Red
- White
- Yellow

Filtering data by time enables you to exclude data collected before or after a specified point in time. You can also restrict the data in your chart to a narrow range of time by excluding data collected both before a certain time and after a certain time.

You can use LUN trending charts to discover ways to adjust LUN settings on your system to achieve the best performance.

To save the content of a trending chart, you can print a snapshot of a trending chart or export the data displayed in the chart to your local workstation as a comma-separated value (CSV) or XML file.

For example, if one Microsoft Exchange LUN is configured with the Microsoft Exchange Database storage profile and another similar LUN is configured with a General Purpose storage profile, you can configure a trending chart to compare the two to see which one provides the best performance for your system. To capture the data displayed in this chart to include in your status report, you can print a snapshot of the trending chart and export the data displayed in the snapshot to a CSV file that you import into your favorite program to format as a spreadsheet.

For example, to create a default trending chart for a LUN named SLUN1 that appears in the LUN Statistics and Trending list, select the SLUN1 row in the list and choose **LUN Statistics Trending** from the Action menu. A trending chart showing the following default statistics appears in the LUN Statistics Trending dialog.

- Volume Allocated Capacity in GB: Capacity (GB)
- Megabytes Written: (Cumulative)
- Megabytes Read: (Cumulative)
- Megabytes Read: MB/s
- Megabytes Written: MB/s

Related references

- [LUN Statistics and Trending Overview Page](#)
- [LUN Statistics Trending Dialog](#)
- [Configure Trending Chart, Trend Configuration Tab \(LUNs\)](#)

Related tasks

- [Configure a LUN Statistics Trending Chart](#)
- [Export a Trending Chart](#)
- [Print a Trending Chart](#)

Configure a LUN Statistics Trending Chart

LUN trending charts provide a graphical view of the statistics available for the LUNs on your Pillar Axiom system.

To display a LUN statistics trending chart, you need to add a minimum of one or more LUNs, one or more Slammer control units (CUs), and one or more statistics to the trending chart configuration.

One or more LUNs must be present on your Pillar Axiom system to create a LUN statistics trending chart.

Your configured trending chart will appear in the LUN Statistics Trending dialog.

- 1 From the **Monitor** tab, click **Statistics and Trending > SAN > LUNs**.
- 2 Choose **Actions > LUN Statistics Trending**.
- 3 Click **Add** below each list to include specific items from each category in the trending chart.
 - **LUNs to Trend:** Follow the instructions in the dialog to add LUNs to the list.
Tip: You can add as many LUNs as you want, but it may be difficult to distinguish between a large number of LUNs in the trending chart.
 - **Slammer Control Unit Data to Trend:** Select one or more Slammer CUs from the drop-down menu to add to the list.
Tip: The default is **<aggregate across all CUs>**. Remove this item from the list if you want to add specific Slammer CUs from the drop-down menu.
 - **Statistics to Trend:** Select one or more statistics from the drop-down menu to add to the list.

Tip: Default statistics do not appear in the drop-down menu. To add specific statistics, clear the list of all default statistics first, and then add the statistics you want from the drop-down menu.

- 4 To remove a specific item from the list, select the item and click **Remove**. Click **Clear** to remove all items from the list.
- 5 (Optional) Click the **Chart Thresholds** tab to add a chart threshold line to the chart.
- 6 (Optional) Click the **Data Filtering** tab to add a time filter to the data used in the chart.

Select one or both filters to specify a time range.

Choose from:

- **Filter out statistics older than:** Excludes all statistics collected before the specified date from the trending chart.
- **Filter out statistics more recent than:** Excludes all statistics collected after the specified date from the trending chart.

- 7 Click **OK**.

A trending chart displaying the data specified in the Configure Trending Chart dialog appears in the LUN Statistics Trending dialog.

Related concepts

- [About LUN Statistics Trending Charts](#)

Related references

- [Configure Trending Chart, Trend Configuration Tab \(LUNs\)](#)
- [Configure Trending Chart, Chart Thresholds Tab \(LUNs\)](#)
- [Configure Trending Chart, Data Filtering Tab \(LUNs\)](#)
- [Create Chart Threshold Dialog \(LUNs\)](#)

Related tasks

- [Create a Chart Threshold](#)

About SAN Slammer Statistics and Trending

The Pillar Axiom system collects statistics that can keep you informed about the storage network status and performance of the Slammers on your system.

SAN Slammer statistics and details can be displayed for reference in static tables, or they can be displayed dynamically in a graphical trending chart. The chart represents information about the Slammer during I/O activity. A system restart might reset this information to zero, which will affect the results of your chart.

Statistics are arranged by Slammer name in the SAN Slammer Protocol Statistics table. The following statistics collected over the collection period are available for each Slammer:

- Negotiated link speed
- Average throughput
- Average I/O latency and size
- Commands received
- Channel errors

Detailed statistics for each Slammer protocol (FC or iSCSI) can be displayed for the Slammers listed in the table. These detailed statistics include:

- SCSI task management
- FC loop activity and channel errors
- iSCSI port requests, events, and errors
- Performance information
- I/O latency

To view the interplay of SAN Slammer statistics in a graphical format, display them in a trending chart. Build your own trending chart by selecting specific Slammer ports and control units, and select from a range of protocol-specific statistics to include in the chart. Customize the chart by specifying threshold lines to display, and use data filters to restrict the age of the data used in the chart. The following types of statistics are available to use in a Slammer statistics trending chart:

- FC-specific commands and tasks
- iSCSI-specific commands and tasks

- Read and write data

About SAN Slammer Statistics

SAN Slammer protocol statistics provide an overview of the Slammer ports on your Pillar Axiom system.

You can review the status of the following:

Network interface	Identifies the physical port on the CU.
Port type	Identifies the Slammer port connection type, Fibre Channel (FC) or Internet Small Computer System Interface (iSCSI).
Negotiated link speed	Displays the transmission speed in gigabits/second for the port.
Average throughput	Displays the average throughput in MB/second. <ul style="list-style-type: none">○ Read: The average read throughput in MB/second.○ Write: The average write throughput in MB/second.
Commands received	Displays the number of read and write commands received each second over the last sampling period.
Channel errors	Displays the cumulative number of errors that have occurred on the channel since the Slammer control unit was started.

You can view more detailed information about Slammers by viewing details for a selected Slammer. Detailed information is available for Fibre Channel (FC) or iSCSI Slammers, depending on the type of Slammer selected.

You can use this statistical information to monitor the Slammers in your Pillar Axiom system, or to compare Slammer characteristics for planning improvements to your system.

Related references

- [Slammers Overview Page](#)
- [View Details Dialog \(FC Slammers\)](#)
- [View Details Dialog \(iSCSI Slammers\)](#)

Related tasks

- [View SAN Slammer Statistics](#)

View SAN Slammer Statistics

You can view statistical information about all Slammers configured on the Pillar Axiom system at the SAN Slammer Protocol Statistics and Trending Overview page.

- 1 From the **Monitor** tab, click **Statistics and Trending > SAN > Slammer Protocols**.
Result:
All Slammers are listed in the SAN Slammer Protocol Statistics and Trending table.
- 2 Click a column heading to sort the list by the contents of that column.
- 3 Select a Slammer from the list.
- 4 To view detailed information about the selected Slammer, choose **Actions > View Details**.

Related concepts

- [About SAN Slammer Statistics](#)

Related references

- [SAN Slammer Protocol Statistics and Trending Overview Page](#)
- [View Details Dialog \(FC Slammers\)](#)
- [View Details Dialog \(iSCSI Slammers\)](#)

About SAN Slammer Statistics Trending Charts

You can create charts of statistics collected from the Slammer ports in your Pillar Axiom system to show trends in the data.

Statistics collected from Slammer ports that can be used to produce trending charts include:

- The total amounts and rates of data read and written through a specified Slammer port.

- Statistics specific to the Fibre Channel (FC) or iSCSI protocol.

From the SAN Protocol Statistics and Trending Overview page, you can choose **Slammer Statistics Trending** from the Actions menu to configure a trending chart from scratch, or you can select a Slammer port before you choose **Slammer Statistics Trending**.

- When you select a Slammer port before you choose **Slammer Statistics Trending**, that Slammer port is automatically listed in the Ports to Trend list in the Configure Trending Chart dialog.
- When you choose **Slammer Statistics Trending** without previously selecting a Slammer port, no ports will be listed in the Ports to Trend list in the Configure Trending Chart dialog, so you will need to add ports to the list by clicking the **Add** button.

Configuring a trending chart gives you the ability to specify only those Slammer ports, Slammer CUs, and statistics in which you are interested. In addition, you can add threshold lines to your chart and filter the data by specifying time constraints.

A chart threshold line establishes a visual benchmark against which you can compare other charted values. Having a named chart threshold line on the chart makes it easy to see when the lines representing other charted values exceed or drop below the threshold value. Threshold lines can be color coded to distinguish them from each other, and from the trending lines in the chart. Available colors are:

- Black
- Blue
- Cyan
- Green
- Magenta
- Orange
- Pink
- Red
- White
- Yellow

Filtering data by time enables you to exclude data collected before or after a specified point in time. You can also restrict the data in your chart to a narrow

range of time by excluding data collected both before a certain time and after a certain time.

To save the content of a trending chart, you can print a snapshot of a trending chart or export the data displayed in the chart to your local workstation as a comma-separated value (CSV) or XML file.

You can use this performance trend information to discover ways to route LUN I/O through the Slammer ports that will achieve the best performance.

For example, if a LUN configured with the Microsoft Exchange Database storage profile is assigned to Port 1 on Slammer01 control unit (CU) 1, and a similarly configured LUN is assigned to Port 0 on Slammer01 CU1, you can configure a trending chart to compare the I/O performance of these two ports to determine which is optimal for this type of LUN. To capture the data displayed in this chart to include in your status report, you can print a snapshot of the trending chart and export the data displayed in the snapshot to a CSV file that you import into your favorite program to format as a spreadsheet.

Related references

- [SAN Slammer Protocol Statistics and Trending Overview Page](#)
- [Slammer Statistics Trending Dialog](#)
- [Configure Trending Chart, Trend Configuration Tab \(Slammers\)](#)

Related tasks

- [Configure a SAN Slammer Statistics Trending Chart](#)
- [Export a Trending Chart](#)
- [Print a Trending Chart](#)

Configure a SAN Slammer Statistics Trending Chart

Slammer trending charts provide a graphical view of the statistics available for the Slammers on your Pillar Axiom system.

To display a Slammer statistics trending chart, you need to add a minimum of one or more Slammer ports, one or more Slammer control units (CUs), and one or more statistics to the trending chart configuration.

Your configured trending chart will appear in the Slammer Statistics Trending dialog.

- 1 From the **Monitor** tab, click **Statistics and Trending > SAN > Slammer Protocols**.
- 2 Choose **Actions > Slammer Statistics Trending**.
- 3 Click **Add** below each list to include specific items from each category in the trending chart.

- **Ports to Trend:** Select ports from the drop-down menu to add to the list.

Tip: Ports that are already displayed in the trend list are not listed in the drop-down menu.

- **Slammer Control Unit Data to Trend:** Select one or more Slammer CUs from the drop-down menu to add to the list.

Tip: The default is **<aggregate across all CUs>**. Remove this item from the list if you want to add specific Slammer CUs from the drop-down menu.

- **Statistics to Trend:** Select one or more statistics from the drop-down menu to add to the list.

Tip: Default statistics do not appear in the drop-down menu. To add specific statistics, clear the list of all default statistics first, and then add the statistics you want from the drop-down menu.

- 4 (Optional) Click the **Chart Thresholds** tab to add a chart threshold line to the chart.
- 5 (Optional) Click the **Data Filtering** tab to add a time filter to the data used in the chart.

Select one or both filters to specify a time range.

Choose from:

- **Filter out statistics older than:** Excludes all statistics collected before the specified date from the trending chart.
- **Filter out statistics more recent than:** Excludes all statistics collected after the specified date from the trending chart.

- 6 Click **OK**.

A trending chart displaying the data specified in the Configure Trending Chart dialog appears in the Slammer Statistics Trending dialog.

Related concepts

- [About SAN Slammer Statistics Trending Charts](#)

Related references

- [Configure Trending Chart, Trend Configuration Tab \(Slammers\)](#)
- [Configure Trending Chart, Chart Thresholds Tab \(Slammers\)](#)
- [Configure Trending Chart, Data Filtering Tab \(Slammers\)](#)
- [Create Chart Threshold Dialog \(Slammers\)](#)

Related tasks

- [Create a Chart Threshold](#)

Create a Chart Threshold

A chart threshold is a labeled horizontal line that you can add to your trending chart to serve as a visual benchmark for comparing the values of the trending lines that appear in the chart.

Create a chart threshold in the Chart Threshold tab of the Configure Trending Chart dialog.

- 1 From the **Monitor** tab, click the desired menu path. Valid paths:
 - **Statistics and Trending > SAN > LUNs**
 - **Statistics and Trending > SAN > Slammer Protocols**
- 2 Choose the desired menu action. Valid actions:
 - **Actions > LUN Statistics Trending**
 - **Actions > Slammer Statistics Trending**
- 3 In the Configure Trending Chart dialog, click the **Chart Threshold** tab.
- 4 To open the Create Chart Threshold dialog, click **Add**.
- 5 Enter a name in the **Name** field.

You must provide a name to identify the chart threshold. This name appears as a label for the chart threshold line on the trending chart.
- 6 From the **Statistic Metric Type** menu, choose a type of statistical metric for the threshold.

The Statistic Metric Type appears under the **Scale** heading in the Chart Thresholds list, and it corresponds to one of the scale rulers that appear on the left and right of the trending chart.
- 7 Enter a numeric **Value** for the threshold.

This value determines the level at which the chart threshold line appears in the chart, which corresponds to the level at which the value appears in the corresponding scale ruler.
- 8 From the **Color** menu, choose a color for the chart threshold line and label.

Tip: If possible, choose a color that will distinguish the threshold line from the other trending lines in the chart.
- 9 From the **Rendering Mode** menu, choose a method for displaying the chart threshold.

10 Click **OK**.

Result:

The chart threshold is listed in the Chart Threshold tab of the Configure Trending Chart dialog, and it appears in each trending chart created during this session until it is deleted.

Related concepts

- [*About LUN Statistics Trending Charts*](#)
- [*About SAN Slammer Statistics Trending Charts*](#)

Related references

- [*Create Chart Threshold Dialog \(LUNs\)*](#)
- [*Create Chart Threshold Dialog \(Slammers\)*](#)

Export a Trending Chart

Exported trending charts provide a report of the statistics shown at one point in time in the chart.

You must have previously created a trending chart and displayed it in the LUN or Slammer Statistics Trending dialog before you can export the trending chart.

Because trending charts cannot be saved, exporting a trending chart enables you to record the statistics displayed in the chart in a textual format for later use.

- 1 From the **Monitor** tab, click the desired menu path. Valid paths:
 - **Statistics and Trending > SAN > LUNs**
 - **Statistics and Trending > SAN > Slammer Protocols**
- 2 Choose the desired menu action. Valid actions:
 - **Actions > LUN Statistic Trending**
 - **Actions > Slammer Statistics Trending**
- 3 Create a trending chart.
- 4 Click **Export** in the LUN or Slammer Statistics Trending dialog.
- 5 From the **Format** menu, choose a format for your report. Valid formats:
 - **CSV**
 - **XML**
- 6 Click the expansion button to the right of the **Export to** field and navigate to a location on your local workstation where you want to store the report.
- 7 Enter a filename for the report.
- 8 Click **OK**.

Related concepts

- [About LUN Statistics Trending Charts](#)
- [About SAN Slammer Statistics Trending Charts](#)

Related references

- [Export Dialog](#)

Related tasks

- [Configure a LUN Statistics Trending Chart](#)
- [Configure a SAN Slammer Statistics Trending Chart](#)

Print a Trending Chart

Printed trending charts provide a graphical snapshot of the trends shown at one point in time in the chart.

You must have previously created a trending chart and displayed it in the LUN or Slammer Statistics Trending dialog before you can print the trending chart.

Because trending charts cannot be saved, printing a trending chart enables you to record the trends displayed in the chart for later use.

- 1 Right-click in the LUN or Slammer Statistics Trending dialog.
- 2 Select **Print** from the context menu.

The system sends a print image of the displayed trending chart to the default printer on your workstation.

CHAPTER 14

Managing Multiple Pillar Axiom Systems

About Pillar Axiom MaxMan

Pillar Axiom MaxMan allows you to manage multiple Pillar Axiom 600 systems from a single client application. The Pillar Axiom MaxMan client provides a convenient way to monitor the health of multiple Pillar Axiom systems or manage a specific system.

The Pillar Axiom MaxMan application saves the list of monitored Pillar Axiom 600 systems in a configuration file. The configuration file contains the system name and IP address for each managed system. You can add or remove managed systems as necessary, which allow you to view a collection of Pillar Axiom systems as a logical group.

For each managed Pillar Axiom system, Pillar Axiom MaxMan displays:

- Health status of the following components:
 - Pillar Axiom 600 systems
 - Pilots
 - Slammers
 - Bricks
 - Uninterruptible power supplies (UPSs)
- System alerts and event notifications
- Performance statistics for LUNs and Slammers
- Storage capacity usage
- Scheduled tasks and generated reports
- Overview of LUNs and SAN hosts
- System software configuration
- Administrator accounts information

To manage a selected system, use the **Manage Axiom System** option from the Actions menu.

Related concepts

- [*About Managing Configuration Files*](#)

Related references

- [*Axioms Overview Page*](#)

Related tasks

- [*Create a Configuration File*](#)

Run the Pillar Axiom MaxMan GUI Application

The files needed to run the Pillar Axiom MaxMan software were installed when you installed the Pillar Axiom Storage Services Manager.

- 1 Locate the extracted or installed file on the client workstation.
- 2 Launch the Pillar Axiom MaxMan application.

Depending on your operating system, perform one of the following actions:

- Windows Explorer: Double-click the file `C:\Program Files\Oracle Corporation\Pillar Axiom MaxMan.exe`.
- Windows command line: Run the batch script `runPillarAxiomMaxMan.bat`.
- Linux: Run the shell script `runPillarAxiomMaxMan.sh`.

Result:

The Pillar Axiom MaxMan GUI opens to the Axioms overview page, or the last page you visited when you last logged off.

Related concepts

- [About Pillar Axiom MaxMan](#)
- [About Client Application Download Formats](#)
- [About Accessing Pillar Axiom 600 Applications](#)

Related tasks

- [Install the GUI Application with Windows Installer](#)
- [Install the GUI Application Archive File](#)

Add Systems to the Monitored List

A monitored list is a list of one or more Pillar Axiom systems that are managed by the Pillar Axiom MaxMan. A monitored list is necessary for the system to manage the Pillar Axiom systems. You can save the list properties in a configuration file.

There is no limit to the number of Pillar Axiom systems that the Pillar Axiom MaxMan system can manage.

- 1 Choose **Axiom > Manage Axiom List**.
- 2 From the Manage the List of Axiom Systems dialog, select a Pillar Axiom system to add in the **Axiom** field:
 - Select a Pillar Axiom system from the drop-down list
 - Enter the name of the Pillar Axiom system

Tip: After you manually enter the name of the Pillar Axiom system, the name is included in the drop-down list for selection at a later time.

- 3 To add the Pillar Axiom system to the list, click **Add**.
- 4 Continue adding Pillar Axiom systems if desired.
- 5 When you have finished adding your systems, click **OK**.

Result:

After you click **OK**, the GUI prompts you for the login credentials. The Configuring List of Axioms dialog appears to inform you of the login progress. After the Pillar Axiom MaxMan system successfully logs in, you should see the system in the Pillar Axiom overview page.

- 6 To save your changes, choose **Axiom > Save**.

Related concepts

- [About Managing Configuration Files](#)

Related references

- [Manage the List of Axiom Systems Dialog](#)

Related tasks

- [Create a Configuration File](#)

Remove Systems From the Monitored List

You can remove Pillar Axiom system from a monitored list of systems connected to the Pillar Axiom MaxMan. For example, you may need to remove a system while it is offline for maintenance.

- 1 Choose **Axiom > Add / Remove Axioms**.
- 2 From the Add / Remove Axioms dialog, select the Pillar Axiom system from the list.
- 3 Click **Remove** to remove the system from the list.
- 4 Click **OK**.

After clicking **OK**, the Pillar Axiom MaxMan system removes the Pillar Axiom system from the list. If you are logged into the Pillar Axiom system you removed from the list, you will be prompted to log off.

Related concepts

- [About Managing Configuration Files](#)

Related tasks

- [Add Systems to the Monitored List](#)
- [Create a Configuration File](#)

Manage a Specific Pillar Axiom System

You can manage a Pillar Axiom system that is monitored by Pillar Axiom MaxMan. If you have several systems to manage Pillar Axiom MaxMan provides a single interface from which to launch the graphical user interface (GUI) for each Pillar Axiom system.

- 1 From the Pillar Axiom MaxMan, select a Pillar Axiom system to manage.
- 2 Select the Pillar Axiom system object that you want to manage, such as a LUN.
- 3 Choose **Actions > Manage Axiom System**.

Tip: The system displays the same Pillar Axiom interface location from which you launched the Pillar Axiom MaxMan.

Example:

If you want to manage LUNs for a specific Pillar Axiom system, select the system and the LUN from the Pillar Axiom MaxMan and choose **Manage Axiom System** from the **Actions** menu.

Related concepts

- [About Pillar Axiom MaxMan](#)

Related tasks

- [Add Systems to the Monitored List](#)

About Managing Configuration Files

The Pillar Axiom MaxMan allows you to save a list of managed Pillar Axiom systems in a configuration file.

The configuration file contains the system name and IP address for each managed system. The file is stored locally on the client computer from which the application is launched. User names and passwords for managed systems are not stored in the configuration file.

You create a configuration file by adding one or more Pillar Axiom systems that you want to manage and saving the file. When you open the file from the Pillar Axiom MaxMan, the system prompts you for the login credentials and logs into each of the managed Pillar Axiom systems. Although the configuration file is an XML document with a pdsmac extension, editing the file manually is not recommended.

Related concepts

- [About Pillar Axiom MaxMan](#)

Related tasks

- [Create a Configuration File](#)
- [Add Systems to the Monitored List](#)
- [Modify a Configuration File](#)
- [Open a Configuration File](#)
- [Remove Systems From the Monitored List](#)

Create a Configuration File

A Pillar Axiom configuration file saves you time by letting you launch the Pillar Axiom MaxMan pre-configured with the collection of Pillar Axiom systems that you want to manage.

Creating a new configuration file of Pillar Axiom systems requires that you log off all currently managed systems. If you want to save the current list of Pillar Axiom systems in a configuration file, skip to Step 4.

- 1 To start a new configuration file, choose **Axiom > New**.
- 2 From the New confirmation dialog, select **OK**.
- 3 Follow the instructions for adding Pillar Axiom systems in **Add Systems to the Monitored List**.

- 4 To save the list of managed Pillar Axiom systems in a configuration file, choose **Axiom > Save**.
- 5 Enter the name for the configuration file, then click **OK**.

Result:

After you click **OK**, the GUI prompts you for the login credentials. The Configuring List of Axioms dialog appears to inform you of the login progress. After the Pillar Axiom MaxMan system successfully logs in, you should see the system in the Pillar Axiom overview page.

Related concepts

- [About Managing Configuration Files](#)

Related tasks

- [Add Systems to the Monitored List](#)
- [Remove Systems From the Monitored List](#)

Open a Configuration File

You can open a configuration file that contains a list of managed Pillar Axiom systems monitored by the Pillar Axiom MaxMan. For example, if a new Pillar Axiom system is available you can add the system to configuration file.

Tip: If you are using a Windows® operating system to manage the Pillar Axiom system you can load the managed Pillar Axiom systems by double-clicking the configuration file.

- 1 Choose **Axiom > Open**.
- 2 From the Open dialog, enter the name of the configuration file or click the browse button [...] to select the configuration file.
- 3 Click **OK**.

Result:

After you click **OK**, the GUI prompts you for the login credentials. The Configuring List of Axioms dialog appears to inform you of the login progress. After the Pillar Axiom MaxMan system successfully logs in, you should see the system in the Pillar Axiom overview page.

Related concepts

- [About Managing Configuration Files](#)

Related tasks

- [Create a Configuration File](#)
- [Add Systems to the Monitored List](#)

Modify a Configuration File

You can revise the list of managed Pillar Axiom systems in a configuration file. For example, you may need to remove a Pillar Axiom system from the list when that system has been taken offline for maintenance.

- 1 Open the configuration file as described in [Open a Configuration File](#).
- 2 Enter the login credentials to load the managed Pillar Axiom systems.
- 3 Choose **Axiom > Add/Remove Axioms**.
- 4 From the Add / Remove Axioms dialog, add or remove Pillar Axiom systems as desired.
- 5 When you have finished updating your list of managed Pillar Axiom systems, click **OK**.

Result:

After you click **OK**, the GUI prompts you for the login credentials. The Configuring List of Axioms dialog appears to inform you of the login progress. After the Pillar Axiom MaxMan system successfully logs in, you should see the system in the Pillar Axiom overview page.

- 6 To save your changes, choose **Axiom > Save**.

Related concepts

- [About Managing Configuration Files](#)

Related tasks

- [Add Systems to the Monitored List](#)
- [Remove Systems From the Monitored List](#)

APPENDIX A

GUI Field Definitions

Pillar Axiom System Limits

Note: A Pillar Axiom system uses binary units to calculate and display the capacity of physical storage and the size of logical volumes:

1 MB = 1024^2 (1,048,576) bytes

1 GB = 1024^3 (1,073,741,824) bytes

1 TB = 1024^4 (1,099,511,627,776) bytes

Table 24 System operating limits

Parameter	Limits
Volume groups	<p>Minimum: 1 Maximum: 5000</p> <p>Note: A volume group can contain up to 100 nested groups. Nesting is limited to five levels. Also, the root volume (/Volumes) is always available.</p>
SAN LUNs	<p>Maximum:</p> <ul style="list-style-type: none">• 8191 visible for any given SAN Slammer• 8191 visible across all SAN Slammers in a given system (2730 if all LUNs have non-zero clone repositories)• 255 visible for each host <p>Note: A visible (active) LUN requires one virtual LUN (VLUN). Clones for that LUN require a VLUN for the data repository. Each active clone of the source LUN also requires a separate VLUN. For example, a LUN that has two clones requires four VLUNs.</p>
SAN LUN size	<p>Minimum: 1 to 2 GB. The exact value depends on these factors</p>

Table 24 System operating limits (continued)

Parameter	Limits
	<ul style="list-style-type: none"> Brick type (Fibre Channel or SATA) RAID geometry (RAID 5 or Distributed RAID) Strip size (1 MB or normal) <p>Maximum: System capacity</p> <p>Note: All capacity values must be in increments of 1 GB.</p>
Pillar Axiom Path Manager (APM)	Maximum Pillar Axiom systems: 8 for each SAN host
APM data paths	Maximum: 32 to each LUN
APM FC HBA ports	Maximum: 32 for each SAN host
Clone LUNs	<p>Maximum:</p> <ul style="list-style-type: none"> Number of available LUNs 13 active at a time (for a single source)
iSCSI protocol	<p>Maximums for each iSCSI port:</p> <ul style="list-style-type: none"> 1 VLAN ID 256 TCP connections 256 iSCSI initiators 512 simultaneous commands <p>Maximum for each LUN: 32 persistent reservation registration keys</p>
Administrator accounts	<p>Minimum: 2</p> <p>Maximum: Unlimited</p> <p>Note: Minimum provides for the Primary system administrator and Pillar support administrator.</p>
Administrator sessions	Maximum: 25 simultaneous
Administrator login attempts	<p>Minimum: 1</p> <p>Maximum: Unlimited, unless set by the administrator</p>
Session time-out period (minutes)	<p>Minimum: 0</p> <p>Maximum: 999</p>

Table 24 System operating limits (continued)

Parameter	Limits
	Note: Default time-out period is 20 minutes.
Storage Domains	Maximum: 64 for each system
Number of Bricks in a Storage Domain	Minimum: <ul style="list-style-type: none"> Serial ATA (SATA) or solid state drives (SSD) Bricks: 1 Fibre Channel (FC) Bricks: 2 Maximum: <ul style="list-style-type: none"> SATA Bricks: 64 FC or SSD Bricks: 32

Table 25 Field input limits

Field	Length or Type	Notes
Names for: <ul style="list-style-type: none"> Alerts Brick storage enclosures Pillar Axiom system Schedules Slammer storage controllers Volume groups 	1 through 16 8-bit Unicode Transformation Format (UTF-8) printable characters. UTF-8 is described in RFC 2279, which you can find online with any Internet search engine.	Embedded spaces are permitted. Invalid characters: <ul style="list-style-type: none"> Non-printable characters, including ASCII 0 through 31 / (slash) and \ (backslash) . and .. (dot and dot-dot alone) Embedded tabs Pillar Axiom processing: <ul style="list-style-type: none"> Leading and trailing white space is stripped Comparison is case sensitive
Names for: <ul style="list-style-type: none"> LUNs Storage Domains 	1 through 82 UTF-8 printable characters	Invalid characters: <ul style="list-style-type: none"> Nonprintable characters, including ASCII 0 through 31 / (slash) and \ (backslash) . and .. (dot and dot-dot alone) Embedded tabs
Names for SAN hosts	1 through 63 UTF-8 printable characters	

Table 25 Field input limits (continued)

Field	Length or Type	Notes
DNS domains	0 through 255, in all four parts	IP version 4 (IPv4) dotted-decimal notation (nnn.nnn.nnn.nnn)
Administrator user name	1 through 16 UTF-8 printable characters	Case-sensitive value Invalid characters: <ul style="list-style-type: none"> • Embedded spaces • / (slash)
Administrator password	6 through 16 UTF-8 printable characters	<ul style="list-style-type: none"> • Case-sensitive value • Embedded spaces are permitted.
Optional entries for administrator full names	0 through 40 UTF-8 printable characters	Embedded spaces are permitted.
Optional entries for telephone numbers	0 through 80 UTF-8 printable characters	Embedded spaces are permitted.
Alert descriptions	0 through 80 UTF-8 printable characters	Embedded spaces are permitted.
Email address (emailuser@host)	1 through 64 characters for email user	a-z A-Z 0-9 ! # \$ % & ' * + - / = ? ^ _ ` { } ~ . are permitted, except that . (dot) cannot be the first or last character.
	1 through 255 characters for host	a-z A-Z 0-9 - . are permitted, except that: <ul style="list-style-type: none"> • 0-9 - . cannot be the first character. • . - cannot be the last character. An IP address cannot be the host part of the email address.
IP addresses	0 through 255, in all four parts	IP version 4 (IPv4) dotted-decimal notation (nnn.nnn.nnn.nnn)
Virtual LAN (VLAN) ID or tag	0 through 4094 (integer)	<ul style="list-style-type: none"> • 1 through 4094 denote that VLAN tagging is enabled. • 0 denotes that VLAN tagging is disabled.

Table 25 Field input limits (continued)

Field	Length or Type	Notes
SNMP community string	6 through 255 ASCII printable characters 33 through 126	Invalid characters: <ul style="list-style-type: none">• Embedded spaces• Control characters
Chap Secrets	100 UTF-8 characters	Non-character (for example, integer) CHAP secret values are not supported. CHAP secrets should be more than 12 bytes if IPsec is not used on insecure network segments.

APPENDIX B

Configure Tab Reference Pages

Administrator Accounts Overview Page

Navigation: Global Settings > Administrator Accounts

Displays the user name, ID or FQN, role, full name, email address, phone number, and whether each account is enabled. This page provides options to create, modify, delete, and view administrator accounts.

Up to 10 active administrator sessions can be defined. Of these 10 sessions, one is reserved for the Primary Administrator role and another one for the Administrator 1 role.

Login Name

Lists administrator login, or user names. Click a name to review or modify the administrator account.

Role

Identifies the role that is assigned to the administrator account. A role defines which permissions are granted to the administrator.

- Primary Administrator
- Administrator 1
- Administrator 2
- Monitor
- Support
- Pillar support

Disabled

Identifies whether the administrator account is disabled.

No

Indicates that the account is active. Administrators whose accounts are enabled can log in to the Pillar Axiom system.

Yes

Indicates that the account is inactive. Administrators whose accounts are disabled cannot log in.

Full Name

Identifies the first and last name associated with the administrator account.

Email Address

Identifies the email address of the recipient. The email server to which the Pillar Axiom system sends alerts must be able to receive messages at this address. The system does not validate this address.

Phone Number

Identifies the phone number associated with the administrator account. The Pillar Axiom system does not verify the validity of this entry.

Related references

- [*Pillar Axiom System Limits*](#)

Related tasks

- [*Create a Pillar Axiom Administrator Account*](#)
- [*Display Administrator Account Details*](#)
- [*Modify an Administrator Account*](#)
- [*Delete an Administrator Account*](#)

Associate Hosts Dialog

Navigation: Storage > SAN > Hosts > Actions > Associate Hosts

Enables the Pillar Axiom system to recognize Fibre Channel (FC) or iSCSI SAN hosts that do not have Pillar Axiom Path Manager (APM) installed.

Host Name

Identifies the SAN host that accesses LUNs or Clone LUNs configured on the Pillar Axiom system.

Create Association

Specifies the name of the host bus adapter (HBA) that is used for the SAN host association.

Valid options:

Specify WWN

Allows you to enter an HBA port world-wide name (WWN) that the Pillar Axiom system does not yet detect. Can also be used to specify that a host, which was created by Pillar Axiom Path Manager or by an administrator, is to be associated with a high level group such as a *host group*.

Select iSCSI device name

Allows you to enter an iSCSI device name that the Pillar Axiom system does not yet detect.

Select from discovered WWNs

Provides a list of HBA WWN ports on the Pillar Axiom system detects on the network.

Note: Because sometimes a McData switch may return an error for a valid command, the GUI may display a connection to a host port that is not connected.

Select from discovered iSCSI Names

Provides a list of iSCSI HBA ports that the Pillar Axiom system detects on the network.

Note: Because sometimes a McData switch may return an error for a valid command, the GUI may display a connection to a host port that is not connected.

Create

Creates an association between the specified storage area network (SAN) host and the WWNs of the HBA.

Modify

Changes the selected configuration settings of the object.

Remove

Deletes the selected objects.

Related concepts

- [About Host Groups](#)

Related references

- [Pillar Axiom System Limits](#)

Related tasks

- [Associate a SAN Host](#)
- [Modify a Host: Reconfigure Port Settings](#)

Create SAN Clone LUN, Quality of Service Tab

Navigation: Storage > SAN > LUNs > Actions > Clone LUN > Quality of Service

Allows you to create the capacity and performance settings for a LUN of any type (source, clone, or copy).

Repository Capacity for Source LUN

Displays the allocated and growth potential for the Clone LUN within the source LUN repository. The graph uses colored bars to indicate the capacity status of the logical volume you are creating.

- Solid Green: Indicates the allocated and used capacity for the volume.
- Shaded Green: Indicates the allocated and unused capacity for the volume.
- Dark Gray: Indicates the growth potential for the Clone LUN within the source LUN repository.

Storage Domain

Identifies the name of the storage domain associated with the LUN.

Volume Name

Identifies the name that is assigned to a LUN for administrative purposes. LUN names must be unique across the Pillar Axiom system and must be 82 or fewer UTF characters, or 255 or fewer ASCII characters.

Volume Group

Allows you to assign the LUN to an existing volume group.

[...] Opens the dialog that allows you to create new Volume Groups.

Storage Profile

Identifies the set of QoS attributes applied to the LUN.

[...] Opens the View Storage Profiles dialog that allows you to review the profile details.

Recommended Storage Class

Displays the recommended storage class based on the Storage Profile selection.

Storage Class

Identifies the category of physical media on which the logical volume resides: Valid types:

- SATA
- FC
- SSD SLC (solid state drive, single-level cell)

Typical Access

Identifies the most common method of data access. Valid options:

Sequential	Read and write requests from client applications tend to request operations on the data one record after the other.
Random	Read and write requests from client applications tend to request operations on the data records in an arbitrary order.
Mixed	Read and write requests from client applications tend to mix the request operations on the data sometimes in sequential and sometimes in random order.

I/O Bias

Identifies the typical read-write ratio. Valid options:

Read	Most requests from client applications are for <code>read</code> operations.
Write	Most requests from client applications are for <code>write</code> operations.
Mixed	Requests from client applications are likely equal for <code>read</code> and <code>write</code> operations.

Redundancy

Identifies how many mirror copies of the original data are stored in the storage pool. Valid options:

Standard	Stores original data only. Data striping over multiple RAID groups maintains full redundancy, even without mirror copies.
Double	Stores original data and one mirror copy, with data striping over multiple RAID groups.

Priority Level

In addition to determining the placement of data onto specific areas of the drive platters relative to the drive spindles, the priority level of a volume determines the processing *queue priority* for that volume. Queue priority defines the percentage of Slammer CPU cycles that are dedicated to the volume.

Valid options:

Premium	Highest processing queue priority. Striping occurs across eight serial ATA (SATA) RAID groups or four Fibre Channel (FC) RAID groups on the outermost 20% of the drive platters.
High	Next highest processing queue priority. Striping occurs across eight SATA RAID groups or four FC RAID groups on the outermost 20-40% of the drive platters.
Medium	Intermediate processing queue priority. Striping occurs across six SATA RAID groups or three FC RAID groups on the outermost 40-60% of the drive platters.
Low	Next to lowest processing queue priority. Striping occurs across four SATA RAID groups or two FC RAID groups on the outermost 60-80% of the drive platters.
Archive	Lowest processing queue priority. Striping occurs across four SATA RAID groups or two FC RAID groups on the outermost 80-100% of the drive platters.

Allocated Logical Capacity

Identifies the amount of capacity to be allocated to the logical volume.

Maximum Logical Capacity

Identifies the maximum capacity to which the logical volume can grow. For a clone, this field identifies how much addressable space will be available.

Background Copy Priority

Identifies the strategy the system should use to control the impact on performance when background tasks need to copy or move data from one location in the storage pool to another.

Note: When the system is idle or lightly loaded, the above background task maximizes the amount of work done regardless of the option selected.

Valid options:

System Chooses	Balances the background copy with the incoming client I/O. This option is the default.
-----------------------	--

Minimize Impact	Restricts the amount of work performed on a loaded system. This option is intended to have a minimal impact on client I/O throughput at the expense of longer copy times.
Maximum Speed	Prioritizes the background copy at the expense of client I/O throughput.

The following types of operations are affected by the strategy you select:

- Copy
- Restore
- Quality of Service (QoS) changes in:
 - Priority
 - Redundancy
 - Storage Class

Allocated Logical Capacity

Identifies the amount of capacity to be allocated to the logical volume.

Addressable Logical Capacity

Identifies the maximum capacity to which the logical volume can grow. For a clone, this field identifies how much addressable space will be available.

Related concepts

- [*About Creating LUNs*](#)
- [*About Copying and Cloning LUNs*](#)
- [*About Priority Levels*](#)
- [*About Redundancy*](#)
- [*About I/O Bias*](#)
- [*About Access Bias*](#)
- [*About Storage Classes*](#)

Related references

- [*Effects of Access Bias and I/O Bias*](#)

Create SAN Clone LUN, Mapping Tab

Navigation: Storage > SAN > LUNs > Actions > Clone LUN > Mapping

Allows you to create the LUN-to-host mapping settings for a Clone LUN.

Access Protocol

Valid options:

- Fibre Channel (FC): Specifies that hosts can use the FC protocol to access this LUN.
Tip: FC paths will always be used at a preference over iSCSI paths. Also, load balancing will not be mixed between these two protocols.
- iSCSI: Specifies that hosts can use the iSCSI protocol to access this LUN.

Only selected hosts (via maps)

Specifies that only designated SAN hosts can access this LUN using a specific, possibly different, LUN number on each of those hosts. If the LUN is mapped, the LUN number must be unique to the mapped SAN host.

All hosts may access this LUN using LUN Number

Specifies all SAN hosts accessing this LUN use the same LUN number. Select this option to activate the LUN number selection drop-down list.

Available LUN Number

You can map a LUN or Clone LUN to either a single host or a host group.

LUN Slammer Control Unit Assignment

Current Slammer CU

Identifies the current Slammer CU on which the LUN is currently homed.

Note: For new source LUNs, this field is not available; instead, use Assigned Slammer CU.

Assigned Slammer CU <Auto-Assign>

Identifies the Slammer CU to which the system should assign the LUN. Available options:

<auto assign>

Select this option if you want the system to determine the Slammer CU.

Slammer CU Select a specific Slammer CU from the list to assign to the LUN.

Ports Masked for this LUN

Displays the physical Slammer ports to exclude (mask) so they cannot access the LUN.

Masked

Indicates whether the port for the LUN is masked.

Protocol

Identifies the type of access protocol, FC or iSCSI.

Slammer

Identifies the name of the Slammer.

CU

Identifies the control unit (CU) of the Slammer.

Port

Identifies the name of the Slammer CU port.

Slammer Port Address

Identifies the unique identifier of each Slammer network port. For FC networks, this identifier is the World Wide Name (WWN). For iSCSI networks, this identifier is the Media Access Control (MAC) address.

LUN Mapping

Note: The LUN mapping table only displays when you select the **Only selected hosts (via maps)** option.

Hosts Mapped to this LUN

Name	Identifies the SAN host that accesses LUNs configured on the Pillar Axiom system. If the Pillar Axiom Path Manager is not installed, the system displays the WWN of the FC HBA or the IP address of the iSCSI device.
Map via LUN #	Identifies the number to assign to the LUN for the associated SAN host. This number must be unique for that particular host. It need not be unique across all hosts.

Port Status by CU:Port	Identifies a masked physical Slammer port. A port mask prevents the LUN from being accessed from this port. Masked ports are depicted by a blue mask icon, while unmasked ports are identified with a light gray and white mask.
-------------------------------	--

Create

Opens the dialog that allows you to create the LUN-to-host mapping based on your selections for host name and the LUN number to be used by that host.

Modify

Opens the dialog that allows you to change the LUN mapped to the associated host.

Remove

Removes the LUN mapping for the selected SAN host.

Related concepts

- [About Creating LUNs](#)
- [About Copying and Cloning LUNs](#)
- [About Licensing Optional Premium Features](#)

Related references

- [Create LUN Map Dialog](#)
- [Connection Status of Slammer Ports](#)
- [Pillar Axiom System Limits](#)

Related tasks

- [Modify a LUN: Define Quality of Service](#)
- [Create LUN: Define Mapping by Selected Hosts](#)
- [Create LUN: Define Quality of Service](#)

Create SAN Clone LUN, Data Protection Tab

Navigation: Storage > SAN > LUNs > Actions > Clone LUN > Data Protection

Allows you to set the storage capacity of a Clone LUN. You can also manage Clone LUN replication schedules from this page.

Clone LUN Capacity

Maximum capacity (in GB) to allocate for Clone LUNs

Specifies the maximum amount of space to make available on the Storage Domain on which the copy of the clones will reside.



Pillar strongly recommends that you allocate sufficient repository capacity to minimize the chances of running out of this space (which could lead to data inconsistency or loss). To set sufficient capacity, use a value equal to the source volume capacity times the number of replicas times the maximum rate of change. For example, for a 100 GB volume that is projected to have 20 active replicas at a time and no more than a 20% rate of change, use a value of 400 GB for the clone repository.

Number of existing Clone LUNs

Specifies the number of clones that have been created for this LUN and its clones.

Available capacity for Clone LUNs

The amount of current storage capacity allocated for clones of this LUN.

Clone Schedules

Name

Specifies the name of the replication schedule.

Start Time

Specifies the date and time to begin scheduling replication.

Frequency

Specifies the frequency at which the scheduled replication runs. Frequencies include:

- Run Once

- Hourly
- Daily
- Weekly

Enabled

Specifies whether the scheduled replication is enabled.

Enabled	Indicates that the scheduled event performs at the specified time.
----------------	--

Disabled	Indicates that the operation will not perform as scheduled. Disable the schedule, for example, when the source volume (LUN or Clone LUN) has not been made available to users.
-----------------	--

Create

Displays a dialog to create a new replication schedule.

Modify

Displays a dialog to modify an existing replication schedule.

Delete

Removes an existing replication schedule.

Related concepts

- [About Modifying LUNs](#)

Related references

- [Pillar Axiom System Limits](#)

Related tasks

- [Modify LUN: Define Data Protection](#)
- [Create a Clone LUN Schedule](#)
- [Modify a LUN Data Protection Schedule](#)
- [Delete a LUN Data Protection Schedule](#)

Copy SAN LUN, Quality of Service Tab

Navigation: Storage > SAN > LUNs > Actions > Copy LUN > Quality of Service

Allows you to create the capacity and performance settings for a LUN of any type (source, clone, or copy).

Selected Storage Class Capacity

Displays the storage capacity of the selected storage class and Storage Domain that is available for the LUN. The graph uses colored bars of different thicknesses to indicate the capacity status of the logical volume you are creating as well as the overall system capacity.

- Solid Green (thin): Indicates the allocated and growth potential capacity for the volume.
- Solid Blue (thick): Indicates the allocated and used capacity for the volume in the selected Storage Domain and storage class, including the impact of the current volume.
- Shaded Gray (thick): Indicates the growth potential for the selected Storage Domain and storage class, including the impact of the current volume.
- Dark Gray (thick): Indicates the available (free) capacity in the selected Storage Domain and storage class, including the impact of the current volume.
- Shaded Red (thick): Indicates the growth potential that cannot be satisfied for the volume in the selected Storage Domain and storage class, including the impact of the current volume.

System Capacity By Storage Class

Displays the storage capacity in use by the selected Storage Domain and that is in use by each media type configured in the system:

- System
- SSD SLC (solid state drive, single-level cell)
- FC (Fibre Channel)
- SATA (serial ATA)

Storage Domain

Allows you to assign the LUN to an existing Storage Domain.

[...] Opens the dialog that allows you to review the physical capacity attributes and the Brick types that are associated with the predefined Storage Domains.

Note: The Storage Domain Details button appears when more than one Storage Domain exists.

Volume Name

Identifies the name that is assigned to a LUN for administrative purposes. LUN names must be unique across the Pillar Axiom system and must be 82 or fewer UTF characters, or 255 or fewer ASCII characters.

Volume Group

Allows you to assign the LUN to an existing volume group.

[...] Opens the dialog that allows you to create new Volume Groups.

Storage Profile

Identifies the set of QoS attributes applied to the LUN.

[...] Opens the View Storage Profiles dialog that allows you to review the profile details.

Recommended Storage Class

Displays the recommended storage class based on the Storage Profile selection.

Storage Class

Identifies the category of physical media on which the logical volume resides: Valid types:

- SATA
- FC
- SSD SLC (solid state drive, single-level cell)

Typical Access

Identifies the most common method of data access. Valid options:

Sequential Read and write requests from client applications tend to request operations on the data one record after the other.

Random	Read and write requests from client applications tend to request operations on the data records in an arbitrary order.
---------------	--

Mixed	Read and write requests from client applications tend to mix the request operations on the data sometimes in sequential and sometimes in random order.
--------------	--

I/O Bias

Identifies the typical read-write ratio. Valid options:

Read	Most requests from client applications are for <code>read</code> operations.
-------------	--

Write	Most requests from client applications are for <code>write</code> operations.
--------------	---

Mixed	Requests from client applications are likely equal for <code>read</code> and <code>write</code> operations.
--------------	---

Redundancy

Identifies how many mirror copies of the original data are stored in the storage pool. Valid options:

Standard	Stores original data only. Data striping over multiple RAID groups maintains full redundancy, even without mirror copies.
-----------------	---

Double	Stores original data and one mirror copy, with data striping over multiple RAID groups.
---------------	---

Priority Level

In addition to determining the placement of data onto specific areas of the drive platters relative to the drive spindles, the priority level of a volume determines the processing *queue priority* for that volume. Queue priority defines the percentage of Slammer CPU cycles that are dedicated to the volume.

Valid options:

Premium	Highest processing queue priority. Striping occurs across eight serial ATA (SATA) RAID groups or four Fibre Channel (FC) RAID groups on the outermost 20% of the drive platters.
----------------	--

High	Next highest processing queue priority. Striping occurs across eight SATA RAID groups or four FC RAID groups on the outermost 20-40% of the drive platters.
Medium	Intermediate processing queue priority. Striping occurs across six SATA RAID groups or three FC RAID groups on the outermost 40-60% of the drive platters.
Low	Next to lowest processing queue priority. Striping occurs across four SATA RAID groups or two FC RAID groups on the outermost 60-80% of the drive platters.
Archive	Lowest processing queue priority. Striping occurs across four SATA RAID groups or two FC RAID groups on the outermost 80-100% of the drive platters.

Background Copy Priority

Identifies the strategy the system should use to control the impact on performance when background tasks need to copy or move data from one location in the storage pool to another.

Note: When the system is idle or lightly loaded, the above background task maximizes the amount of work done regardless of the option selected.

Valid options:

System Chooses	Balances the background copy with the incoming client I/O. This option is the default.
Minimize Impact	Restricts the amount of work performed on a loaded system. This option is intended to have a minimal impact on client I/O throughput at the expense of longer copy times.
Maximum Speed	Prioritizes the background copy at the expense of client I/O throughput.

The following types of operations are affected by the strategy you select:

- Copy
- Restore
- Quality of Service (QoS) changes in:
 - Priority
 - Redundancy
 - Storage Class

Allocated Logical Capacity

Identifies the amount of capacity to be allocated to the logical volume.

Addressable Logical Capacity

Identifies the maximum capacity to which the logical volume can grow. For a clone, this field identifies how much addressable space will be available.

Allocated/Maximum Capacity

Provides an estimate of the physical storage capacity requirements, which are based on your QoS attribute selections.

Estimated Physical Capacity	Identifies the estimated physical capacity (allocated and maximum) for this LUN.
Estimated Clone Capacity	Identifies the estimated capacity (allocated and maximum) for clones of this LUN.
Estimated Total Capacity	Identifies the estimated total capacity (allocated and maximum) for this LUN.

Related concepts

- [*About Creating LUNs*](#)
- [*About Copying and Cloning LUNs*](#)
- [*About Priority Levels*](#)
- [*About Redundancy*](#)
- [*About I/O Bias*](#)
- [*About Access Bias*](#)
- [*About Storage Classes*](#)

Copy SAN LUN, Mapping Tab

Navigation: Storage > SAN > LUNs > Actions > Copy LUN > Mapping

Allows you to create and modify the LUN-to-host mapping settings for a LUN.

Access Protocol

Valid options:

- Fibre Channel (FC): Specifies that hosts can use the FC protocol to access this LUN.
Tip: FC paths will always be used at a preference over iSCSI paths. Also, load balancing will not be mixed between these two protocols.
- iSCSI: Specifies that hosts can use the iSCSI protocol to access this LUN.

Only selected hosts (via maps)

Specifies that only designated SAN hosts can access this LUN using a specific, possibly different, LUN number on each of those hosts. If the LUN is mapped, the LUN number must be unique to the mapped SAN host.

All hosts may access this LUN using LUN Number

Specifies all SAN hosts accessing this LUN use the same LUN number. Select this option to activate the LUN number selection drop-down list.

Available LUN Number

You can map a LUN or Clone LUN to either a single host or a host group.

LUN Slammer Control Unit Assignment

Current Slammer CU

Identifies the current Slammer CU on which the LUN is currently homed.

Note: For new source LUNs, this field is not available; instead, use Assigned Slammer CU.

Assigned Slammer CU <Auto-Assign>

Identifies the Slammer CU to which the system should assign the LUN. Available options:

<auto assign>

Select this option if you want the system to determine the Slammer CU.

Slammer CU Select a specific Slammer CU from the list to assign to the LUN.

Ports Masked for this LUN

Displays the physical Slammer ports to exclude (mask) so they cannot access the LUN.

Masked
Indicates whether the port for the LUN is masked.

Protocol
Identifies the type of access protocol, FC or iSCSI.

Slammer
Identifies the name of the Slammer.

CU
Identifies the control unit (CU) of the Slammer.

Port
Identifies the name of the Slammer CU port.

Slammer Port Address
Identifies the unique identifier of each Slammer network port. For FC networks, this identifier is the World Wide Name (WWN). For iSCSI networks, this identifier is the Media Access Control (MAC) address.

LUN Mapping

Note: The LUN mapping table only displays when you select the **Only selected hosts (via maps)** option.

Hosts Mapped to this LUN

Name	Identifies the SAN host that accesses LUNs configured on the Pillar Axiom system. If the Pillar Axiom Path Manager is not installed, the system displays the WWN of the FC HBA or the IP address of the iSCSI device.
Map via LUN #	Identifies the number to assign to the LUN for the associated SAN host. This number must be unique for that particular host. It need not be unique across all hosts.

Port Status by CU:Port	Identifies a masked physical Slammer port. A port mask prevents the LUN from being accessed from this port. Masked ports are depicted by a blue mask icon, while unmasked ports are identified with a light gray and white mask.
-------------------------------	--

Create

Opens the dialog that allows you to create the LUN-to-host mapping based on your selections for host name and the LUN number to be used by that host.

Modify

Opens the dialog that allows you to change the LUN mapped to the associated host.

Remove

Removes the LUN mapping for the selected SAN host.

Related concepts

- [About Licensing Optional Premium Features](#)

Related references

- [Create LUN Map Dialog](#)
- [Connection Status of Slammer Ports](#)
- [Pillar Axiom System Limits](#)

Related tasks

- [Modify a LUN: Define Quality of Service](#)
- [Create LUN: Define Mapping by Selected Hosts](#)
- [Create LUN: Define Quality of Service](#)

Copy SAN LUN, Data Protection Tab

Navigation: Storage > SAN > LUNs > Actions > Copy LUN > Data Protection

Allows you to set the storage capacity of the Clone LUN. You can also manage Clone LUN replication schedules from this page.

Selected Storage Class Capacity

Displays the storage capacity of the selected storage class and Storage Domain that is available for the LUN. The graph uses colored bars of different thicknesses to indicate the capacity status of the logical volume you are creating as well as the overall system capacity.

- Solid Green (thin): Indicates the allocated and growth potential capacity for the volume.
- Solid Blue (thick): Indicates the allocated and used capacity for the volume in the selected Storage Domain and storage class, including the impact of the current volume.
- Shaded Gray (thick): Indicates the growth potential for the selected Storage Domain and storage class, including the impact of the current volume.
- Dark Gray (thick): Indicates the available (free) capacity in the selected Storage Domain and storage class, including the impact of the current volume.
- Shaded Red (thick): Indicates the growth potential that cannot be satisfied for the volume in the selected Storage Domain and storage class, including the impact of the current volume.

Clone LUN Capacity

Maximum capacity (in GB) to allocate for Clone LUNs

Specifies the maximum amount of space to make available on the Storage Domain on which the copy of the clones will reside.



Pillar strongly recommends that you allocate sufficient repository capacity to minimize the chances of running out of this space (which could lead to data inconsistency or loss). To set sufficient capacity, use a value equal to the source volume capacity times the number of replicas times the maximum rate of change. For example, for a 100 GB volume that is projected to have 20 active replicas at a time and no more than a 20% rate of change, use a value of 400 GB for the clone repository.

Number of existing Clone LUNs

Specifies the number of clones that have been created for this LUN and its clones.

Available capacity for Clone LUNs

The amount of current storage capacity allocated for clones of this LUN.

Clone Schedules**Name**

Specifies the name of the replication schedule.

Start Time

Specifies the date and time to begin scheduling replication.

Frequency

Specifies the frequency at which the scheduled replication runs. Frequencies include:

- Run Once
- Hourly
- Daily
- Weekly

Enabled

Specifies whether the scheduled replication is enabled.

Enabled

Indicates that the scheduled event performs at the specified time.

Disabled

Indicates that the operation will not perform as scheduled. Disable the schedule, for example, when the source volume (LUN or Clone LUN) has not been made available to users.

Create

Displays a dialog to create a new replication schedule.

Modify

Displays a dialog to modify an existing replication schedule.

Delete

Removes an existing replication schedule.

Related concepts

- [About Modifying LUNs](#)

Related references

- [Pillar Axiom System Limits](#)

Related tasks

- [Modify LUN: Define Data Protection](#)
- [Create a Clone LUN Schedule](#)
- [Modify a LUN Data Protection Schedule](#)
- [Delete a LUN Data Protection Schedule](#)

Create Administrator Account Dialog

Navigation: Global Settings > Administrator Accounts > Actions > Create Account

Allows you to create administrator accounts.

Login Name

Identifies the login name assigned to the administrator account. This field is limited to 20 characters.

Role

Identifies the authorized privileges for an administrator account. Different roles are authorized to perform different functions:

Administrator 1	A login account that has the authority to perform all administration, configuration, and recovery tasks.
Administrator 2	<p>A login account that has the authority to perform all administrative and configuration tasks, except:</p> <ul style="list-style-type: none">■ Create, modify, or delete administrator accounts and File Servers.■ Modify system-wide settings such as Simple Network Management Protocol (SNMP).■ Modify software or hardware configurations.■ Shut down the system.
Monitor	A login account that has the authority to perform read-only management tasks in a Pillar Axiom system and the ability to modify their own account attributes.
Support	<p>A unique login account solely for support representatives. This login account is not authorized to modify or delete data resources, system alerts, or administrator accounts.</p> <p>Important! Use this account only if you are familiar with it or instructed by Oracle Pillar Customer Support.</p>

For the following predefined roles, you cannot assign administrators to them and you cannot delete them:

Primary system administrator	A login account that has the same privileges as the Administrator 1 role.
Primary support administrator	A login account that has the same privileges as the Monitor role, as well as privileges to perform support-related tasks.

Full Name

Identifies the first and last name associated with the administrator account.

Email Address

Identifies the email address associated with the administrator account. The email username can have up to 64 characters and the email domain can have up to 255 characters. The email server to which the Pillar Axiom system sends alerts must be able to receive messages at this address. The system does not validate this address.

Note: An IP address cannot be entered as the email domain.

Phone Number

Identifies the phone number associated with the administrator account. The Pillar Axiom system does not verify the validity of this entry.

Password

Identifies the password of the administrator account. Passwords can be between 6 and 20 characters in length. Passwords are case sensitive and embedded spaces are permitted. Blank passwords are not permitted.

Confirm Password

Confirms that the password was entered correctly.

Disable Account

Indicates whether the administrative account is disabled. The Pillar Axiom system maintains disabled accounts but does not allow them to log in. A disabled account can be enabled at a later time by modifying it. This setting takes effect immediately. If the administrator is logged in when you disable the account, the system logs out the administrator immediately.

Note: You cannot disable the **Primary system administrator** account.

Related references

- [Administrator Accounts Overview Page](#)
- [Pillar Axiom System Limits](#)

Related tasks

- [Create a Pillar Axiom Administrator Account](#)
- [Modify an Administrator Account](#)

Create Job Schedule Dialog

Navigation:

- *Groups > Volume Groups > Actions > ... > Data Protection > Create*
- *Storage > SAN > LUNs > Actions > ... > Data Protection > Create*

Allows you to create a data replication job schedule.

Note: A schedule should be synchronized with the host applications that access the logical volume so that all data I/O is quieted before the replication operation starts.

Schedule Name

Identifies the unique name of a scheduled operation, which is an action to be performed at the specified time or at regular intervals.

Data Protection Type

Identifies the type of data protection, such as clone, that is used in the schedule.

Volume Group

Allows you to assign the clone volume to an existing volume group.

Enabled

Indicates whether the schedule is enabled.

- Enable the schedule so that the operation is performed at the specified time.
- Disable the schedule so that operations are not performed. This option allows you to define a schedule before the source volume (LUN or Clone LUN) has been made available to users.

Start Time

Identifies the date and time at which the Pillar Axiom system starts a scheduled operation.

Recurrence

Identifies how often the system should perform the scheduled operation. Valid values vary based on the schedule's recurrence interval and frequency.

Valid values are listed in the following table.

Table 26 Job schedule recurrence intervals

Recurrence interval	Valid values
Hourly	1 through 24
Daily	1 through 7
Weekly	1 though 4

Related references

- [Pillar Axiom System Limits](#)

Related tasks

- [Create a Clone LUN Schedule](#)
- [Modify a LUN Data Protection Schedule](#)
- [Delete a LUN Data Protection Schedule](#)

Create LUN Map Dialog

Navigation:

- *Groups > Volume Groups > Actions > ... > Mapping > Create*
- *Storage > SAN > LUNs > Actions > ... > Mapping > Create*

Allows you to establish LUN connections to a specified host.

LUN Name

Identifies the name of the LUN or Clone LUN on the Pillar Axiom system.

Type

Lists the type of SAN hosts available to access the LUN.

All Hosts	Provides a list of all unassociated and recognized SAN hosts.
Unassociated Hosts	Provides a list of World Wide Names (WWNs) for Fibre Channel (FC) hosts and iSCSI names (iSCSI) for hosts on the SAN network that are not using Pillar Axiom Path Manager.
Recognized Hosts	Provides a list of SAN hosts that are using the Pillar Axiom Path Manager.

Host Name

Identifies the SAN host that accesses LUNs or Clone LUNs configured on the Pillar Axiom system.

LUN Number

You can map a LUN or Clone LUN to either a single host or a host group.

Related references

- [Create SAN Clone LUN, Mapping Tab](#)

Related tasks

- [Create LUN: Define Mapping by Selected Hosts](#)

Create SAN LUN, Quality of Service Tab

Navigation: Storage > SAN > LUNs > Actions > Create LUN > Quality of Service

Allows you to create the capacity and performance settings for a LUN of any type (source, clone, or copy).

Selected Storage Class Capacity

Displays the storage capacity of the selected storage class and Storage Domain that is available for the LUN. The graph uses colored bars of different thicknesses to indicate the capacity status of the logical volume you are creating as well as the overall system capacity.

- Solid Green (thin): Indicates the allocated and growth potential capacity for the volume.
- Solid Blue (thick): Indicates the allocated and used capacity for the volume in the selected Storage Domain and storage class, including the impact of the current volume.
- Shaded Gray (thick): Indicates the growth potential for the selected Storage Domain and storage class, including the impact of the current volume.
- Dark Gray (thick): Indicates the available (free) capacity in the selected Storage Domain and storage class, including the impact of the current volume.
- Shaded Red (thick): Indicates the growth potential that cannot be satisfied for the volume in the selected Storage Domain and storage class, including the impact of the current volume.

System Capacity By Storage Class

Displays the storage capacity in use by the selected Storage Domain and that is in use by each media type configured in the system:

- System
- SSD SLC (solid state drive, single-level cell)
- FC (Fibre Channel)
- SATA (serial ATA)

Storage Domain

Allows you to assign the LUN to an existing Storage Domain.

[...] Opens the dialog that allows you to review the physical capacity attributes and the Brick types that are associated with the predefined Storage Domains.

Note: The Storage Domain Details button appears when more than one Storage Domain exists.

Volume Name

Identifies the name that is assigned to a LUN for administrative purposes. LUN names must be unique across the Pillar Axiom system and must be 82 or fewer UTF characters, or 255 or fewer ASCII characters.

Volume Group

Allows you to assign the LUN to an existing volume group.

[...] Opens the dialog that allows you to create new Volume Groups.

Storage Profile

Identifies the set of QoS attributes applied to the LUN.

[...] Opens the View Storage Profiles dialog that allows you to review the profile details.

Recommended Storage Class

Displays the recommended storage class based on the Storage Profile selection.

Storage Class

Identifies the category of physical media on which the logical volume resides: Valid types:

- SATA
- FC
- SSD SLC (solid state drive, single-level cell)

Typical Access

Identifies the most common method of data access. Valid options:

Sequential Read and write requests from client applications tend to request operations on the data one record after the other.

Random	Read and write requests from client applications tend to request operations on the data records in an arbitrary order.
---------------	--

Mixed	Read and write requests from client applications tend to mix the request operations on the data sometimes in sequential and sometimes in random order.
--------------	--

I/O Bias

Identifies the typical read-write ratio. Valid options:

Read	Most requests from client applications are for <code>read</code> operations.
-------------	--

Write	Most requests from client applications are for <code>write</code> operations.
--------------	---

Mixed	Requests from client applications are likely equal for <code>read</code> and <code>write</code> operations.
--------------	---

Redundancy

Identifies how many mirror copies of the original data are stored in the storage pool. Valid options:

Standard	Stores original data only. Data striping over multiple RAID groups maintains full redundancy, even without mirror copies.
-----------------	---

Double	Stores original data and one mirror copy, with data striping over multiple RAID groups.
---------------	---

Priority Level

In addition to determining the placement of data onto specific areas of the drive platters relative to the drive spindles, the priority level of a volume determines the processing *queue priority* for that volume. Queue priority defines the percentage of Slammer CPU cycles that are dedicated to the volume.

Background Copy Priority

Identifies the strategy the system should use to control the impact on performance when background tasks need to copy or move data from one location in the storage pool to another.

Note: When the system is idle or lightly loaded, the above background task maximizes the amount of work done regardless of the option selected.

Valid options:

System Chooses	Balances the background copy with the incoming client I/O. This option is the default.
Minimize Impact	Restricts the amount of work performed on a loaded system. This option is intended to have a minimal impact on client I/O throughput at the expense of longer copy times.
Maximum Speed	Prioritizes the background copy at the expense of client I/O throughput.

The following types of operations are affected by the strategy you select:

- Copy
- Restore
- Quality of Service (QoS) changes in:
 - Priority
 - Redundancy
 - Storage Class

Allocated Logical Capacity

Identifies the amount of capacity to be allocated to the logical volume.

Addressable Logical Capacity

Identifies the maximum capacity to which the logical volume can grow. For a clone, this field identifies how much addressable space will be available.

Physical Capacity

Provides an estimate of the physical storage capacity requirements, which are based on your QoS attribute selections.

Estimated Physical Capacity	Identifies the estimated physical capacity (allocated and maximum) for this LUN.
Estimated Clone Capacity	Identifies the estimated capacity (allocated and maximum) for clones of this LUN.
Estimated Total Capacity	Identifies the estimated total capacity (allocated and maximum) for this LUN.

Related concepts

- [*About Creating LUNs*](#)
- [*About Priority Levels*](#)
- [*About Redundancy*](#)
- [*About I/O Bias*](#)
- [*About Access Bias*](#)
- [*About Storage Classes*](#)

Related references

- [*Effects of Access Bias and I/O Bias*](#)
- [*Create SAN LUN, Mapping Tab*](#)
- [*Create SAN LUN, Data Protection Tab*](#)
- [*Pillar Axiom System Limits*](#)

Related tasks

- [*Create LUN: Define Quality of Service*](#)
- [*Modify a LUN: Define Quality of Service*](#)

Create SAN LUN, Mapping Tab

Navigation: Storage > SAN > LUNs > Actions > Create LUN > Mapping

Allows you to create and modify the LUN-to-host mapping settings for a LUN.

Access Protocol

Valid options:

- Fibre Channel (FC): Specifies that hosts can use the FC protocol to access this LUN.
Tip: FC paths will always be used at a preference over iSCSI paths. Also, load balancing will not be mixed between these two protocols.
- iSCSI: Specifies that hosts can use the iSCSI protocol to access this LUN.

Only selected hosts (via maps)

Specifies that only designated SAN hosts can access this LUN using a specific, possibly different, LUN number on each of those hosts. If the LUN is mapped, the LUN number must be unique to the mapped SAN host.

All hosts may access this LUN using LUN Number

Specifies all SAN hosts accessing this LUN use the same LUN number. Select this option to activate the LUN number selection drop-down list.

Available LUN Number

You can map a LUN or Clone LUN to either a single host or a host group.

LUN Slammer Control Unit Assignment

Current Slammer CU

Identifies the current Slammer CU on which the LUN is currently homed.

Note: For new source LUNs, this field is not available; instead, use Assigned Slammer CU.

Assigned Slammer CU <Auto-Assign>

Identifies the Slammer CU to which the system should assign the LUN. Available options:

<auto assign>

Select this option if you want the system to determine the Slammer CU.

Slammer CU Select a specific Slammer CU from the list to assign to the LUN.

Ports Masked for this LUN

Displays the physical Slammer ports to exclude (mask) so they cannot access the LUN.

Masked

Indicates whether the port for the LUN is masked.

Protocol

Identifies the type of access protocol, FC or iSCSI.

Slammer

Identifies the name of the Slammer.

CU

Identifies the control unit (CU) of the Slammer.

Port

Identifies the name of the Slammer CU port.

Slammer Port Address

Identifies the unique identifier of each Slammer network port. For FC networks, this identifier is the World Wide Name (WWN). For iSCSI networks, this identifier is the Media Access Control (MAC) address.

LUN Mapping

Note: The LUN mapping table only displays when you select the **Only selected hosts (via maps)** option.

Hosts Mapped to this LUN

Name	Identifies the SAN host that accesses LUNs configured on the Pillar Axiom system. If the Pillar Axiom Path Manager is not installed, the system displays the WWN of the FC HBA or the IP address of the iSCSI device.
Map via LUN #	Identifies the number to assign to the LUN for the associated SAN host. This number must be unique for that particular host. It need not be unique across all hosts.

Port Status by CU:Port	Identifies a masked physical Slammer port. A port mask prevents the LUN from being accessed from this port. Masked ports are depicted by a blue mask icon, while unmasked ports are identified with a light gray and white mask.
-------------------------------	--

Create

Opens the dialog that allows you to create the LUN-to-host mapping based on your selections for host name and the LUN number to be used by that host.

Modify

Opens the dialog that allows you to change the LUN mapped to the associated host.

Remove

Removes the LUN mapping for the selected SAN host.

Related concepts

- [About Licensing Optional Premium Features](#)

Related references

- [Create LUN Map Dialog](#)
- [Connection Status of Slammer Ports](#)
- [Pillar Axiom System Limits](#)

Related tasks

- [Modify a LUN: Define Quality of Service](#)
- [Create LUN: Define Mapping by Selected Hosts](#)
- [Create LUN: Define Quality of Service](#)

Create SAN LUN, Data Protection Tab

Navigation: Storage > SAN > LUNs > Actions > Create LUN > Data Protection

Allows you to set the storage capacity of the Clone LUN. You can also manage Clone LUN replication schedules from this page.

Selected Storage Class Capacity

Displays the storage capacity of the selected storage class and Storage Domain that is available for the LUN. The graph uses colored bars of different thicknesses to indicate the capacity status of the logical volume you are creating as well as the overall system capacity.

- Solid Green (thin): Indicates the allocated and growth potential capacity for the volume.
- Solid Blue (thick): Indicates the allocated and used capacity for the volume in the selected Storage Domain and storage class, including the impact of the current volume.
- Shaded Gray (thick): Indicates the growth potential for the selected Storage Domain and storage class, including the impact of the current volume.
- Dark Gray (thick): Indicates the available (free) capacity in the selected Storage Domain and storage class, including the impact of the current volume.
- Shaded Red (thick): Indicates the growth potential that cannot be satisfied for the volume in the selected Storage Domain and storage class, including the impact of the current volume.

Clone LUN Capacity

Maximum capacity (in GB) to allocate for Clone LUNs

Specifies the maximum amount of space to make available on the Storage Domain on which the copy of the clones will reside.

**Caution**

Pillar strongly recommends that you allocate sufficient repository capacity to minimize the chances of running out of this space (which could lead to data inconsistency or loss). To set sufficient capacity, use a value equal to the source volume capacity times the number of replicas times the maximum rate of change. For example, for a 100 GB volume that is projected to have 20 active replicas at a time and no more than a 20% rate of change, use a value of 400 GB for the clone repository.

Number of existing Clone LUNs

Specifies the number of clones that have been created for this LUN and its clones.

Available capacity for Clone LUNs

The amount of current storage capacity allocated for clones of this LUN.

Clone Schedules**Name**

Specifies the name of the replication schedule.

Start Time

Specifies the date and time to begin scheduling replication.

Frequency

Specifies the frequency at which the scheduled replication runs. Frequencies include:

- Run Once
- Hourly
- Daily
- Weekly

Enabled

Specifies whether the scheduled replication is enabled.

Enabled

Indicates that the scheduled event performs at the specified time.

Disabled

Indicates that the operation will not perform as scheduled. Disable the schedule, for example, when the source volume (LUN or Clone LUN) has not been made available to users.

Create

Displays a dialog to create a new replication schedule.

Modify

Displays a dialog to modify an existing replication schedule.

Delete

Removes an existing replication schedule.

Related concepts

- [About Creating LUNs](#)

Related references

- [Pillar Axiom System Limits](#)

Related tasks

- [Create LUN: Define Data Protection](#)
- [Modify a LUN: Define Quality of Service](#)
- [Create a Clone LUN Schedule](#)
- [Modify a LUN Data Protection Schedule](#)
- [Delete a LUN Data Protection Schedule](#)

Create SNMP Host Dialog

Navigation: Global Settings > SNMP > Actions > Create SNMP Host

Allows you to create Simple Network Management Protocol (SNMP) trap hosts.

Name

Identifies the name for the SNMP host.

Host IP

Identifies the IP address or domain name of a client that receives the Pillar Axiom SNMP information.

Community string

Identifies the community string for use when the Pillar Axiom system sends an event trap to the SNMP host.

Note: When an administrator does not specify a community string for read-only access, SNMP servers and clients will typically use `public`.

Receive traps

Indicates that the SNMP host receives event traps sent to it.

Trap Port Number

Identifies the SNMP host port number to use for sending an event trap.

Severity threshold

Identifies the severity threshold for events that are to be sent to the SNMP host by event traps.

Severity levels:

- **Informational**
- **Warning**
- **Critical**

Related concepts

- [*About Licensing Optional Premium Features*](#)

Related references

- [*Pillar Axiom System Limits*](#)

Related tasks

- [*Create SNMP Hosts*](#)
- [*Delete SNMP Hosts*](#)
- [*Modify SNMP Hosts*](#)

Global Settings Overview Page

Navigation: Global Settings

Allows you to select system-wide settings for the Pillar Axiom system. After you select a category of settings, you can review or modify the collection of settings for that category.

Networking

Allows you to review or modify various characteristics of the customer network, including for example:

- The Pillar Axiom management interface
- Call-Home configuration
- iSCSI connectivity

Security

Allows you to manage account security settings.

Administrator Accounts

Allows you to create and manage the administrator accounts that are configured on the Pillar Axiom system.

SNMP

Allows you to manage the Simple Network Management Protocol (SNMP) trap hosts.

System Time

Allows you to set and synchronize the time across all Pillar Axiom components.

Related references

- [*Modify Network Settings, Interfaces Tab*](#)
- [*Modify Security Settings Dialog*](#)
- [*Administrator Accounts Overview Page*](#)
- [*SNMP Hosts Overview Page*](#)
- [*System Time Overview Page*](#)
- [*Pillar Axiom System Limits*](#)

Related tasks

- [*Configure the Management Interface*](#)
- [*Configure Email Notification Settings*](#)
- [*Modify Call-Home Settings*](#)
- [*Modify an Administrator Account*](#)
- [*Create a Pillar Axiom Administrator Account*](#)
- [*Test Call-Home*](#)

Groups Overview Page

Navigation: Groups

Allows you to access options to manage volume groups and Storage Domains for the Pillar Axiom system.

Volume groups are organizational units that can contain any grouping of logical volumes and nested volume groups.

Storage Domains allow storage administrators to assign logical volumes to a specific collection of Bricks. Such assignments can be made to reduce contention among volumes, to implement different levels of security for those volumes, or both.

Volume Groups

Allows you to create and manage volume groups.

Storage Domains

Allows you to create and manage Storage Domains.

Related references

- [Volume Groups Overview Page](#)
- [Storage Domains Overview Page](#)

Host to LUN Mapping Overview Page

Navigation: Storage > SAN > Host-LUN Mapping

Allows you to review the mapping between the SAN hosts and the Pillar Axiom system LUNs with which the hosts are associated. This page also displays the status of the connections between these hosts and the associated Slammer ports.

Host to LUN Map

Provides a list of SAN Hosts and LUNs to which they are mapped.

HBA Port/Device	Identifies the SAN hosts associated with the LUNs: <ul style="list-style-type: none">■ For Fibre Channel networks: The World Wide Name (WWN) of the SAN host HBA port that is associated with the LUN.■ For iSCSI networks: The IP address of the iSCSI device that is associated with the LUN.
-----------------	--

Map via LUN #	Identifies the LUN number used for the SAN host mapping.
---------------	--

LUN Name on Host	Identifies the name used by the SAN host to identify the LUN.
------------------	---

Number of Paths

Provides the number of optimized and non-optimized data paths for the LUN mapping.

Optimized	Identifies the number of optimized (fastest path available) access paths to the LUN.
Non Optimized	Identifies the number of non-optimized access paths to the LUN.

Pillar Slammer Port by CU: Port

Identifies the connection status of each SAN Slammer port.

Related references

- [*SAN Hosts Overview Page*](#)
- [*LUN to Host Mapping Overview Page*](#)
- [*Connection Status of Slammer Ports*](#)

LUN to Host Mapping Overview Page

Navigation: Storage > SAN > LUN-Host Mapping

Allows you to review the mappings between the Pillar Axiom LUNs and the SAN hosts with which they are associated. This page also displays the status of the connections between these hosts and the associated Slammer ports.

LUN to Host Map

Provides a list of LUNs and SAN Hosts to which they are mapped.

Name	Identifies the name of the LUN or Clone LUN on the Pillar Axiom system.
Map via LUN #	Identifies the LUN number used for the SAN host mapping.
LUN Name on Host	Identifies the name used by the SAN host to identify the LUN.

Number of Paths

Provides the number of optimized and non-optimized data paths for the LUN mapping.

Optimized	Identifies the number of optimized (fastest path available) access paths to the LUN.
Non Optimized	Identifies the number of non-optimized access paths to the LUN.

Pillar Slammer Port by CU:Port

Identifies the connection status of each SAN Slammer port.

Related references

- [SAN Hosts Overview Page](#)
- [Host to LUN Mapping Overview Page](#)
- [Connection Status of Slammer Ports](#)

Manage SAN Host Groups, Groups Tab

Navigation: Storage > SAN > Host > Actions > Manage SAN Host Groups > Groups

Allows you to create and modify host groups to which you can assign a Pillar Axiom Path Manager registered SAN host.

A *host group* is a named collection of SAN hosts that the system manages as a group, which simplifies the task of associating hosts to LUNs.

Name

Indicates the name of the Host Group.

Create

Creates a new row for the Host Group.

Delete

Deletes the selected Host Group.

Related concepts

- [About Host Groups](#)
- [About SAN Host Management](#)

Related references

- [Manage SAN Host Groups, Hosts Tab](#)

Related tasks

- [Create a SAN Host Group](#)
- [Delete a SAN Host Group](#)

Manage SAN Host Groups, Hosts Tab

Navigation: Storage > SAN > Host > Actions > Manage SAN Host Groups > Hosts

Allows you to associate Pillar Axiom Path Manager registered SAN hosts to a host group.

A *host group* is a named collection of SAN hosts that the system manages as a group, which simplifies the task of associating hosts to LUNs.

Name

Indicates the name of the SAN Host.

Host Group

Indicates the name of the available host group.

Related concepts

- [*About Host Groups*](#)

Related tasks

- [*Create a SAN Host Group*](#)
- [*Delete a SAN Host Group*](#)

Manage Storage Domains, Bricks Tab

Navigation: Configure > Groups > Storage Domains > Actions > Manage Storage Domains > Bricks

Assigns Bricks to specific Storage Domains. A Pillar Axiom Storage Domain is a subset of a virtual storage pool that is comprised of a grouping of physical Bricks.

Brick Name

Specifies the external name for the Brick.

Brick Type

Identifies the category of physical storage on which logical volumes can reside:

- SATA
- FC
- SSD SLC (solid state drive, single-level cell)

Storage Domain

Specifies the name of the Storage Domain.

Clicking the Storage Domain name for a particular Brick exposes a list of the available domains to which this Brick can be assigned.

Note: Reassigning a Brick to another domain is allowed only when no logical volumes are using that Brick.

Physical Capacity (GB)

Allocated

Displays the amount of raw capacity, in gigabytes (GB), that has been assigned and designated to all logical volumes residing on the indicated Brick.

Free

Displays the amount of raw capacity (in GB) that is available for allocation in the indicated Brick.

Unavailable

Displays the amount of raw capacity (in GB) that is currently being initialized. This value typically results from a volume having been deleted. This value decreases over a period of time while the value for free capacity correspondingly increases for the indicated Storage Domain.

Total Capacity

Displays the total amount of raw capacity (in GB) provided by the indicated Brick.

Related concepts

- [*About Storage Domains*](#)

Related references

- [*Storage Domains Overview Page*](#)

Related tasks

- [*Reassign a Brick to Another Storage Domain*](#)

Manage Storage Domains, Storage Domains Tab

Navigation: Configure > Groups > Storage Domains > Actions > Manage Storage Domains > Storage Domains

Adds and removes Storage Domains.

Note: Storage Domains might limit the ability of the system to provide the best optimization of the storage arrays and system performance.

Storage Domain

Specifies the name of the Storage Domain.

Note: For an existing domain, you can modify the name.

Primary

Indicates whether this Storage Domain is the primary Storage Domain.

Allocated

Displays the amount of raw capacity, in gigabytes (GB), that has been assigned and designated to all logical volumes residing on the indicated Storage Domain.

Free

Displays the amount of raw capacity (in GB) that is available for allocation in the indicated Storage Domain.

Unavailable

Displays the amount of raw capacity (in GB) that is currently being initialized. This value typically results from a volume having been deleted. This value decreases over a period of time while the value for free capacity correspondingly increases for the indicated Storage Domain.

Total Capacity

Displays the total amount of raw capacity (in GB) provided by the Bricks defined within the indicated Storage Domain.

Create

Creates a Storage Domain.

Note: The Pillar Axiom system must contain at least three Bricks before a Storage Domain can be created.

Clicking this button causes a new row to be created in the display, allowing you to enter a name for the new Storage Domain.

Remove

Removes one or more Storage Domains from the Pillar Axiom system.

Note: You cannot delete the primary Storage Domain. Also, you cannot delete a Storage Domain that has any logical volumes or Bricks assigned to it.

Related concepts

- [About Storage Domains](#)
- [About Licensing Optional Premium Features](#)

Related references

- [Storage Domains Overview Page](#)

Related tasks

- [Create a Storage Domain](#)
- [Delete a Storage Domain](#)
- [Modify a Storage Domain](#)
- [Reassign a Brick to Another Storage Domain](#)
- [Set a Storage Domain as the Primary](#)

Manage Storage Domains, Volumes Tab

Navigation: Configure > Groups > Storage Domains > Actions > Manage Storage Domains > Volumes

Assigns logical volumes to a specific Storage Domain or, if the proper conditions exist, moves a logical volume from one domain to another.

Name

Specifies the name for the logical volume.

Storage Domain

Specifies the name of the Storage Domain.

If the proper conditions exist, you can assign a logical volume to a different domain by clicking on the Storage Domain for a particular logical volume. Clicking on the name of the Storage Domain exposes a list of the available domains to which you can assign this volume.

Important! Assigning a volume to a new Storage Domain, if sufficient space is available in that domain, causes data migration.

Physical Capacity

Redundancy

Identifies how many mirror copies of the original data are stored in the storage pool. Valid options:

Standard	Stores original data only. Data striping over multiple RAID groups maintains full redundancy, even without mirror copies.
Double	Stores original data and one mirror copy, with data striping over multiple RAID groups.

Disk Protection

Indicates the RAID drive data protection method. Valid options:

Parity	Indicates that data on a RAID drive is protected through use of a special algorithm, the results of which are stored on a separate drive for fault tolerance.
Mirroring	Indicates that data on a RAID drive is protected by means of an exact copy of that

data. A mirror set is created for a volume that has a double redundancy setting.

Default

Indicates that the Pillar Axiom system selects the appropriate data protection based on selected QoS settings.

Volume Overhead

Identifies the physical and logical storage capacity that is required to meet the logical volume Quality of Service (QoS) settings.

Used

Identifies the current capacity consumed by the volume.

Allocated

Specifies the amount of raw capacity in gigabytes (GB) that has been assigned and designated to this logical volume.

Maximum

Identifies the maximum capacity to which the logical volume can grow. For a clone, this field identifies how much addressable space will be available.

Related concepts

- [About Storage Domains](#)

Related references

- [Storage Domains Overview Page](#)

Related tasks

- [Move a Volume to Another Storage Domain](#)

Manage Storage Profiles Dialog

Navigation: Storage > Storage Profiles > Actions > Manage Storage Profiles

Allows you to manage a set of Quality of Service (QoS) settings that can be used for creating new logical volumes. You can create your own profile or duplicate an existing profile and then modify the duplicate to satisfy your needs.

Manage Standard Storage Profiles

Provides options to create a Storage Profile by using regular QoS properties.

Note: For the descriptions of these properties, refer to the section below that describes the Storage Profiles table.

Manage Advanced Storage Profiles (expert users only)

Provides access to the full set of QoS properties when creating a custom Storage Profile.

Note: This option is recommended for expert administrators who understand the full range of QoS properties.

Storage Profiles

The Storage Profiles table provides detailed information about each Storage Profile setting, including the QoS settings associated with a particular profile. Additional fields are displayed when you select the Manage Advanced Storage Profiles option for expert users.

Type

Identifies the source of the Storage Profile. Valid types:

Advanced	Administrator defined – includes specifications for the size of a strip and the number of RAID groups.
Custom	Administrator defined– uses the default settings for the size of a strip and the number of RAID groups.
System	Pillar defined.

Name

Identifies the name of the Storage Profile. The name includes, in some instances, the name of the application that is associated with the profile.

Storage Profile names can consist of up to 128 UTF-8 characters.

Priority Level

In addition to determining the placement of data onto specific areas of the drive platters relative to the drive spindles, the priority level of a volume

determines the processing *queue priority* for that volume. Queue priority defines the percentage of Slammer CPU cycles that are dedicated to the volume.

Valid options:

Premium	Highest processing queue priority. Striping occurs across eight serial ATA (SATA) RAID groups or four Fibre Channel (FC) RAID groups on the outermost 20% of the drive platters.
High	Next highest processing queue priority. Striping occurs across eight SATA RAID groups or four FC RAID groups on the outermost 20-40% of the drive platters.
Medium	Intermediate processing queue priority. Striping occurs across six SATA RAID groups or three FC RAID groups on the outermost 40-60% of the drive platters.
Low	Next to lowest processing queue priority. Striping occurs across four SATA RAID groups or two FC RAID groups on the outermost 60-80% of the drive platters.
Archive	Lowest processing queue priority. Striping occurs across four SATA RAID groups or two FC RAID groups on the outermost 80-100% of the drive platters.

Redundancy

Identifies how many mirror copies of the original data are stored in the storage pool. Valid options:

Standard	Stores original data only. Data striping over multiple RAID groups maintains full redundancy, even without mirror copies.
Double	Stores original data and one mirror copy, with data striping over multiple RAID groups.

Typical Access

Identifies the most common method of data access. Valid options:

Sequential	Read and write requests from client applications tend to request operations on the data one record after the other.
Random	Read and write requests from client applications tend to request operations on the data records in an arbitrary order.

Mixed Read and write requests from client applications tend to mix the request operations on the data sometimes in sequential and sometimes in random order.

I/O Bias

Identifies the typical read-write ratio. Valid options:

Read Most requests from client applications are for `read` operations.

Write Most requests from client applications are for `write` operations.

Mixed Requests from client applications are likely equal for `read` and `write` operations.

Strip Size

This property is available for advanced Storage Profiles only.

Identifies the number of contiguous bytes in each block of data written to the drives. Valid options:

1MB Used for the Oracle Automatic Storage Management (ASM) Storage Profile. These strips are 1024 KB (1 MB) in size.

**Default
Normal** The number of bytes in the strip depends on the type of media contained within a Brick:

- 64 KB for Fibre Channel (FC) media
- 128 KB for serial ATA (SATA) media
- 128 KB for solid-state drive (SSD) media

Number of RAID Groups

This property is available for advanced Storage Profiles only.

Identifies the number of RAID groups over which striping is to be performed. Typical usage is as follows:

2 Priority level is archive or low.
Storage Class is Fibre Channel (FC).

3 Priority level is medium.
Storage Class is FC.

- | | |
|---|---|
| 4 | <ul style="list-style-type: none">■ Priority level is high or premium.
Storage Class is FC.■ Priority level is archive or low.
Storage Class is serial ATA (SATA). |
| 6 | Priority level is medium.
Storage Class is SATA. |
| 8 | Priority level is high or premium.
Storage Class is SATA. |

Note: When the Storage Class is solid state drive (SSD), the system stripes data across all drives, regardless of the priority level associated with the logical volume.

Auto-select allows the system to choose the number of RAID groups. For example, if you duplicate the Performance Benchmark profile and set the number of RAID groups to Auto-select, the system will use all Bricks to stripe the data.

Read Ahead

Indicates the read-ahead settings to use for the profile. The settings adjust the amount of additional data that is read into cache. Valid options:

Normal	Reads only the requested data. No additional data is put into cache.
Aggressive	Reads large extents of the cached data.
Default	Reads beyond the requested data and puts the additional data into cache.
Conservative	Writes data to physical storage in full stripe extents. Data is retained in cache for a shorter period of time.

Writes

Identifies the write caching rules to use for the profile. Valid options:

Write-through	Writes data to the Slammer cache and on the Bricks before the write request returns. This rule ensures that the data is safely written to the Bricks before the write request returns to the application. This option performs more slowly than write-
----------------------	--

back because the data is also being written to the Bricks as well as to the faster cache.

Write-back caching

Writes data to the Slammer cache, and the write request returns immediately. During idle cycles, the system writes the data from the cache to the Bricks. Write-back caching performs faster because the data only needs to be written to the cache prior to returning from the write call.

Important! If the system crashes, the data in the cache that has not been written to the Bricks might be lost.

The system ensures all cached data is written to the Bricks during the shutdown process.

Default

Indicates that the Pillar Axiom system selects the appropriate write cache based on selected QoS settings.

Disk Protection

Indicates the RAID drive data protection method. Valid options:

Parity

Indicates that data on a RAID drive is protected through use of a special algorithm, the results of which are stored on a separate drive for fault tolerance.

Mirroring

Indicates that data on a RAID drive is protected by means of an exact copy of that data. A mirror set is created for a volume that has a double redundancy setting.

Default

Indicates that the Pillar Axiom system selects the appropriate data protection based on selected QoS settings.

Preferred Storage Classes

Identifies the category of physical media on which the logical volume resides: Valid types:

- SATA
- FC
- SSD SLC (solid state drive, single-level cell)

Create Standard/Advanced Profile

Add a new standard or advanced Storage Profile and adjust the QoS settings as desired.

Duplicate

This button is available for advanced Storage Profiles only. Creates a copy of the selected Storage Profile as a new advanced profile. If you duplicate a system Storage Profile, the system creates an advanced profile with the same properties as the original, which you can then edit.

Remove

Deletes the selected Storage Profile.

Note: You cannot delete a system Storage Profile.

Related concepts

- [About Redundancy](#)
- [About Storage Profiles](#)

Related references

- [System Storage Profile Properties](#)

Manage Storage Profiles Overview Page

Navigation: Storage > Storage Profiles

Allows you to review the Quality of Service (QoS) settings for all of the available Storage Profiles on the system. You can also create and manage custom profiles from this page.

Type

Identifies the source of the Storage Profile. Valid types:

Advanced	Administrator defined – includes specifications for the size of a strip and the number of RAID groups.
Custom	Administrator defined– uses the default settings for the size of a strip and the number of RAID groups.
System	Pillar defined.

Name

Identifies the name of the Storage Profile. The name includes, in some instances, the name of the application that is associated with the profile.

Priority Level

Determines how much of the system resources are devoted to the volume. Valid options:

Premium	Highest processing queue priority. Striping occurs across eight serial ATA (SATA) RAID groups or four Fibre Channel (FC) RAID groups on the outermost 20% of the drive platters.
High	Next highest processing queue priority. Striping occurs across eight SATA RAID groups or four FC RAID groups on the outermost 20-40% of the drive platters.
Medium	Intermediate processing queue priority. Striping occurs across six SATA RAID groups or three FC RAID groups on the outermost 40-60% of the drive platters.
Low	Next to lowest processing queue priority. Striping occurs across four SATA RAID groups or two FC RAID groups on the outermost 60-80% of the drive platters.
Archive	Lowest processing queue priority. Striping occurs across four SATA RAID groups or two FC RAID groups on the outermost 80-100% of the drive platters.

Redundancy

Identifies how many mirror copies of the original data are stored in the storage pool. Valid options:

Standard	Stores original data only. Data striping over multiple RAID groups maintains full redundancy, even without mirror copies.
Double	Stores original data and one mirror copy, with data striping over multiple RAID groups.

Related concepts

- [About Storage Profiles](#)

Related references

- [System Storage Profile Properties](#)
- [Manage Storage Profiles Dialog](#)

Manage Volume Groups, Volume Groups Tab

Navigation: Groups > Volume Groups > Actions > Manage Volume Groups > Volume Groups

Allows you to manage the organizational units that group any number of logical volumes.

Volume Group

Identifies the name of the volume group. Valid volume group names consist of letters and digits up to 14 characters long. Each volume group name must be unique within its parent volume group.

Parent Volume Group Name

Identifies the name of the parent volume group in a nested volume group relationship.

Physical Capacity (GB)

Identifies an overview of the actual physical storage capacity usage and requirements of all the volumes on the system.

Used	Identifies the current capacity consumed by the volume.
Allocated	Specifies the amount of raw capacity in gigabytes (GB) that has been assigned and designated to this logical volume.
Maximum	Identifies the maximum capacity for the volume group. The maximum capacity of the logical volumes and nested volume groups that are associated with the volume group cannot exceed this value. A value of 0 (zero) identifies that the volume group is configured with unlimited capacity. You can increase the maximum capacity of associated logical volumes and nested volume groups without constraints.
Physical Distribution	A graphical representation of the capacity used compared to the maximum allocated.

Create

Creates a new row for the volume group.

Remove

Deletes the selected volume group.

Related references

- [*Manage Volume Groups, Volumes Tab*](#)
- [*Pillar Axiom System Limits*](#)

Related tasks

- [*Create Volume Groups*](#)
- [*Modify Volume Group Attributes*](#)
- [*Move a Volume to a Different Volume Group*](#)
- [*Delete a Volume Group*](#)

Manage Volume Groups, Volumes Tab

Navigation: Groups > Volume Groups > Actions > Manage Volume Groups > Volumes

Allows you to manage the organizational units that group any number of logical volumes.

Volume Name

Identifies the names of the configured logical volumes.

Storage Domain

Lists the name of the Storage Domain associated with the logical volume.

Logical Capacity (GB)

Identifies an overview of the logical storage capacity usage and requirements of the volume group.

Used	Identifies the storage capacity currently consumed by the volume.
Allocated	Identifies the total amount of storage capacity that is reserved in the Storage Domain for this volume.
Maximum	Identifies the maximum storage capacity to which the logical volume can grow.

Physical Capacity (GB)

Identifies an overview of the actual physical storage capacity usage and requirements of all the volumes on the system.

Redundancy	Identifies how many mirror copies of the original data are stored online.
Disk Protection	Indicates the RAID drive data protection method.
Volume Overhead	Identifies the physical and logical storage capacity that is required to meet the logical volume Quality of Service (QoS) settings.
Used	Identifies the current capacity consumed by the volume.
Allocated	Specifies the amount of raw capacity in gigabytes (GB) that has been assigned and designated to this logical volume.

Maximum

Identifies the maximum capacity for the volume group. The maximum capacity of the logical volumes and nested volume groups that are associated with the volume group cannot exceed this value. A value of 0 (zero) identifies that the volume group is configured with unlimited capacity. You can increase the maximum capacity of associated logical volumes and nested volume groups without constraints.

Priority Level

Identifies the assigned priority level when the volume was created.

- Premium
- High
- Medium
- Low
- Archive

Related references

- [*Manage Volume Groups, Volume Groups Tab*](#)
- [*Pillar Axiom System Limits*](#)

Related tasks

- [*Create Volume Groups*](#)
- [*Modify Volume Group Attributes*](#)
- [*Move a Volume to a Different Volume Group*](#)
- [*Delete a Volume Group*](#)

Manage Volume Groups Dialog

Navigation: Groups > SAN > LUNs > Actions > Create LUN > Quality of Service > Manage Volume Groups

Allows you to create and manage the organizational units that group any number of logical volumes. For example, you may want to nest one volume group within another or change the maximum capacity for a volume group.

Volume Group

Identifies the name of the volume group. Valid volume group names consist of letters and digits up to 14 characters long. Each volume group name must be unique within its parent volume group.

Parent Volume Group Name

Identifies the name of the parent volume group in a nested volume group relationship.

Physical Capacity (GB)

Identifies an overview of the actual physical storage capacity usage and requirements of all the volumes on the system.

Used	Identifies the current capacity consumed by the volume.
Allocated	Specifies the amount of raw capacity in gigabytes (GB) that has been assigned and designated to this logical volume.
Maximum	Identifies the maximum capacity for the volume group. The maximum capacity of the logical volumes and nested volume groups that are associated with the volume group cannot exceed this value. A value of 0 (zero) identifies that the volume group is configured with unlimited capacity. You can increase the maximum capacity of associated logical volumes and nested volume groups without constraints.
Physical Distribution	A graphical representation of the capacity used compared to the maximum allocated.

Create

Creates a new row for the volume group.

Remove

Deletes the selected volume group.

Related references

- [*Create SAN LUN, Quality of Service Tab*](#)
- [*Pillar Axiom System Limits*](#)

Related tasks

- [*Create Volume Groups*](#)

Modify Administrator Account Dialog

Navigation: Global Settings > Administrator Accounts > Actions > Modify Account

Allows you to modify a specific administrator account.

Login Name

Identifies the login name assigned to the administrator account. This field is limited to 20 characters.

Role

Identifies the authorized privileges for an administrator account. Different roles are authorized to perform different functions:

Administrator 1	A login account that has the authority to perform all administration, configuration, and recovery tasks.
Administrator 2	<div>A login account that has the authority to perform all administrative and configuration tasks, except:<ul style="list-style-type: none">■ Create, modify, or delete administrator accounts and File Servers.■ Modify system-wide settings such as Simple Network Management Protocol (SNMP).■ Modify software or hardware configurations.■ Shut down the system.</div>
Monitor	A login account that has the authority to perform read-only management tasks in a Pillar Axiom system and the ability to modify their own account attributes.
Support	<div>A unique login account solely for support representatives. This login account is not authorized to modify or delete data resources, system alerts, or administrator accounts.</div> <div>Important! Use this account only if you are familiar with it or instructed by Oracle Pillar Customer Support.</div>

For the following predefined roles, you cannot assign administrators to them and you cannot delete them:

Primary system administrator	A login account that has the same privileges as the Administrator 1 role.
Primary support administrator	A login account that has the same privileges as the Monitor role, as well as privileges to perform support-related tasks.

Full Name

Identifies the first and last name associated with the administrator account.

Email Address

Identifies the email address associated with the administrator account. The email username can have up to 64 characters and the email domain can have up to 255 characters. The email server to which the Pillar Axiom system sends alerts must be able to receive messages at this address. The system does not validate this address.

Note: An IP address cannot be entered as the email domain.

Phone Number

Identifies the phone number associated with the administrator account. The Pillar Axiom system does not verify the validity of this entry.

Password

Identifies the password of the administrator account. Passwords can be between 6 and 20 characters in length. Passwords are case sensitive and embedded spaces are permitted. Blank passwords are not permitted.

Confirm Password

Confirms that the password was entered correctly.

Disable Account

Indicates whether the administrative account is disabled. The Pillar Axiom system maintains disabled accounts but does not allow them to log in. A disabled account can be enabled at a later time by modifying it. This setting takes effect immediately. If the administrator is logged in when you disable the account, the system logs out the administrator immediately.

Note: You cannot disable the **Primary system administrator** account.

Related references

- [Administrator Accounts Overview Page](#)
- [Pillar Axiom System Limits](#)

Related tasks

- [Create a Pillar Axiom Administrator Account](#)
- [Modify an Administrator Account](#)

Modify Asset Information Dialog

Navigation: Summary > System > Actions > Modify Asset Information

Allows you to manage the Pillar Axiom system asset information.

Name

Indicates the name of the Pillar Axiom system.

Description

Indicates the description of the Pillar Axiom system.

Location

Indicates the location of the Pillar Axiom system.

Contact Name

Lists the individuals who are responsible for the Pillar Axiom system.

Contact Phone

Indicates the phone number of the contact.

Asset Number

Indicates the corporate asset number assigned to the Pillar Axiom system.

Related tasks

- [*Modify Asset Information*](#)

Modify Host, Advanced Tab

Navigation: Storage > SAN > Hosts > Actions > Modify Host > Advanced

Allows you to set or unset the HP compatibility option for a SAN host bus adapter (HBA).

HP-UX Compatibility Mode

Use this option when the SAN hosts that access the LUNs have HP-UX initiator ports and HP HBAs. When this option is enabled, the system determines LUN numbers using the HP-UX addressing scheme, allowing up to 255 LUNs. Also when enabled, the host cannot have a visible LUN using ID 0. You can verify the current host mappings in the **Pillar Axiom Path Manager** tab.

Related concepts

- [About Modifying SAN Hosts](#)

Related references

- [Pillar Axiom System Limits](#)

Related tasks

- [Modify a Host: Reconfigure Advanced Settings](#)

Modify Host, Pillar Axiom Path Manager Tab

Navigation: Storage > SAN > Hosts > Actions > Modify Host > Pillar Axiom Path Manager

Allows you to manage the load balancing settings of LUNs.

Host Information

Host Name

Identifies the name of the SAN host that have access to the Pillar Axiom system.

Management IP Address

Identifies the IP address of the SAN host. The system uses this address to exchange management requests and responses with the Pillar Axiom Path Manager (APM) that is installed on the host. If APM is not installed, this field displays *N/A*.

Operating System

Identifies the operating system of the SAN host in which the Pillar Axiom Path Manager driver has been installed.

Pillar Axiom Path Manager Version

Identifies the version of the APM host driver, if it has been installed, that is running on the SAN host.

Path Manager Settings

LUN Name

Identifies the name of the LUN or Clone LUN on the Pillar Axiom system.

Name on Host

Identifies the name used by the SAN host to identify the LUN.

Load Balancing

Identifies the type of load balancing that the storage area network (SAN) hosts should perform to access Pillar Axiom LUNs.

Valid types:

Static

Indicates load balancing across multiple paths to the configured LUNs.

The software selects the best available path, and all commands are sent over that

path until the path is no longer operational, in which case the failed path fails over to another appropriate path.

Round-robin

Indicates load balancing across multiple paths to the configured LUNs.

Commands are sent one by one using the best available paths, which ensures that LUN commands are evenly distributed over any path that is available to access the LUNs.

Optimized Paths

Identifies the number of optimized (fastest path available) access paths to the LUN.

Non-Optimized Paths

Identifies the number of non-optimized access paths to the LUN.

Related concepts

- [About Modifying SAN Hosts](#)

Related references

- [Pillar Axiom System Limits](#)

Related tasks

- [Modify a Host: Reconfigure Port Settings](#)

Modify Host, iSCSI Access Tab

Navigation: Storage > SAN > Hosts > Actions > Modify Host > iSCSI Access

Allows you to review the storage area network (SAN) host driver information. If you are configuring iSCSI on the host port, you must also configure iSCSI on the Pillar Axiom system.

Note: iSCSI settings are not available for a SAN host that uses the Fibre Channel protocol.

iSCSI Host Specific Settings

Enable Authentication

Indicates whether Challenge Handshake Authentication Protocol (CHAP) for iSCSI sessions between the SAN host and the Pillar Axiom system is enabled.

Note: Depending on the global settings, CHAP name and CHAP secret may not be required. Those parameters are not required, for example, if authentication is performed through a RADIUS server.

Chap Name

Identifies the name of the iSCSI initiator that is to be used during authentication.

CHAP Secret

Identifies the encrypted CHAP authentication password (secret) to be used in the exchange of user names and secrets between two devices. Both devices must support Point-to-Point (PPP) authentication.

Note: The Pillar Axiom system supports up to 100 UTF-8 non-integer characters. However, when connecting to Windows servers, you must limit the secret to a value between 12 and 16 characters in length.

Retype CHAP Secret

Re-enter the encrypted CHAP authentication password.

Grant Access to Axiom

Specifies whether the Pillar Axiom system must reject iSCSI login attempts from initiators that have not explicitly been granted permission by the user through the Pillar Axiom Storage Services Manager interface or through the Pillar Axiom Command Line Interface (CLI).

Related concepts

- [*About iSCSI Settings*](#)

Related references

- [*Modify Network Settings, iSCSI Tab*](#)
- [*Pillar Axiom System Limits*](#)

Related tasks

- [*Modify a Host: Reconfigure Port Settings*](#)

Modify Host, Ports Tab

Navigation: Storage > SAN > Hosts > Actions > Modify Host > Ports

Allows you to review the storage area network (SAN) host driver information. If you are configuring iSCSI on the host port, you must also configure iSCSI on the Pillar Axiom system.

FC Port Information

Alias

Identifies the host bus adapter (HBA) alias name.

Note: Select the field to make necessary changes.

Port

Identifies the WWN assigned to an FC HBA port.

Speed

Displays the transmission speed, in Gbs, of a hardware component.

Manufacturer

Displays the manufacturer of a hardware component.

HBA Model

Displays the model number of a hardware component.

Driver Version

Identifies version of the HBA driver.

Firmware Version

Identifies the HBA firmware version.

iSCSI Port Information

Alias

Identifies the HBA alias name.

Note: Select the field to make necessary changes.

iSCSI Device Name

Identifies the name of the iSCSI initiator for the SAN host. An initiator encapsulates SCSI commands and data requests within iSCSI packets and transfers the packets across the IP network.

IP Addresses

Identifies the IP address of the iSCSI port.

Related concepts

- [About iSCSI Settings](#)

Related references

- [Pillar Axiom System Limits](#)

Related tasks

- [Modify a Host: Reconfigure Port Settings](#)

Modify iSCSI Port Settings Dialog

Navigation: Storage > SAN > Slammer Ports > Actions > Modify iSCSI Ports Settings

Allows you to configure the settings for the Slammer ports dedicated to Internet SCSI (Small Computer System Interface) protocol.

CU

Identifies a control unit (CU) in a Slammer.

Port

Identifies an iSCSI port in the Slammer CU.

MAC Address

Identifies the unique identifier of the host bus adapter (HBA) port in the SAN host. For iSCSI networks, this identifier is the Media Access Control (MAC) address.

Vlan Enabled

Signifies whether a virtual LAN (VLAN) has been defined for the iSCSI network.

Vlan ID

Identifies the group portal tag number.

Address Type

Identifies the configuration method the Pillar Axiom system uses to obtain the IP address of the HBA port. Valid options:

DHCP

Identifies whether a DHCP server automatically assigns the IP addresses to network clients. This setting makes the Pillar Axiom system known to the DHCP software. For this option, you must use a Microsoft DHCP server that has been configured by the Microsoft iSNS Server installer to return the server IP address using DHCP option 43 (vendor-specific) or DHCP option 83 (iSNS).

Note: Microsoft does not support DHCP option 83 until the Windows Server 2008 release.

Static

Identifies whether a permanent IP address will be assigned to the Pilot in a Pillar Axiom system. Choose this option if you do not use DHCP.

IP Address

Enter the primary IP address that is permanently assigned to the management interface of the Pillar Axiom system.

Netmask

Enter a netmask for the primary IP address that is permanently assigned to the management interface of the Pillar Axiom system.

Gateway

Enter a gateway IP address that is permanently assigned to the management interface of the Pillar Axiom system.

MTU

Identifies the maximum transmission unit (MTU) value for the Slammer port.

The frame size (MTU) does not include the Ethernet header portion of the packet. If your network switch has trouble with this, you can set the switch to a larger value or lower the MTU size to correct the problem.

If your network supports extended Ethernet (jumbo) frames, enter an integer greater than 1500 and less than 9001. Make sure that this Pillar Axiom MTU size matches the network MTU size. If the MTU sizes are mismatched, performance may be severely degraded.

TCP Port Number

Identifies the Transmission Control Protocol (TCP) port number that is configured on the iSCSI port.

Related concepts

- [About Licensing Optional Premium Features](#)

Related references

- [Pillar Axiom System Limits](#)

Related tasks

- [Modify iSCSI Port Settings](#)
- [Modify a Host: Reconfigure Port Settings](#)

Modify Job Schedule Dialog

Navigation:

- *Groups > Volume Groups > Actions > ... > Data Protection > Modify*
- *Storage > SAN > LUNs > Actions > ... > Data Protection > Modify*

Allows you to modify a data replication schedule.

Schedule Name

Identifies the unique name of a scheduled operation, which is an action to be performed at the specified time or at regular intervals.

Data Protection Type

Identifies the type of data protection, such as clone, that is used in the schedule.

Volume Group

Allows you to assign the clone volume to an existing volume group.

Enabled

Indicates whether the schedule is enabled.

- Enable the schedule so that the operation is performed at the specified time.
- Disable the schedule so that operations are not performed. This option allows you to define a schedule before the source volume (LUN or Clone LUN) has been made available to users.

Start Time

Identifies the date and time at which the Pillar Axiom system starts a scheduled operation.

Recurrence

Identifies how often the system should perform the scheduled operation. Valid values vary based on the schedule's recurrence interval and frequency.

Related tasks

- [Modify a LUN Data Protection Schedule](#)
- [Delete a LUN Data Protection Schedule](#)

Modify LUN Number Dialog

Navigation: Storage > SAN > LUNs > Actions > Create LUN > Mapping > Modify

Allows you to change the assigned LUN number.

LUN Number

You can map a LUN or Clone LUN to either a single host or a host group.

Related references

- [Create SAN LUN, Mapping Tab](#)

Modify Network Settings, Interfaces Tab

Navigation: Global Settings > Networking > Actions > Modify Network Settings > Interfaces

Allows you to create and modify the Pillar Axiom management and data-path interfaces.

Management Interface

Enable DHCP

Indicates if you have a Dynamic Host Configuration Protocol (DHCP) server that automatically assigns IP addresses to network clients. This setting makes the Pillar Axiom system known to the DHCP software.

Static IP Address

Identifies whether a permanent IP address will be assigned to the Pilot in a Pillar Axiom system. Choose this option if you do not use DHCP.

Note: Selecting this option enables the Public Interface fields.

Transmit Setting

Important! Use care when setting the transmit speed and duplex mode. A management interface setting that is not supported by the external network could result in loss of access to the Pilot. If access is lost, contact the Oracle Pillar Customer Support for assistance.

Select from the drop-down list the speed and duplex mode that you want the Pilot management interface to use. Valid options:

- Auto
- Half - 10 Mbps
- Full - 10 Mbps
- Half - 100 Mbps
- Full - 100 Mbps
- Half - 1000 Mbps
- Full - 1000 Mbps

Note: Auto negotiate is the default transmit setting. We recommend the default setting for all but special circumstances.

Transmit Mode

Displays the actual speed and duplex mode being used by the management interface.

Public Interface*(when Static IP Address is selected)*

Enter an IP address that is permanently assigned to the public interface to the Pilot.

Pilot CU 0/1

Enter the IP addresses that are permanently assigned to the ports on the CUs in the Pilot. You can use these static IP addresses as an alternate method to access the active Pilot.

Netmask

Enter a subnet mask for the public IP address that is permanently assigned to the Pillar Axiom system.

Gateway

Enter the public IP address of the gateway server in the subnet of which the Pillar Axiom system is a member.

DNS Settings

Primary DNS Server

Enter the Domain Name Server (DNS) that is used to resolve IP addresses.

Secondary DNS Server

Enter the IP address of the secondary DNS server in the network if the primary DNS server cannot be reached.

Related references

- [Pillar Axiom System Limits](#)

Related tasks

- [Configure the Management Interface](#)
- [Modify Asset Information](#)

Modify Network Settings, iSCSI Tab

Navigation: Global Settings > Networking > Actions > Modify Network Settings > iSCSI

Allows you to configure system-wide iSCSI settings if you have iSCSI hosts configured to use Challenge Handshake Authentication Protocol (CHAP), Access Control, Internet Storage Name Service (iSNS), or some combination of these parameters. This configures the authentication and access controls on the Pillar Axiom system, which the host must match to gain access. If you have CHAP and Access Control configured for each initiator, you do not need to configure iSCSI globally.

Connectivity and Communication

iSCSI Device Name

Identifies the name of the iSCSI initiator for the SAN host. An initiator encapsulates SCSI commands and data requests within iSCSI packets and transfers the packets across the IP network.

iSCSI Device Alias

Identifies an easily understood, alternative name for the iSCSI device. By default, the device alias is constructed using the Pillar Axiom model plus the system serial number using the following format:

- Pillar Axiom <model-number> SSN:<serial-number>

Enable Header Digest

When an iSCSI initiator logs in to the Pillar Axiom system, the initiator negotiates the parameters for the iSCSI session. If the initiator does not give the system a choice regarding the use of iSCSI header digests, the system complies with what the initiator wants. If the initiator gives the system a choice and if Enable Header Digest is enabled, the system will choose to use header digests, regardless of the preference identified by the initiator.

Note: When selected, this parameter provides additional error checking for the header portion of the iSCSI packet.

Enable Data Digest

When an iSCSI initiator logs in to the Pillar Axiom system, the initiator negotiates the parameters for the iSCSI session. If the initiator does not give the system a choice regarding the use of iSCSI data digests, the system complies with what the initiator wants. If the initiator gives the system a choice and if Enable Data Digest is enabled, the system will choose to use data digests, regardless of the preference identified by the initiator.

Note: When selected, this parameter provides additional error checking for the data portion of the iSCSI packet.

iSNS Server Registration

Enable iSNS Server Registration

Choosing this option allows Pillar Axiom iSCSI targets to be registered in the iSNS server.

For discovery of the iSNS server IP address, specify either DHCP or static addressing:

Static

This option requires the following information:

Server	Indicates the server IP address.
TCP port	Indicates the TCP port that the Pillar Axiom system uses to register with the iSNS server.

Security

Access Control

Specifies the access control method for iSCSI initiators. Valid options:

None	Specifies that the Pillar Axiom system permits all iSCSI initiators to login.
Axiom	Specifies that the Pillar Axiom system rejects iSCSI login attempts from initiators that have not explicitly been granted permission by the user through the Pillar Axiom Storage Services Manager interface.

Authentication

Identifies the authentication of the host (initiator) during login. Valid options:

All Initiators	Specifies that CHAP authentication is required for all iSCSI connections to the Pillar Axiom system, regardless of what is configured for each host.
Per Initiator	Specifies that CHAP authentication is required only for those iSCSI connections for which it is configured for each host.

Note: If the initiator on the SAN host has been configured to require CHAP authentication, login will fail unless the Pillar Axiom system has been configured to authenticate to All Initiators or authentication has been set to Per Initiator and the Enable Bi-Directional CHAP option has been selected. In either case, specify the CHAP Secret for the initiator.

Authentication Server

Specifies whether the Pillar Axiom system or a Radius server performs the authentication.

Axiom Indicates that the Pillar Axiom system performs the authentication.

Radius Indicates that a RADIUS server performs the authentication.

Note: When this option is selected, the system ignores any CHAP name or secret that is configured for a host in the Pillar Axiom Storage Services Manager.

Enable Bi-Directional CHAP

Enables the CHAP protocol to be used for requests for data (from the iSCSI initiator) and responses to requests (from the iSCSI target). If bi-directional CHAP support is disabled for the Pillar Axiom system, bi-directional CHAP must be disabled for all initiators; otherwise the initiator login will fail.

CHAP Secret

Identifies the encrypted CHAP authentication password (secret) used in the exchange of user names and secrets between two iSCSI devices. Both devices must support Point-to-Point Protocol (PPP) authentication.

Note: The Pillar Axiom system supports up to 100 UTF-8 non-integer characters. However, when connecting to Windows servers, you must limit the secret to a value between 12 and 16 characters in length.

Retype CHAP Secret

Re-enter the encrypted CHAP authentication password used.

Primary Radius Server and Secondary Radius Server

Identifies the details for connecting to the primary and secondary Radius servers. This information is required when the Authentication Server is set to Radius.

IP Address	Specifies the IP address of the Radius server.
UDP Port	Specifies the UDP port of the Radius server to which the Radius server is listening.
Radius Secret	Specifies the secret used to access the Radius server.
Retype Radius Secret	Specifies the retyped secret used to access the primary Radius server.

Related concepts

- [About iSCSI Settings](#)
- [About Licensing Optional Premium Features](#)

Related references

- [Pillar Axiom System Limits](#)

Related tasks

- [Configure iSCSI System Settings](#)
- [Modify a Host: Reconfigure Port Settings](#)

Modify Network Settings, Notification Tab

Navigation: Global Settings > Networking > Actions > Modify Network Settings > Notification

Allows you to configure the electronic mail (email) server that receives email and Call-Home notifications from the Pillar Axiom system and sends the email messages to the designated recipients.

Email Notificatons

Specifies the email server details necessary to send notification from the Pillar Axiom system.

Enable Email Notifications

Identifies whether email is enabled.

- Enable email if you intend to define alerts to send email notifications.
- Disable email if you do not want to send email notifications from the Pillar Axiom system.

SMTP Server IP Address

Identifies the Simple Mail Transfer Protocol (SMTP) server to use for sending any emails. Valid options:

- IP: The IP address for the SNMP server
- DNS: The Domain Name Service (DNS) for the SNMP server

SMTP Server Port

Specifies the port to which the SMTP server listens for incoming email.

Email Domain

Specifies the sending domain identifier other than the Pillar Axiom system.

Call-Home Triggering

Allows you to specify when events logs and messages are sent to the Call-Home server.

Enable event triggered call-home

Enables Call-Home support, which enables the Pillar Axiom system to send status messages to the designated server.

Enable standard periodic Call-Home

Enables the periodic sending of the Pillar Axiom event logs to the Call-Home server.

Start Date	Indicates the time and date when to begin the periodic transfers.	
Interval	Indicates the unit of occurrence at which the system performs the scheduled transfer. Valid options:	
	Daily	Performs the scheduled task on a daily basis.
	Weekly	Performs the scheduled task on a weekly basis.
	Monthly	Performs the scheduled task on a monthly basis.
Recurrence	Indicates the number of intervals to wait before starting the next scheduled Call-Home operation. Enter or select a value from 1 to 100. The default recurrence setting is one week.	

Enable larger periodic Call-Home

Enables large files to be sent to the Call-Home server so that trace logs and performance statistics are automatically included in the Call-Home logs.

Start Date	Indicates the time and date when to begin the periodic transfers.	
Interval	Indicates the unit of occurrence at which the system performs the scheduled transfer. Valid options:	
	Daily	Performs the scheduled task on a daily basis.
	Weekly	Performs the scheduled task on a weekly basis.
	Monthly	Performs the scheduled task on a monthly basis.
Recurrence	Indicates the number of intervals to wait before starting the next scheduled Call-Home operation. Enter or select a value from 1 to 100. The default recurrence setting is 90 days.	

Call-Home Configuration

Specifies the Call-Home server settings. You can configure a Pillar server or a local server to receive the event logs and messages.

Use Pillar Server

Specifies that Call-Home logs and messages should be sent to Pillar Data Systems.

Server Address	Identifies the IP address or the domain name of the Call-Home server, callhome.support.pillardata.com. Valid options: <ul style="list-style-type: none">■ IP: The IP address for the SNMP server■ DNS: The Domain Name Service (DNS) for the SNMP server
Connect via SCP	Specifies the use of secure copy (SCP) with 1024-bit encryption and secure keys to transfer files directly over the Internet to the Oracle Pillar Customer Support.
Connect via HTTPS	Sends files either directly to the Pillar server through a secure Internet connection or to a proxy server.
Use Proxy	Sends Call-Home logs through a proxy server for security purposes or when the Pillar Axiom system does not have direct access to the Internet. Sends Call-Home logs without using a proxy server.
Proxy Server Address	Identifies the DNS server name or IP address of the proxy server.
Proxy Server Port	Identifies the port that is used by the proxy server to send the Call-Home log files.
Protocol	Identifies the type of protocol that is used to access the proxy server. Valid options: Unknown

Use Local Server

Specifies that Call-Home status messages should be sent to a local server by providing the IP address or domain name of the local server.

SCP Server Specifies the use of secure copy (SCP) with 1024-bit encryption and secure keys to transfer files directly over the Internet to the Oracle Pillar Customer Support.

Remote Directory Identifies the full directory path on the target server in which to store the Call-Home log files.

Password Authentication

Specifies that authentication is required to access the local server. Use login credentials or a customer-supplied certificate to authenticate access to the local server.

Username Specifies the name of the user.

Password Specifies the password associated with the username.

Certificate Authentication

Specifies that a customer-supplied certificate is required to authenticate the connection to the local server.

Enable large file transfers

Identifies whether trace logs and performance statistics are included in Call-Home data transfers.

- Enable this option to allow large files so that trace logs and performance statistics are automatically included in the messages that are sent to Oracle Pillar Customer Support.
- Disable this option to exclude trace logs and performance statistics from the Call-Home messages that are sent to Oracle Pillar Customer Support. You can collect, download, and transmit the trace logs separately if they are needed.

Number of recent events to send in header

Specifies the maximum number of system events to be included in the Call-Home status messages. The number of system events should be greater than or equal to zero.

Related references

- [*Pillar Axiom System Limits*](#)

Related tasks

- [*Test Call-Home*](#)
- [*Create a Log Bundle*](#)
- [*Configure Email Notification Settings*](#)
- [*Modify Call-Home Settings*](#)

Modify SAN LUN, Quality of Service Tab

Navigation: Storage > SAN > LUNs > Actions > Modify LUN > Quality of Service

Allows you to update the capacity and performance settings for a LUN of any type (source, clone, or copy).

Selected Storage Class Capacity

Displays the storage capacity of the selected storage class and Storage Domain that is available for the LUN. The graph uses colored bars of different thicknesses to indicate the capacity status of the logical volume you are creating as well as the overall system capacity.

- Solid Green (thin): Indicates the allocated and growth potential capacity for the volume.
- Solid Blue (thick): Indicates the allocated and used capacity for the volume in the selected Storage Domain and storage class, including the impact of the current volume.
- Shaded Gray (thick): Indicates the growth potential for the selected Storage Domain and storage class, including the impact of the current volume.
- Dark Gray (thick): Indicates the available (free) capacity in the selected Storage Domain and storage class, including the impact of the current volume.
- Shaded Red (thick): Indicates the growth potential that cannot be satisfied for the volume in the selected Storage Domain and storage class, including the impact of the current volume.

System Capacity By Storage Class

Displays the storage capacity in use by the selected Storage Domain and that is in use by each media type configured in the system:

- System
- SSD SLC (solid state drive, single-level cell)
- FC (Fibre Channel)
- SATA (serial ATA)

Storage Domain

Allows you to assign the LUN to an existing Storage Domain.

[...]

Opens the dialog that allows you to review the physical capacity attributes and the Brick types that are associated with the predefined Storage Domains.

Note: The Storage Domain Details button appears when more than one Storage Domain exists.

Volume Name

Identifies the name that is assigned to a LUN for administrative purposes. LUN names must be unique across the Pillar Axiom system and must be 82 or fewer UTF characters, or 255 or fewer ASCII characters.

Volume Group

Allows you to assign the LUN to an existing volume group.

[...]

Opens the dialog that allows you to create new Volume Groups.

Storage Profile

Identifies the set of QoS attributes applied to the LUN.

[...]

Opens the View Storage Profiles dialog that allows you to review the profile details.

Recommended Storage Class

Displays the recommended storage class based on the Storage Profile selection.

Storage Class

Identifies the category of physical media on which the logical volume resides: Valid types:

- SATA
- FC
- SSD SLC (solid state drive, single-level cell)

Typical Access

Identifies the most common method of data access. Valid options:

Sequential

Read and write requests from client applications tend to request operations on the data one record after the other.

Random	Read and write requests from client applications tend to request operations on the data records in an arbitrary order.
---------------	--

Mixed	Read and write requests from client applications tend to mix the request operations on the data sometimes in sequential and sometimes in random order.
--------------	--

I/O Bias

Identifies the typical read-write ratio. Valid options:

Read	Most requests from client applications are for <code>read</code> operations.
-------------	--

Write	Most requests from client applications are for <code>write</code> operations.
--------------	---

Mixed	Requests from client applications are likely equal for <code>read</code> and <code>write</code> operations.
--------------	---

Redundancy

Identifies how many mirror copies of the original data are stored in the storage pool. Valid options:

Standard	Stores original data only. Data striping over multiple RAID groups maintains full redundancy, even without mirror copies.
-----------------	---

Double	Stores original data and one mirror copy, with data striping over multiple RAID groups.
---------------	---

Priority Level

In addition to determining the placement of data onto specific areas of the drive platters relative to the drive spindles, the priority level of a volume determines the processing *queue priority* for that volume. Queue priority defines the percentage of Slammer CPU cycles that are dedicated to the volume.

Valid options:

Premium	Highest processing queue priority. Striping occurs across eight serial ATA (SATA) RAID groups or four Fibre Channel (FC) RAID groups on the outermost 20% of the drive platters.
----------------	--

High	Next highest processing queue priority. Striping occurs across eight SATA RAID groups or four FC RAID groups on the outermost 20-40% of the drive platters.
Medium	Intermediate processing queue priority. Striping occurs across six SATA RAID groups or three FC RAID groups on the outermost 40-60% of the drive platters.
Low	Next to lowest processing queue priority. Striping occurs across four SATA RAID groups or two FC RAID groups on the outermost 60-80% of the drive platters.
Archive	Lowest processing queue priority. Striping occurs across four SATA RAID groups or two FC RAID groups on the outermost 80-100% of the drive platters.

Background Copy Priority

Identifies the strategy the system should use to control the impact on performance when background tasks need to copy or move data from one location in the storage pool to another.

Note: When the system is idle or lightly loaded, the above background task maximizes the amount of work done regardless of the option selected.

Valid options:

System Chooses	Balances the background copy with the incoming client I/O. This option is the default.
Minimize Impact	Restricts the amount of work performed on a loaded system. This option is intended to have a minimal impact on client I/O throughput at the expense of longer copy times.
Maximum Speed	Prioritizes the background copy at the expense of client I/O throughput.

The following types of operations are affected by the strategy you select:

- Copy
- Restore
- Quality of Service (QoS) changes in:
 - Priority
 - Redundancy
 - Storage Class

Allocated Logical Capacity

Identifies the amount of capacity to be allocated to the logical volume.

Addressable Logical Capacity

Identifies the maximum capacity to which the logical volume can grow. For a clone, this field identifies how much addressable space will be available.

Physical Capacity

Provides an estimate of the physical storage capacity requirements, which are based on your QoS attribute selections.

Estimated Physical Capacity	Identifies the estimated physical capacity (allocated and maximum) for this LUN.
Estimated Clone Capacity	Identifies the estimated capacity (allocated and maximum) for clones of this LUN.
Estimated Total Capacity	Identifies the estimated total capacity (allocated and maximum) for this LUN.

Related concepts

- [About Modifying LUNs](#)
- [About Priority Levels](#)
- [About Redundancy](#)
- [About I/O Bias](#)
- [About Access Bias](#)
- [About Storage Classes](#)

Related references

- [Effects of Access Bias and I/O Bias](#)
- [Pillar Axiom System Limits](#)

Related tasks

- [Modify a LUN: Define Quality of Service](#)

Modify SAN LUN, Mapping Tab

Navigation: Storage > SAN > LUNs > Actions > Modify LUN > Mapping

Allows you to modify the LUN-to-host mapping settings for a LUN.

Access Protocol

Valid options:

- Fibre Channel (FC): Specifies that hosts can use the FC protocol to access this LUN.
Tip: FC paths will always be used at a preference over iSCSI paths. Also, load balancing will not be mixed between these two protocols.
- iSCSI: Specifies that hosts can use the iSCSI protocol to access this LUN.

Only selected hosts (via maps)

Specifies that only designated SAN hosts can access this LUN using a specific, possibly different, LUN number on each of those hosts. If the LUN is mapped, the LUN number must be unique to the mapped SAN host.

All hosts may access this LUN using LUN Number

Specifies all SAN hosts accessing this LUN use the same LUN number. Select this option to activate the LUN number selection drop-down list.

Available LUN Number

You can map a LUN or Clone LUN to either a single host or a host group.

LUN Slammer Control Unit Assignment

Current Slammer CU

Identifies the current Slammer CU on which the LUN is currently homed.

Note: For new source LUNs, this field is not available; instead, use Assigned Slammer CU.

Assigned Slammer CU <Auto-Assign>

Identifies the Slammer CU to which the system should assign the LUN. Available options:

<auto assign>

Select this option if you want the system to determine the Slammer CU.

Slammer CU Select a specific Slammer CU from the list to assign to the LUN.

Ports Masked for this LUN

Displays the physical Slammer ports to exclude (mask) so they cannot access the LUN.

Masked

Indicates whether the port for the LUN is masked.

Protocol

Identifies the type of access protocol, FC or iSCSI.

Slammer

Identifies the name of the Slammer.

CU

Identifies the control unit (CU) of the Slammer.

Port

Identifies the name of the Slammer CU port.

Slammer Port Address

Identifies the unique identifier of each Slammer network port. For FC networks, this identifier is the World Wide Name (WWN). For iSCSI networks, this identifier is the Media Access Control (MAC) address.

LUN Mapping

Note: The LUN mapping table only displays when you select the **Only selected hosts (via maps)** option.

Hosts Mapped to this LUN

Name	Identifies the SAN host that accesses LUNs configured on the Pillar Axiom system. If the Pillar Axiom Path Manager is not installed, the system displays the WWN of the FC HBA or the IP address of the iSCSI device.
Map via LUN #	Identifies the number to assign to the LUN for the associated SAN host. This number must be unique for that particular host. It need not be unique across all hosts.

Port Status by CU:Port	Identifies a masked physical Slammer port. A port mask prevents the LUN from being accessed from this port. Masked ports are depicted by a blue mask icon, while unmasked ports are identified with a light gray and white mask.
-------------------------------	--

Create

Opens the dialog that allows you to create the LUN-to-host mapping based on your selections for host name and the LUN number to be used by that host.

Modify

Opens the dialog that allows you to change the LUN mapped to the associated host.

Remove

Removes the LUN mapping for the selected SAN host.

Related concepts

- [About Modifying LUNs](#)
- [About Licensing Optional Premium Features](#)

Related references

- [Connection Status of Slammer Ports](#)
- [Pillar Axiom System Limits](#)

Related tasks

- [Modify LUN: Define Mapping by Selected Hosts](#)

Modify SAN LUN, Data Protection Tab

Navigation: Storage > SAN > LUNs > Actions > Modify LUN > Data Protection

Allows you to view and modify the storage capacity of a Clone LUN. You can also manage Clone LUN replication schedules from this page.

Selected Storage Class Capacity

Displays the storage capacity of the selected storage class and Storage Domain that is available for the LUN. The graph uses colored bars of different thicknesses to indicate the capacity status of the logical volume you are creating as well as the overall system capacity.

- Solid Green (thin): Indicates the allocated and growth potential capacity for the volume.
- Solid Blue (thick): Indicates the allocated and used capacity for the volume in the selected Storage Domain and storage class, including the impact of the current volume.
- Shaded Gray (thick): Indicates the growth potential for the selected Storage Domain and storage class, including the impact of the current volume.
- Dark Gray (thick): Indicates the available (free) capacity in the selected Storage Domain and storage class, including the impact of the current volume.
- Shaded Red (thick): Indicates the growth potential that cannot be satisfied for the volume in the selected Storage Domain and storage class, including the impact of the current volume.

Clone LUNs Capacity

Maximum capacity (in GB) to allocate for Clone LUNs

Specifies the maximum amount of space to make available on the Storage Domain on which the copy of the clones will reside.



Pillar strongly recommends that you allocate sufficient repository capacity to minimize the chances of running out of this space (which could lead to data inconsistency or loss). To set sufficient capacity, use a value equal to the source volume capacity times the number of replicas times the maximum rate of change. For example, for a 100 GB volume that is projected to have 20 active replicas at a time and no more than a 20% rate of change, use a value of 400 GB for the clone repository.

Number of existing Clone LUNs

Specifies the number of clones that have been created for this LUN and its clones.

Available capacity for Clone LUNs

The amount of current storage capacity allocated for clones of this LUN.

Clone Schedules**Name**

Specifies the name of the replication schedule.

Start Time

Specifies the date and time to begin scheduling replication.

Frequency

Specifies the frequency at which the scheduled replication runs. Frequencies include:

- Run Once
- Hourly
- Daily
- Weekly

Enabled

Specifies whether the scheduled replication is enabled.

Enabled

Indicates that the scheduled event performs at the specified time.

Disabled

Indicates that the operation will not perform as scheduled. Disable the schedule, for example, when the source volume (LUN or Clone LUN) has not been made available to users.

Create

Displays a dialog to create a new replication schedule.

Modify

Displays a dialog to modify an existing replication schedule.

Delete

Removes an existing replication schedule.

Related concepts

- [About Modifying LUNs](#)

Related references

- [Pillar Axiom System Limits](#)

Related tasks

- [Modify LUN: Define Data Protection](#)
- [Create a Clone LUN Schedule](#)
- [Modify a LUN Data Protection Schedule](#)
- [Delete a LUN Data Protection Schedule](#)

Modify Security Settings Dialog

Navigation: Global Settings > Security > Actions > Modify Security Settings

Allows you to set the various account security properties and the login welcome message.

Account Security

Consecutive failed login attempts allowed

Identifies the number of times that an administrator can attempt, and fail, to log in to the Pillar Axiom system. When the number of failed login attempts exceeds this limit, the system locks out the account. Only the Primary system administrator and administrators having the role of Administrator 1 can unlock the account.

Session timeout period (in minutes) for all administrators

Identifies an inactivity time limit, after which an administrator session is terminated. Sessions in progress continue to use the previous value and are not affected by changes that you make. Sessions that start after you change the value use the modified session time-out value.

The default for the session time-out is 999 minutes.

After an administrator logs in, if the administrator is inactive for a length of time equal to the session time-out period, the Pillar Axiom system automatically logs the account out of the system.

The session time-out period applies only to property dialogs and popup windows in the Pillar Axiom Storage Services Manager. The session time-out period does not apply to the main window because of activity that occurs to verify the system status and health.

Login Screen Message

Specifies a message that is displayed when system administrators log in to the Pillar Axiom system. You can enter up to 256 Unicode characters.

Related references

- [Pillar Axiom System Limits](#)

Related tasks

- [Modify Security Settings](#)
- [Modify an Administrator Account](#)

Modify SNMP Host Dialog

Navigation: Global Settings > SNMP > Actions > Modify SNMP Host

Allows you to modify Simple Network Management Protocol (SNMP) trap hosts.

Name

Identifies the name for the SNMP host.

Host IP

Identifies the IP address or domain name of a client that receives the Pillar Axiom SNMP information.

Community String

Identifies the community string for use when the Pillar Axiom system sends an event trap to the SNMP host.

Note: When an administrator does not specify a community string for read-only access, SNMP servers and clients will typically use `public`.

Receive traps

Indicates that the SNMP host receives event traps sent to it.

Trap Port Number

Identifies the SNMP host port number to use for sending an event trap.

Severity Threshold

Identifies the severity threshold for events that are to be sent to the SNMP host by event traps.

Severity levels:

- **Informational**
- **Warning**
- **Critical**

Related concepts

- [*About Licensing Optional Premium Features*](#)

Related references

- [*Pillar Axiom System Limits*](#)

Related tasks

- [*Create SNMP Hosts*](#)
- [*Modify SNMP Hosts*](#)
- [*Delete SNMP Hosts*](#)

Modify System Time Dialog

Navigation: Global Settings > System Time > Actions > Modify System Time

Allows you to synchronize the Pillar Axiom clock time with a Network Time Protocol (NTP) server or to set the date and time manually.

Use External Time Source

Identifies that the Pillar Axiom system synchronizes its clocks with Network Time Protocol (NTP) servers.

- Enable NTP if you want to specify a primary NTP server and up to two alternate NTP servers with which the system synchronizes its clocks.
- Disable NTP if you want to manually set the date and time for the Pillar Axiom system.

NTP Server 1, 2, and 3

Identifies the IP addresses that are assigned to the primary and alternate NTP servers with which the Pillar Axiom system synchronizes its clocks. Select the DNS from the drop-down to enter a fully qualified server name.

If the primary NTP server is unavailable, the system consults the alternate servers in round-robin fashion until the Pillar Axiom system connects to an available NTP server. Enter IP addresses or DNS names for up to two alternate NTP servers.

Use Internal Hardware Clock

Identifies that the Pillar Axiom system synchronizes its clocks with a date and time that you set manually. Pillar Axiom clocks are synchronized with each other, and their time may differ from other clocks in your network.

Date/Time

Presents a wizard that allows you to set the Pillar Axiom date and time manually. The time that you set is converted internally to the Coordinated Universal Time (abbreviated UTC) format.

Related references

- [Pillar Axiom System Limits](#)

Related tasks

- [Modify the Pillar Axiom System Time](#)
- [Configure Email Notification Settings](#)

Networking Overview Page

Navigation: Global Settings > Networking

Allows you to review the settings for Pillar Axiom networking properties.

Management Interface

DHCP Enabled

Identifies whether Dynamic Host Configuration Protocol (DHCP) is enabled.

IP Address

Identifies the public IP address that is assigned to the Pilot. This IP address is what the administrator uses to access the Pillar Axiom Storage Services manager over the management interface.

Subnet Mask

Identifies the subnet mask for the public IP address that is permanently assigned to the Pilot.

Gateway

Identifies the IP address of the gateway server in the subnet of which the Pillar Axiom system (the Pilot) is a member.

MAC Address

The MAC identifier represents the MAC address of the *active* Pilot control unit (CU). In the event that a Pilot CU fails, the passive CU becomes the active CU. The MAC ID changes to the MAC address of the formerly passive CU.

Transmit Mode

Identifies the actual port speed and duplex mode at which the management interface is running.

DNS Settings

Primary DNS Server

Identifies the IP address of the primary Domain Name Server (DNS) that is used to resolve the IP addresses.

Secondary DNS Server

Identifies the IP address of the secondary DNS server that should be used if the primary DNS server cannot be reached.

Notification

Email Enabled

Identifies whether email is enabled to notify recipients of system events.

Email Server IP

Identifies the IP address of the Simple Mail Transfer Protocol (SMTP) server that receives system event notifications.

Email Server Port

Identifies the port that the SMTP server listens to for incoming email requests.

Event Triggered

Indicates whether event-triggered Call-Home is enabled.

Standard Periodic

Indicates whether standard Call-Home messages are scheduled and enabled.

Larger Periodic

Indicates whether larger Call-Home messages are scheduled and enabled.

Large Files

Indicates whether large files are sent to the Call-Home server.

iSCSI Connectivity and Communication

Device Name

Identifies the name of the iSCSI initiator for the SAN host. An initiator encapsulates SCSI commands and data requests within iSCSI packets and transfers the packets across the IP network.

Device Alias

Identifies an easily understood, alternative name for the iSCSI device. By default, the device alias is constructed using the Pillar Axiom model plus the system serial number using the following format:

- Pillar Axiom <model-number> SSN:<serial-number>

Header Digest

Identifies that the system is using iSCSI header digests.

Data Digest

Identifies that the system is using iSCSI data digests.

iSNS Settings

iSNS Server Registration

Identifies whether the Pillar Axiom iSCSI targets are registered in the iSNS server.

iSCSI Security

Access Control

Specifies that the Pillar Axiom system rejects iSCSI login attempts from initiators that have not explicitly been granted permission by the user through the Pillar Axiom Storage Services Manager interface or Pillar Axiom command line interface (CLI).

Authentication

Identifies the authentication of the host (initiator) during login.

Authentication Server

Indicates the server name used to authenticate the iSCSI requests.

Bi-directional CHAP Enabled

Identifies the status of the CHAP protocol for data requests (from the iSCSI initiator) and request responses (from the iSCSI target).

Related references

- [*Modify Network Settings, Notification Tab*](#)
- [*Pillar Axiom System Limits*](#)

Related tasks

- [*Configure the Management Interface*](#)
- [*Modify Asset Information*](#)

SAN Hosts Overview Page

Navigation: Storage > SAN > Hosts

Allows you to review the storage area network (SAN) hosts defined on a Pillar Axiom 600 system. Actions from this page allow you to manage the host on the system.

Host

Identifies the SAN host information. Valid options:

Host Name	Identifies the name of the SAN host.
Number of LUNs Mapped	Identifies the number of LUNs that are mapped to that particular SAN host either because of specific mapping or because the LUN is available to all SAN hosts.

Pillar Axiom Path Manager

Identifies certain global characteristics associated with the Pillar Axiom Path Manager (APM). Valid options:

Status	Identifies whether or not the APM driver is communicating, or if it is not registered. If the driver is not registered, install a path manager, such as the Pillar Axiom Path Manager.
Version	Identifies the version of the APM host driver, if it has been installed, that is running on the SAN host.
Host IP Address	Identifies the IP address of the SAN host. The system uses this address to exchange management requests and responses with the Pillar Axiom Path Manager (APM) that is installed on the host. If APM is not installed, this field displays <i>N/A</i> .

HBA

HBA Alias Name	Identifies the HBA alias name.
-----------------------	--------------------------------

Slammer Port by CU:Port

Identifies the connection status of each SAN Slammer port.

Related references

- [*Connection Status of Slammer Ports*](#)
- [*Pillar Axiom System Limits*](#)

Related tasks

- [*Display SAN Host Settings*](#)
- [*Modify a Host: Reconfigure Port Settings*](#)
- [*Delete a SAN Host Entry*](#)
- [*Associate a SAN Host*](#)
- [*Create LUN: Define Mapping by Selected Hosts*](#)

SAN LUNs Overview Page

Navigation: Storage > SAN > LUNs

Allows you to review the LUN and Clone LUN properties that have been defined on the Pillar Axiom system. Action on this page allow you to manage those LUNs as well as to create an immediate Clone LUN.

Name

Identifies the name that is assigned to a LUN for administrative purposes.

Status

Identifies the current status of each LUN. Valid types:

Online	Indicates that the LUN is fully accessible.
Offline	Indicates that the LUN is not accessible.
Inactive	Indicates that the LUN cannot be accessed from the data path.
Partial Offline	Indicates that the actual redundancy level may be different from the redundancy level with which the volume was configured.
Degraded	Indicates that all of the copies of a redundant volume are not available. If one copy is missing, it is not fully redundant. This can happen when a write to one copy of the array fails (which may be a 30 second time-out).
Conservative	Indicates that write-back cache has been disabled so journaling has slowed.

Host Access

Identifies the SAN host mapping status associated with the LUN. Valid types:

- Mapped
- No Mappings
- Inactive
- All

Protocol Access

Identifies the access protocol used to map the LUN to the Slammer.
Protocols include:

- FC only
- iSCSI only
- No Access
- All

Groups

Displays which volume group or storage domain to which the logical volumes belongs.

Volume Group	Lists the name of the volume group where the logical volume is located.
---------------------	---

Storage Domain	Specifies the name of the Storage Domain.
-----------------------	---

Logical Capacity (GB)

Displays the storage requirements for the logical volumes.

Allocated	Identifies the initial capacity that is assigned to the logical volume. This value is a soft limit, which means that data can be stored in a logical volume until the maximum capacity is reached.
------------------	--

Addressable	Identifies the maximum capacity to which the logical volume can grow. For a clone, this field identifies how much addressable space will be available.
--------------------	--

Logical Distribution	Identifies a graphical representation of the initial capacity that is assigned to the logical volume. This value is a soft limit, which means that data can be stored in a logical volume until the maximum capacity is reached.
-----------------------------	--

Capacity (GB) for Clone LUNs

Displays the physical storage usage for the Clone LUNs.

Logical Maximum	Identifies the amount of storage that was requested for the clone repository.
------------------------	---

Physical Used	Identifies the current volume capacity usage of the object.
----------------------	---

Physical Allocated	Identifies the total amount of storage capacity that is reserved on the system.
---------------------------	---

Physical Maximum	Identifies the maximum capacity to which the logical volume can grow. For clones, this field identifies how much addressable space is available.
-------------------------	--

Total Physical Capacity (GB)

Displays the total physical storage capacity for the logical volumes and Clone LUNs.

Redundancy	Identifies how many mirror copies of the original data are stored online.
-------------------	---

Disk Protection	Indicates the RAID drive data protection method.
------------------------	--

LUN Overhead	Identifies the physical and logical storage capacity that is required to meet the LUN Quality of Service (QoS) settings.
---------------------	--

Allocated	Specifies the amount of raw capacity in gigabytes (GB) that has been assigned and designated to this logical volume.
------------------	--

Maximum	Identifies the maximum capacity for the volume group. The maximum capacity of the logical volumes and nested volume groups that are associated with the volume group cannot exceed this value. A value of 0 (zero) identifies that the volume group is configured with unlimited capacity. You can increase the maximum capacity of associated logical volumes and nested volume groups without constraints.
----------------	--

Physical Distribution	A graphical representation of the capacity used compared to the maximum allocated.
------------------------------	--

Priority Level

Identifies the assigned priority level when the volume was created.

- Premium
- High
- Medium

- Low
- Archive

Global LUN Number

Identifies the globally unique identifier of the LUN.

LUID

Identifies the unique identifier of the LUN.

Related concepts

- [*About Creating LUNs*](#)

Related references

- [*Pillar Axiom System Limits*](#)

Related tasks

- [*Create LUN: Define Quality of Service*](#)
- [*Display LUN Details*](#)
- [*Modify a LUN: Define Quality of Service*](#)
- [*Delete a LUN*](#)
- [*Copy a LUN*](#)
- [*Create an Immediate Clone LUN*](#)
- [*Enable the Data Path of a LUN*](#)
- [*Disable the Data Path of a LUN*](#)

SAN Slammer Ports Overview Page

Navigation: Storage > SAN > Slammer Ports

Allows you to review the topology of the network ports on each of the SAN Slammer control units (CUs).

Slammer

Identifies the name of the SAN Slammer.

Control Unit

Identifies a SAN Slammer CU.

Network Interface

Identifies the physical port on the CU.

Port Type

Identifies the type of host interface, Fibre Channel (FC) or Internet SCSI (Small Computer System Interface) (iSCSI).

FC Port Information

WWN	Identifies the unique identifiers of the host bus adapter (HBA) ports that the Pillar Axiom system detects on the network. For FC networks, this identifier is the World Wide Name (WWN). For iSCSI networks, this identifier is the Media Access Control (MAC) address.
MAC Address	

Topology	Identifies the Fibre Channel (FC) transport topology in use by the ports in the network interface module (NIM) to connect to the storage area network (SAN) employed by the customer:
-----------------	---

Fabric	Indicates that the port is an N_Port in a switched fabric (FC-SW).
Loop	Indicates that the port is an NL_Port in an arbitrated loop (FC-AL).
Point-to-Point	Indicates that the port is an N_Port that is connected to another

	N_Port, back to back (FC-P2P).
Public Loop	Indicates that the port is an NL_Port that is connected to a loop in which one port in the loop is an FL_Port in the fabric (FC-FLA). Note: The topology used by the Storage System Fabric (SSF) between the Slammers and the Bricks is private and not reported.

iSCSI Port Information

IP Address	Identifies the IP address of the iSCSI SAN Slammer ports that the Pillar Axiom system detects on the network.
Vlan Enabled	Signifies whether a virtual LAN (VLAN) has been defined for the iSCSI network.
Vlan ID	Identifies the group portal tag number.
Target Portal Group Tag	Identifies the group of iSCSI target ports through which connections for a single session can be made. This allows an iSCSI target to designate multiple ports that can have connections within a single session.

Network Link

Negotiated Link Speed	Displays the transmission speed of the port. Depending on the port type, the speed is reported in megabits per second or gigabits per second.
Medium Type	Identifies the types of network ports for data path traffic between the customer network switches and the Pillar Axiom SAN Slammers: <ul style="list-style-type: none">■ Copper: Identifies RJ-45 copper interfaces.

- **Long Wave Optical:** Identifies longwave optical, small form-factor pluggable (SFP) transceiver interfaces.
- **Short Wave Optical:** Identifies shortwave optical SFP transceiver interfaces.

Related tasks

- [*Modify iSCSI Port Settings*](#)

SAN Storage Overview Page

*Navigation: **Storage** > **SAN***

Allows you to review the logical units (LUNs) and storage area network (SAN) hosts that are configured on the Pillar Axiom system.

LUNs

Allows the administrator to create, view, and modify a logical volume within a SAN. Administrators assign storage resources and Quality of Service (QoS) attributes to each LUN.

Hosts

Allows the administrator to create, view and modify the SAN clients that expose the block-based storage provided by LUNs as filesystems and shares.

Slammer Ports

Allows the administrator to modify certain aspects of the network ports on the Slammer control units.

Hosts to LUN Map

Provides a topology overview of the hosts and associated mapped LUNs.

LUN to Host Map

Provides a topology overview of the LUNs and associated mapped hosts.

Related tasks

- [*Create LUN: Define Quality of Service*](#)
- [*Display LUN Details*](#)
- [*Modify a LUN: Define Quality of Service*](#)
- [*Copy a LUN*](#)
- [*Delete a LUN*](#)
- [*Create LUN: Define Mapping by Selected Hosts*](#)

Security Settings Overview Page

Navigation: Global Settings > Security

Allows you to review the security configuration for administrator accounts.

Account Security

Consecutive failed login attempts allowed

Identifies the number of times that an administrator can attempt, and fail, to log in to the Pillar Axiom system. When the number of failed login attempts exceeds this limit, the system locks out the account. Only the Primary system administrator and administrators having the role of Administrator 1 can unlock the account.

Session timeout period (in minutes) for all administrators

Identifies an inactivity time limit, after which an administrator session is terminated. Sessions in progress continue to use the previous value and are not affected by changes that you make. Sessions that start after you change the value use the modified session time-out value.

The default for the session time-out is 999 minutes.

After an administrator logs in, if the administrator is inactive for a length of time equal to the session time-out period, the Pillar Axiom system automatically logs the account out of the system.

The session time-out period applies only to property dialogs and popup windows in the Pillar Axiom Storage Services Manager. The session time-out period does not apply to the main window because of activity that occurs to verify the system status and health.

Login Screen Message

Specifies a message that is displayed when system administrators log in to the Pillar Axiom system. You can enter up to 256 Unicode characters.

Related references

- [Modify Security Settings Dialog](#)
- [Pillar Axiom System Limits](#)

Related tasks

- [Modify Security Settings](#)
- [Modify an Administrator Account](#)

SNMP Hosts Overview Page

Navigation: Global Settings > SNMP

Allows you to review whether the Simple Network Management Protocol (SNMP) software feature is enabled and to manage the SNMP hosts when the feature is enabled. This page provides options to modify the SNMP settings and to delete SNMP hosts.

Name

Identifies the name for the SNMP host.

Authorized Host IP

Identifies the IP address or domain name of a client that receives the Pillar Axiom SNMP information.

Community String

Identifies the community string for use when the Pillar Axiom system sends an event trap to the SNMP host.

Note: When an administrator does not specify a community string for read-only access, SNMP servers and clients will typically use `public`.

Receives Traps

Indicates that the SNMP host receives event traps sent to it.

Related concepts

- [About Licensing Optional Premium Features](#)

Related references

- [Pillar Axiom System Limits](#)

Related tasks

- [Create SNMP Hosts](#)
- [Modify SNMP Hosts](#)
- [Delete SNMP Hosts](#)

Storage Domains Overview Page

Navigation: Groups > Storage Domains

Describes the properties of each Storage Domain defined on this Pillar Axiom system.

Name

Specifies the name of the Storage Domain and the names of the logical volumes assigned to the domain.

Hardware

Status

Indicates the operating condition of each logical volume contained within a Storage Domain:

Conservative	Write-back cache has been disabled so journaling has slowed.
Degraded	All of the copies of a redundant volume are not available. If one copy is missing, it is not fully redundant. This can happen when a write operation to one copy of the array fails (which may be a 30 second time-out).
Inactive	Cannot be accessed from the data path.
Offline	Not accessible.
Online	Fully accessible.
Partial Offline	The actual redundancy level may be different from the redundancy level with which the clone was configured.

Primary

Indicates whether this Storage Domain is the primary Storage Domain.

Number of Bricks

Specifies the number of Bricks that are dedicated to this Storage Domain.

Storage Domain Physical Capacity

Allocated

Displays the amount of raw capacity, in gigabytes (GB), that has been assigned and designated to all logical volumes residing on the indicated Storage Domain.

Free

Displays the amount of raw capacity (in GB) that is available for allocation in the indicated Storage Domain.

Unavailable

Displays the amount of raw capacity (in GB) that is currently being initialized. This value typically results from a volume having been deleted. This value decreases over a period of time while the value for free capacity correspondingly increases for the indicated Storage Domain.

Total Capacity

Displays the total amount of raw capacity (in GB) provided by the Bricks defined within the indicated Storage Domain.

LUN Physical Capacity**Used**

Specifies the amount of raw capacity (including parity overhead), in gigabytes (GB), that is consumed by this logical volume.

Allocated

Specifies the amount of raw capacity (including parity overhead), in gigabytes (GB), that has been assigned and designated to this logical volume.

Maximum

Identifies the maximum capacity to which the logical volume can grow. For a clone, this field identifies how much addressable space will be available.

Priority Level

Identifies the layout of data that is stored in the Pillar Axiom system. This layout has one of the following settings:

- | | |
|----------------|--|
| Premium | Highest processing queue priority. Striping occurs across eight serial ATA (SATA) RAID groups or four Fibre Channel (FC) RAID groups on the outermost 20% of the drive platters. |
| High | Next highest processing queue priority. Striping occurs across eight SATA RAID groups or four FC RAID groups on the outermost 20-40% of the drive platters. |

Medium	Intermediate processing queue priority. Striping occurs across six SATA RAID groups or three FC RAID groups on the outermost 40-60% of the drive platters.
Low	Next to lowest processing queue priority. Striping occurs across four SATA RAID groups or two FC RAID groups on the outermost 60-80% of the drive platters.
Archive	Lowest processing queue priority. Striping occurs across four SATA RAID groups or two FC RAID groups on the outermost 80-100% of the drive platters.

Related concepts

- [*About Storage Domains*](#)
- [*About Primary Storage Domains*](#)

Related tasks

- [*Create a Storage Domain*](#)
- [*Delete a Storage Domain*](#)
- [*Modify a Storage Domain*](#)
- [*Move a Volume to Another Storage Domain*](#)
- [*Reassign a Brick to Another Storage Domain*](#)

Storage Overview Page

*Navigation: **Storage***

Allows you to select SAN and Storage Profile information for the Pillar Axiom system.

A Storage Profile is a set of predefined Quality of Service (QoS) attributes that can be used to configure a logical volume. A collection of Storage Profiles that are optimized for specific uses within an application context are available on the Pillar Axiom system.

SAN

Opens the SAN overview page where you can access options to manage LUNs, SAN Hosts, Slammer ports, and view LUN-to-Host mappings.

Storage Profiles

Opens the Manage Storage Profile overview page where you can create and manage Storage Profiles.

Note:

Working with Storage Profiles is recommended for advanced users.

Related references

- [SAN Storage Overview Page](#)
- [Manage Storage Profiles Overview Page](#)

Usage Overview Page

Navigation: [Summary](#) > [Usage](#)

Displays capacity usage details for the Pillar Axiom system, for each Storage Class, and for each volume group.

Note: A Pillar Axiom system uses binary units to calculate and display the capacity of physical storage and the size of logical volumes:

1 MB = 1024^2 (1,048,576) bytes

1 GB = 1024^3 (1,073,741,824) bytes

1 TB = 1024^4 (1,099,511,627,776) bytes

Usage Graphs

Two usage graphs are displayed: one for the entire storage pool in the Pillar Axiom system and the other for the individual types of media (Storage Classes).

Allocated	Identifies the total amount of storage capacity that is reserved on the system or Storage Class.
Free	Identifies the storage capacity that is currently unassigned and available on the system or Storage Class. Free capacity is the total capacity minus the allocated capacity.
Unavailable	Identifies the amount of storage capacity that is in the process of being released back to the storage pool.

Volume Groups with Capacity Limits

A usage graph for each administrator-defined volume group is displayed. Refer to the above descriptions for Allocated, Free, and Reconditioning.

Related concepts

- [Volume Capacity and Provisioning Overview](#)
- [Capacity Overhead](#)

Related references

- [Pillar Axiom System Limits](#)

Related tasks

- [Display Capacity Usage](#)

Summary Overview Page

*Navigation: **Summary***

Allows you to select usage and system information for the Pillar Axiom system.

Usage

Allows you to review the storage capacity details for the Pillar Axiom system.

System

Allows you to review or modify the asset information for the Pillar Axiom system.

Related references

- [*Usage Overview Page*](#)
- [*System Summary Page*](#)

System Summary Page

Navigation: Summary > System

Allows you to review system status and configuration for the Pillar Axiom system.

Name

Identifies the name that is assigned to the Pillar Axiom system. The system name also appears in the status bar.

Description

Displays the system description as defined by the system administrator.

Model

Displays the model number of Pillar Axiom system.

Status

Displays the overall health status of the Pillar Axiom system.

Slammers

Displays the number and type of Slammers installed in the system.

Bricks

Displays the number and type of Bricks installed in the system.

Manufacturer

Displays the manufacturer of the Pillar Axiom system.

Location

Displays the system location as defined by the system administrator.

Contact Name

Displays the primary contact person as defined by the system administrator.

Contact Phone

Displays the primary contact phone number as defined by the system administrator.

Asset Number

Displays the system asset number as defined by the system administrator.

Serial Number

Identifies the system serial number (SSN) that is assigned to the Pillar Axiom system.

IP Address

Identifies the public IP address of the Pillar Axiom management interface. This interface provides access to the Pillar Axiom Storage Services Manager.

MAC Address

Identifies the Media Access Control (MAC) address of the currently active Pilot control unit.

Software Version

Identifies the software version of the graphical user interface (GUI) used to administer the system.

Related concepts

- [*About Responding to System Alerts*](#)
- [*About Licensing Optional Premium Features*](#)

Related references

- [*Hardware Overview Page*](#)
- [*System Alerts Overview Page*](#)
- [*Status Bar Description*](#)

Related tasks

- [*Modify the Pillar Axiom System Time*](#)
- [*Create a Pillar Axiom Administrator Account*](#)
- [*Create an Event Notification*](#)
- [*Create SNMP Hosts*](#)
- [*Modify Asset Information*](#)

System Time Overview Page

Navigation: [Global Settings](#) > [System Time](#)

Allows you to view the system time and to review any Network Time Protocol (NTP) servers with which the system clock is synchronized.

System Time

Identifies the current Pillar Axiom date, time, and time zone.

NTP Servers

Identifies whether the Pillar Axiom system synchronizes its clocks with:

- Network Time Protocol (NTP) servers
- A manual time setting that you specify

Related concepts

- [About Responding to System Alerts](#)

Related tasks

- [Modify the Pillar Axiom System Time](#)
- [Create a Pillar Axiom Administrator Account](#)
- [Create an Event Notification](#)
- [Create SNMP Hosts](#)
- [Modify Asset Information](#)

View Account Dialog

Navigation: Global Settings > Administrator Accounts > Actions > View Account

Allows you to review a specific administrator account.

Login Name

Identifies the login name assigned to the administrator account. This field is limited to 20 characters.

Role

Identifies the authorized privileges for an administrator account. Different roles are authorized to perform different functions:

Administrator 1	A login account that has the authority to perform all administration, configuration, and recovery tasks.
Administrator 2	<p>A login account that has the authority to perform all administrative and configuration tasks, except:</p> <ul style="list-style-type: none">■ Create, modify, or delete administrator accounts and File Servers.■ Modify system-wide settings such as Simple Network Management Protocol (SNMP).■ Modify software or hardware configurations.■ Shut down the system.
Monitor	A login account that has the authority to perform read-only management tasks in a Pillar Axiom system and the ability to modify their own account attributes.
Support	<p>A unique login account solely for support representatives. This login account is not authorized to modify or delete data resources, system alerts, or administrator accounts.</p> <p>Important! Use this account only if you are familiar with it or instructed by Oracle Pillar Customer Support.</p>

For the following predefined roles, you cannot assign administrators to them and you cannot delete them:

Primary system administrator	A login account that has the same privileges as the Administrator 1 role.
Primary support administrator	A login account that has the same privileges as the Monitor role, as well as privileges to perform support-related tasks.

Full Name

Identifies the first and last name associated with the administrator account.

Email Address

Identifies the email address associated with the administrator account. The email username can have up to 64 characters and the email domain can have up to 255 characters. The email server to which the Pillar Axiom system sends alerts must be able to receive messages at this address. The system does not validate this address.

Note: An IP address cannot be entered as the email domain.

Phone Number

Identifies the phone number associated with the administrator account. The Pillar Axiom system does not verify the validity of this entry.

Disabled

Indicates whether the administrative account is disabled. The Pillar Axiom system maintains disabled accounts but does not allow them to log in. A disabled account can be enabled at a later time by modifying it. This setting takes effect immediately. If the administrator is logged in when you disable the account, the system logs out the administrator immediately.

Note: You cannot disable the **Primary system administrator** account.

Related references

- [Administrator Accounts Overview Page](#)
- [Pillar Axiom System Limits](#)

Related tasks

- [Create a Pillar Axiom Administrator Account](#)
- [Modify an Administrator Account](#)

View Host, Advanced Tab

Navigation: Storage > SAN > Hosts > Actions > View Host > Advanced

Allows you to view the HP compatibility option for a particular SAN host.

HP-UX Compatibility Mode

Use this option when the SAN host that accesses the LUNs have HP-UX initiator ports and HP HBAs. When this option is enabled, the system determines LUN numbers using the HP-UX addressing scheme, allowing up to 255 LUNs. Also when enabled, the host cannot have a visible LUN using ID 0. You can verify the current host mappings in the **Pillar Axiom Path Manager** tab.

Related concepts

- [About Modifying SAN Hosts](#)

Related references

- [View Host, Pillar Axiom Path Manager Tab](#)
- [Pillar Axiom System Limits](#)

Related tasks

- [Modify a Host: Reconfigure Advanced Settings](#)

View Host, Pillar Axiom Path Manager Tab

Navigation: Storage > SAN > Hosts > Actions > View Host > Pillar Axiom Path Manager

Allows you to view the load balancing settings of LUNs.

Host Information

Host Name

Identifies the name of the SAN host.

Management IP Address

Identifies the IP address of the SAN host. The system uses this address to exchange management requests and responses with the Pillar Axiom Path Manager (APM) that is installed on the host. If APM is not installed, this field displays *N/A*.

Operating System

Identifies the operating system associated with the SAN host, if Pillar Axiom Path Manager is installed on that host; otherwise, this field displays *N/A*.

Pillar Axiom Path Manager Version

Identifies the version of the APM host driver, if it has been installed, that is running on the SAN host.

Path Manager Settings

LUN Name

Identifies the name of the LUN or Clone LUN on the Pillar Axiom system.

Name on Host

Identifies the name used by the SAN host to identify the LUN.

Load Balancing

Identifies the type of load balancing that the storage area network (SAN) hosts should perform to access Pillar Axiom LUNs.

Valid types:

Static

Indicates load balancing across multiple paths to the configured LUNs.

The software selects the best available path, and all commands are sent over that path until the path is no longer operational,

in which case the failed path fails over to another appropriate path.

Round-robin

Indicates load balancing across multiple paths to the configured LUNs.

Commands are sent one by one using the best available paths, which ensures that LUN commands are evenly distributed over any path that is available to access the LUNs.

Number of Optimized Paths

Identifies the number of optimized (fastest path available) access paths to the LUN.

Number of Non-Optimized Paths

Identifies the number of non-optimized access paths to the LUN.

Related concepts

- [About Modifying SAN Hosts](#)

Related references

- [Pillar Axiom System Limits](#)

Related tasks

- [Modify a Host: Reconfigure APM Settings](#)

View Host, iSCSI Access Tab

Navigation: Storage > SAN > Hosts > Actions > View Host > iSCSI Access

Allows you to view iSCSI-specific information for this storage area network (SAN) host.

Note: iSCSI settings are not available for a SAN host using Fibre Channel protocol.

iSCSI Host Specific Settings

Enable Authentication

Indicates whether Challenge Handshake Authentication Protocol (CHAP) for iSCSI sessions between the SAN host and the Pillar Axiom system is enabled.

Note: Depending on the global settings, CHAP name and CHAP secret may not be required. Those parameters are not required, for example, if authentication is performed through a RADIUS server.

Chap Name

Identifies the name of the iSCSI initiator that is to be used during authentication.

CHAP Secret

Identifies the encrypted CHAP authentication password (secret) to be used in the exchange of user names and secrets between two devices. Both devices must support Point-to-Point (PPP) authentication.

Retype CHAP Secret

No information is available for this field.

Grant Access to Axiom

Specifies whether the Pillar Axiom system must reject iSCSI login attempts from initiators that have not explicitly been granted permission by the user through the Pillar Axiom Storage Services Manager interface or through the Pillar Axiom Command Line Interface (CLI).

Related concepts

- [About iSCSI Settings](#)

Related references

- [Pillar Axiom System Limits](#)

Related tasks

- [Modify a Host: Reconfigure Port Settings](#)

View Host, Ports Tab

Navigation: Storage > SAN > Hosts > Actions > View Host > Ports

Allows you to view the storage area network (SAN) host driver information. If you are configuring iSCSI on the host port, you must also configure iSCSI on the Pillar Axiom system.

FC Port Information

Alias

Identifies the HBA alias name.

Port

Identifies the SAN hosts associated with the LUNs:

- For Fibre Channel networks: The World Wide Name (WWN) of the SAN host HBA port that is associated with the LUN.
- For iSCSI networks: The IP address of the iSCSI device that is associated with the LUN.

Speed

Displays the transmission speed, in Gbs, of a hardware component.

Manufacturer

Displays the manufacturer of a hardware component.

HBA Model

Displays the model number of a hardware component.

Driver Version

Identifies version of the HBA driver.

Firmware Version

Identifies the HBA firmware version.

iSCSI Port Information

Alias

Identifies the HBA alias name.

iSCSI Device Name

Identifies the name of the iSCSI initiator for the SAN host. An initiator encapsulates SCSI commands and data requests within iSCSI packets and transfers the packets across the IP network.

IP Addresses

Identifies the IP address of the iSCSI port.

Related concepts

- [About iSCSI Settings](#)

Related references

- [Pillar Axiom System Limits](#)

Related tasks

- [Modify a Host: Reconfigure Port Settings](#)

View SAN LUN, Quality of Service Tab

Navigation: Storage > SAN > LUNs > Actions > View LUN > Quality of Service

Allows you to review the capacity and performance settings for a LUN of any type (source, clone, or copy).

Selected Storage Class Capacity

Displays the storage capacity of the selected storage class and Storage Domain that is available for the LUN. The graph uses colored bars of different thicknesses to indicate the capacity status of the logical volume you are creating as well as the overall system capacity.

- Solid Green (thin): Indicates the allocated and growth potential capacity for the volume.
- Solid Blue (thick): Indicates the allocated and used capacity for the volume in the selected Storage Domain and storage class, including the impact of the current volume.
- Shaded Gray (thick): Indicates the growth potential for the selected Storage Domain and storage class, including the impact of the current volume.
- Dark Gray (thick): Indicates the available (free) capacity in the selected Storage Domain and storage class, including the impact of the current volume.
- Shaded Red (thick): Indicates the growth potential that cannot be satisfied for the volume in the selected Storage Domain and storage class, including the impact of the current volume.

System Capacity By Storage Class

Displays the storage capacity in use by the selected Storage Domain and that is in use by each media type configured in the system:

- System
- SSD SLC (solid state drive, single-level cell)
- FC (Fibre Channel)
- SATA (serial ATA)

Storage Domain

Allows you to assign the LUN to an existing Storage Domain.

[...]

Opens the dialog that allows you to review the physical capacity attributes and the Brick types that are associated with the predefined Storage Domains.

Note: The Storage Domain Details button appears when more than one Storage Domain exists.

Volume Name

Identifies the name that is assigned to a LUN for administrative purposes. LUN names must be unique across the Pillar Axiom system and must be 82 or fewer UTF characters, or 255 or fewer ASCII characters.

Volume Group

Allows you to assign the LUN to an existing volume group.

[...]

Opens the dialog that allows you to create new Volume Groups.

Storage Profile

Identifies the set of QoS attributes applied to the LUN.

[...]

Opens the View Storage Profiles dialog that allows you to review the profile details.

Recommended Storage Class

Displays the recommended storage class based on the Storage Profile selection.

Storage Class

Identifies the category of physical media on which the logical volume resides: Valid types:

- SATA
- FC
- SSD SLC (solid state drive, single-level cell)

Typical Access

Identifies the most common method of data access. Valid options:

Sequential

Read and write requests from client applications tend to request operations on the data one record after the other.

Random	Read and write requests from client applications tend to request operations on the data records in an arbitrary order.
---------------	--

Mixed	Read and write requests from client applications tend to mix the request operations on the data sometimes in sequential and sometimes in random order.
--------------	--

I/O Bias

Identifies the typical read-write ratio. Valid options:

Read	Most requests from client applications are for <code>read</code> operations.
-------------	--

Write	Most requests from client applications are for <code>write</code> operations.
--------------	---

Mixed	Requests from client applications are likely equal for <code>read</code> and <code>write</code> operations.
--------------	---

Redundancy

Identifies how many mirror copies of the original data are stored in the storage pool. Valid options:

Standard	Stores original data only. Data striping over multiple RAID groups maintains full redundancy, even without mirror copies.
-----------------	---

Double	Stores original data and one mirror copy, with data striping over multiple RAID groups.
---------------	---

Priority Level

In addition to determining the placement of data onto specific areas of the drive platters relative to the drive spindles, the priority level of a volume determines the processing *queue priority* for that volume. Queue priority defines the percentage of Slammer CPU cycles that are dedicated to the volume.

Valid options:

Premium	Highest processing queue priority. Striping occurs across eight serial ATA (SATA) RAID groups or four Fibre Channel (FC) RAID groups on the outermost 20% of the drive platters.
----------------	--

High	Next highest processing queue priority. Striping occurs across eight SATA RAID groups or four FC RAID groups on the outermost 20-40% of the drive platters.
Medium	Intermediate processing queue priority. Striping occurs across six SATA RAID groups or three FC RAID groups on the outermost 40-60% of the drive platters.
Low	Next to lowest processing queue priority. Striping occurs across four SATA RAID groups or two FC RAID groups on the outermost 60-80% of the drive platters.
Archive	Lowest processing queue priority. Striping occurs across four SATA RAID groups or two FC RAID groups on the outermost 80-100% of the drive platters.

Allocated Logical Capacity

Identifies the amount of capacity to be allocated to the logical volume.

Maximum Logical Capacity

Identifies the maximum capacity to which the logical volume can grow. For a clone, this field identifies how much addressable space will be available.

Background Copy Priority

Identifies the strategy the system should use to control the impact on performance when background tasks need to copy or move data from one location in the storage pool to another.

Note: When the system is idle or lightly loaded, the above background task maximizes the amount of work done regardless of the option selected.

Valid options:

System Chooses	Balances the background copy with the incoming client I/O. This option is the default.
Minimize Impact	Restricts the amount of work performed on a loaded system. This option is intended to have a minimal impact on client I/O throughput at the expense of longer copy times.
Maximum Speed	Prioritizes the background copy at the expense of client I/O throughput.

The following types of operations are affected by the strategy you select:

- Copy
- Restore

- Quality of Service (QoS) changes in:

- Priority
- Redundancy
- Storage Class

Allocated/Maximum Capacity

Provides an estimate of the physical storage capacity requirements, which are based on your QoS attribute selections.

Estimated Physical Capacity	Identifies the estimated physical capacity (allocated and maximum) for this LUN.
Estimated Clone Capacity	Identifies the estimated capacity (allocated and maximum) for clones of this LUN.
Estimated Total Capacity	Identifies the estimated total capacity (allocated and maximum) for this LUN.

Related concepts

- [About Creating LUNs](#)
- [About Priority Levels](#)
- [About Redundancy](#)
- [About I/O Bias](#)
- [About Access Bias](#)
- [About Storage Classes](#)

Related references

- [Effects of Access Bias and I/O Bias](#)

Related tasks

- [Create LUN: Define Quality of Service](#)
- [Modify a LUN: Define Quality of Service](#)

View SAN LUN, Mapping Tab

Navigation: Storage > SAN > LUNs > Actions > View LUN > Mapping

Allows you to review the LUN-to-host mapping settings for a LUN.

Access Protocol

Valid options:

- Fibre Channel (FC): Specifies that hosts can use the FC protocol to access this LUN.
Tip: FC paths will always be used at a preference over iSCSI paths. Also, load balancing will not be mixed between these two protocols.
- iSCSI: Specifies that hosts can use the iSCSI protocol to access this LUN.

Only selected hosts (via maps)

Specifies that only designated SAN hosts can access this LUN using a specific, possibly different, LUN number on each of those hosts. If the LUN is mapped, the LUN number must be unique to the mapped SAN host.

All hosts may access this LUN using LUN Number

Specifies all SAN hosts accessing this LUN use the same LUN number. Select this option to activate the LUN number selection drop-down list.

Available LUN Number

You can map a LUN or Clone LUN to either a single host or a host group.

LUN Slammer Control Unit Assignment

Current Slammer CU

Identifies the current Slammer CU on which the LUN is currently homed.

Note: For new source LUNs, this field is not available; instead, use Assigned Slammer CU.

Assigned Slammer CU <Auto-Assign>

Identifies the Slammer CU to which the system should assign the LUN. Available options:

<auto assign>

Select this option if you want the system to determine the Slammer CU.

Slammer CU Select a specific Slammer CU from the list to assign to the LUN.

Ports Masked for this LUN

Displays the physical Slammer ports to exclude (mask) so they cannot access the LUN.

Masked
Indicates whether the port for the LUN is masked.

Protocol
Identifies the type of access protocol, FC or iSCSI.

Slammer
Identifies the name of the Slammer.

CU
Identifies the control unit (CU) of the Slammer.

Port
Identifies the name of the Slammer CU port.

Slammer Port Address
Identifies the unique identifier of each Slammer network port. For FC networks, this identifier is the World Wide Name (WWN). For iSCSI networks, this identifier is the Media Access Control (MAC) address.

LUN Mapping

Note: The LUN mapping table only displays when you select the **Only selected hosts (via maps)** option.

Hosts Mapped to this LUN

Name	Identifies the SAN host that accesses LUNs configured on the Pillar Axiom system. If the Pillar Axiom Path Manager is not installed, the system displays the WWN of the FC HBA or the IP address of the iSCSI device.
Map via LUN #	Identifies the number to assign to the LUN for the associated SAN host. This number must be unique for that particular host. It need not be unique across all hosts.

Port Status by CU:Port	Identifies a masked physical Slammer port. A port mask prevents the LUN from being accessed from this port. Masked ports are depicted by a blue mask icon, while unmasked ports are identified with a light gray and white mask.
-------------------------------	--

Create

Opens the dialog that allows you to create the LUN-to-host mapping based on your selections for host name and the LUN number to be used by that host.

Modify

Opens the dialog that allows you to change the LUN mapped to the associated host.

Remove

Removes the LUN mapping for the selected SAN host.

Related concepts

- [About Modifying LUNs](#)
- [About Licensing Optional Premium Features](#)

Related references

- [Connection Status of Slammer Ports](#)
- [Pillar Axiom System Limits](#)

Related tasks

- [Modify LUN: Define Mapping by Selected Hosts](#)

View SAN LUN, Data Protection Tab

Navigation: Storage > SAN > LUNs > Actions > View LUN > Data Protection

Allows you to review the storage capacity of a Clone LUN. You can also review Clone LUN replication schedules from this page.

Selected Storage Class Capacity

Displays the storage capacity of the selected storage class and Storage Domain that is available for the LUN. The graph uses colored bars of different thicknesses to indicate the capacity status of the logical volume you are creating as well as the overall system capacity.

- Solid Green (thin): Indicates the allocated and growth potential capacity for the volume.
- Solid Blue (thick): Indicates the allocated and used capacity for the volume in the selected Storage Domain and storage class, including the impact of the current volume.
- Shaded Gray (thick): Indicates the growth potential for the selected Storage Domain and storage class, including the impact of the current volume.
- Dark Gray (thick): Indicates the available (free) capacity in the selected Storage Domain and storage class, including the impact of the current volume.
- Shaded Red (thick): Indicates the growth potential that cannot be satisfied for the volume in the selected Storage Domain and storage class, including the impact of the current volume.

Clone LUNs Capacity

Maximum capacity (in GB) to allocate for Clone LUNs

Specifies the maximum amount of space to make available on the Storage Domain on which the copy of the clones will reside.



Pillar strongly recommends that you allocate sufficient repository capacity to minimize the chances of running out of this space (which could lead to data inconsistency or loss). To set sufficient capacity, use a value equal to the source volume capacity times the number of replicas times the maximum rate of change. For example, for a 100 GB volume that is projected to have 20 active replicas at a time and no more than a 20% rate of change, use a value of 400 GB for the clone repository.

Number of existing Clone LUNs

Specifies the number of clones that have been created for this LUN and its clones.

Available capacity for Clone LUNs

The amount of current storage capacity allocated for clones of this LUN.

Clone Schedules**Name**

Specifies the name of the replication schedule.

Start Time

Specifies the date and time to begin scheduling replication.

Frequency

Specifies the frequency at which the scheduled replication runs. Frequencies include:

- Run Once
- Hourly
- Daily
- Weekly

Enabled

Specifies whether the scheduled replication is enabled.

Enabled

Indicates that the scheduled event performs at the specified time.

Disabled

Indicates that the operation will not perform as scheduled. Disable the schedule, for example, when the source volume (LUN or Clone LUN) has not been made available to users.

Create

Displays a dialog to create a new replication schedule.

Modify

Displays a dialog to modify an existing replication schedule.

Delete

Removes an existing replication schedule.

Related concepts

- [About Modifying LUNs](#)

Related references

- [Pillar Axiom System Limits](#)

Related tasks

- [Modify LUN: Define Data Protection](#)
- [Create a Clone LUN Schedule](#)
- [Modify a LUN Data Protection Schedule](#)
- [Delete a LUN Data Protection Schedule](#)

View SNMP Host Dialog

Navigation: Global Settings > SNMP > Actions > View SNMP Host

Allows you to view Simple Network Management Protocol (SNMP) trap hosts.

Name

Identifies the name for the SNMP host.

Host IP

Identifies the IP address or domain name of a client that receives the Pillar Axiom SNMP information.

Community string

Identifies the community string for use when the Pillar Axiom system sends an event trap to the SNMP host.

Note: When an administrator does not specify a community string for read-only access, SNMP servers and clients will typically use `public`.

Receive traps

Indicates that the SNMP host receives event traps sent to it.

Severity threshold

Identifies the severity threshold for events that are to be sent to the SNMP host by event traps.

Severity levels:

- Informational
- Warning
- Critical

Related concepts

- [About Licensing Optional Premium Features](#)

Related references

- [Pillar Axiom System Limits](#)

Related tasks

- [Create SNMP Hosts](#)
- [Modify SNMP Hosts](#)
- [Delete SNMP Hosts](#)

Volume Groups Overview Page

Navigation: Groups > Volume Groups

Allows you to review the volume groups and logical volumes that are configured on the Pillar Axiom system.

Available options allow you to create, modify, delete, move, and view volume groups and logical volumes, as well as to create an immediate Clone LUN.

When dashes appear in a field, it means that the field is not applicable to a specific object type.

Name

Lists the names of configured logical volumes and volume groups and identifies those volumes contained within the volume groups.

Status

Identifies the online status of each logical volume.

Storage Domain

Lists the name of the Storage Domain associated with the logical volume.

Logical Capacity (GB)

Identifies an overview of the logical storage capacity usage and requirements of the volume group.

Used	Identifies the current capacity consumed by the volume.
Allocated	Specifies the amount of raw capacity in gigabytes (GB) that has been assigned and designated to this logical volume.
Maximum	Identifies the maximum storage capacity to which the logical volume can grow.
Physical Distribution	A graphical representation of the capacity used compared to the maximum allocated.

Capacity (GB) for Clone LUNs

Displays the physical storage usage for the Clone LUNs.

Logical Maximum	Identifies the amount of storage that was requested for the clone repository.
------------------------	---

Physical Used	Identifies the current volume capacity usage of the object.
Physical Allocated	Identifies the total amount of storage capacity that is reserved on the system.
Physical Maximum	Identifies the maximum capacity to which the logical volume can grow. For clones, this field identifies how much addressable space is available.

Physical Capacity (GB)

Identifies an overview of the actual physical storage capacity usage and requirements of all the volumes on the system.

Redundancy	Identifies how many mirror copies of the original data are stored online.
Disk Protection	Indicates the RAID drive data protection method.
Volume Overhead	Identifies the physical and logical storage capacity that is required to meet the logical volume Quality of Service (QoS) settings.
Used	Identifies the current capacity consumed by the volume.
Allocated	Specifies the amount of raw capacity in gigabytes (GB) that has been assigned and designated to this logical volume.
Maximum	Identifies the maximum capacity for the volume group. The maximum capacity of the logical volumes and nested volume groups that are associated with the volume group cannot exceed this value. A value of 0 (zero) identifies that the volume group is configured with unlimited capacity. You can increase the maximum capacity of associated logical volumes and nested volume groups without constraints.
Physical Distribution	A graphical representation of the capacity used compared to the maximum allocated.

Priority Level

Identifies the assigned priority level when the volume was created.

- Premium
- High
- Medium
- Low
- Archive

Related concepts

- [*About Moving Logical Volumes*](#)

Related references

- [*Manage Volume Groups, Volume Groups Tab*](#)
- [*Pillar Axiom System Limits*](#)

Related tasks

- [*Create Volume Groups*](#)
- [*Modify Volume Group Attributes*](#)
- [*Delete a Volume Group*](#)

APPENDIX C

Monitor Tab Reference Pages

Accept Brick Dialog

Navigation: Hardware > Bricks

Allows you to integrate a new or foreign Brick into the Pillar Axiom system.

Storage Domain

Identifies the Storage Domain to which this Brick should be assigned.

This control is available only when administrator-defined domains exist.

Brick Name

Identifies the logical name to be used for this Brick.

Related tasks

- [Accept a Brick](#)

Bricks Overview Page

Navigation: Hardware > Bricks

Allows you to review the Bricks that are installed on the Pillar Axiom system.

Pillar Axiom systems support three types of Brick storage enclosures:

- serial ATA (SATA)
- SATA version 2 (SATA V2)
- Fibre Channel (FC)

FC Bricks come in two flavors: RAID and Expansion. SATA, SATA V2, and FC RAID Bricks contain two RAID controllers and at least 12 drives. FC Expansion Bricks do not have a RAID controller but instead rely on the controller within the FC RAID Brick to which they are attached.

SATA and SATA V2 Bricks have 13 drives. The 13th drive is used as a spare for automatic failover purposes. FC Bricks do not have a dedicated spare; any drive can be utilized as a spare.

Brick Name

Lists the names of the Bricks. Click a name to display details about that hardware component.

Note: When you move the mouse cursor over a name, the fully qualified name (FQN) for that Brick is displayed.

Enclosure Type

Lists the type of RAID controller installed in the Brick chassis. Valid types:

- Unknown
- SATA
- SATA V2
- FC
- FC V2

Media Type

Lists the type of drives installed within the Brick enclosure. Valid types:

- SATA
- FC

- SSD SLC (solid state drive, single-level cell)

Brick Status

Displays the current status of the hardware components. A status of Normal requires no action. Valid options:

Overall	Displays the summary status of the Brick.
Temperature	Displays the status of the Brick temperature.
Chassis	Displays the status of the Brick chassis.
ES Module	Displays the status of the enclosure services (ES) module, which monitors the fan speed, power supply temperature, drive status, and RAID controller status.
RAID Controller	Displays the status of the RAID controller within the Brick.
Power Supply and Fans	Displays the status of the power supplies and fans within the Brick.
Disks	Displays the status of the drives within the Brick.
Spare Disk	Displays the status of the spare drive within the Brick.

Details

Displays the current capacity of the Brick and the name of the Storage Domain within which the Brick resides. Valid options:

Total Capacity	Displays the total raw capacity for the Brick. This value does not include the capacity of the spare drive.
Storage Domain	Displays the name of the Storage Domain associated with the Brick.

Related references

- [*Hardware Overview Page*](#)
- [*View Brick, Components Tab*](#)
- [*View Brick, I/O Ports Tab*](#)

Related tasks

- [*Display Hardware Component Status*](#)
- [*Modify a Hardware Component Name*](#)
- [*Identify the Hardware Component*](#)
- [*Replace a FRU*](#)

Configure Trending Chart, Chart Threshold Tabs

To view details about the Slammer or LUN Configure Trending Chart, Chart Threshold tab, choose one of:

- [Configure Trending Chart, Chart Thresholds Tab \(LUNs\)](#)
- [Configure Trending Chart, Chart Thresholds Tab \(Slammers\)](#)

Configure Trending Chart, Chart Thresholds Tab (LUNs)

Navigation: *Statistics and Trending > SAN > LUNs > Actions > LUN Statistics Trending > Configure Trending Chart > Chart Thresholds*

Allows you to add a new chart threshold, to modify a chart threshold, or to remove thresholds from the Chart Thresholds list.

A chart threshold is a labeled horizontal line that you can add to your trending chart to serve as a visual benchmark for comparing the values of the trending lines that appear in the chart. All chart thresholds created in your current session are displayed in the Chart Thresholds list.

Name

Displays the name assigned to the threshold.

Scale

Displays the statistic metric assigned to the threshold. The statistic metric corresponds to one of the scale rules displayed on either side of the trending chart.

Value

Specifies the value assigned to the threshold. This is the numeric value of the statistic metric that determines where the chart threshold line is displayed on the chart.

Color

Specifies the color used to display the threshold line in the chart.

The color distinguishes the threshold line from the trending lines in the trending chart.

Rendering Mode

Indicates whether the threshold line is only displayed when it is within the axis scale, or the axis scale is automatically adjusted to ensure that the threshold line is always displayed. Valid modes:

Adjust axis scale to always display	Ensures that the threshold line will be visible in the chart by automatically adjusting the scale of the chart.
Only display if within axis scale	Does not adjust the scale of the chart, so the threshold line does not appear in the chart if the threshold value falls outside the scale.

Add

Opens a dialog for creating a new chart threshold. You can give the threshold a name, specify the threshold statistic type and value, and select a color and mode for rendering the threshold on the chart.

When a chart threshold is added, it is displayed in the Chart Thresholds list.

Modify

Opens a dialog for modifying the selected chart threshold. You can change the name of the chart threshold, the threshold statistic metric or value, or the color and mode for rendering the threshold on the chart.

Clear

Removes all chart thresholds from the Chart Threshold list.

Remove

Removes the selected chart threshold from the Chart Threshold list.

Related concepts

- [About LUN Statistics Trending Charts](#)

Related references

- [Create Chart Threshold Dialog \(LUNs\)](#)

Related tasks

- [Create a Chart Threshold](#)

Configure Trending Chart, Chart Thresholds Tab (Slammers)

Navigation: *Statistics and Trending > SAN > Slammer Protocols > Actions > Slammer Statistics Trending > Configure Trending Chart > Chart Thresholds*

Allows you to add a new chart threshold, to modify a chart threshold, or to remove thresholds from the Chart Thresholds list.

A chart threshold is a labeled horizontal line that you can add to your trending chart to serve as a visual benchmark for comparing the values of the trending

lines that appear in the chart. All chart thresholds created in your current session are displayed in the Chart Thresholds list.

Name

Displays the name assigned to the threshold.

Scale

Displays the statistic metric assigned to the threshold. The statistic metric corresponds to one of the scale rules displayed on either side of the trending chart.

Value

Specifies the value assigned to the threshold. This is the numeric value of the statistic metric that determines where the chart threshold line is displayed on the chart.

Color

Specifies the color used to display the threshold line in the chart.

The color distinguishes the threshold line from the trending lines in the trending chart.

Rendering Mode

Indicates whether the threshold line is only displayed when it is within the axis scale, or the axis scale is automatically adjusted to ensure that the threshold line is always displayed. Valid modes:

Adjust axis scale to always display	Ensures that the threshold line will be visible in the chart by automatically adjusting the scale of the chart.
Only display if within axis scale	Does not adjust the scale of the chart, so the threshold line does not appear in the chart if the threshold value falls outside the scale.

Add

Opens a dialog for creating a new chart threshold. You can give the threshold a name, specify the threshold statistic type and value, and select a color and mode for rendering the threshold on the chart.

When a chart threshold is added, it is displayed in the Chart Thresholds list.

Modify

Opens a dialog for modifying the selected chart threshold. You can change the name of the chart threshold, the threshold statistic metric or value, or the color and mode for rendering the threshold on the chart.

Clear

Removes all chart thresholds from the Chart Threshold list.

Remove

Removes the selected chart threshold from the Chart Threshold list.

Related concepts

- [*About SAN Slammer Statistics Trending Charts*](#)

Related references

- [*Create Chart Threshold Dialog \(Slammers\)*](#)

Related tasks

- [*Create a Chart Threshold*](#)

Configure Trending Chart, Data Filtering Tabs

To view details about the Slammer or LUN Configure Trending Chart, Data Filtering tab, choose one of:

- [Configure Trending Chart, Data Filtering Tab \(LUNs\)](#)
- [Configure Trending Chart, Data Filtering Tab \(Slammers\)](#)

Configure Trending Chart, Data Filtering Tab (LUNs)

Navigation: *Statistics and Trending > SAN > LUNs > Actions > LUN Statistics Trending > Configure Trending Chart > Data Filtering*

Allows you to restrict the data used in a trending chart to data collected before or after a specified time.

Filter out statistics older than

Excludes all statistics collected before the specified date. When used in conjunction with the following filter, specifies a time range for the data displayed in the trending chart.

Filter out statistics more recent than

Excludes all statistics collected after the specified date. When used in conjunction with the previous filter, specifies a time range for the data displayed in the trending chart.

Related concepts

- [About LUN Statistics Trending Charts](#)

Related tasks

- [Configure a LUN Statistics Trending Chart](#)

Configure Trending Chart, Data Filtering Tab (Slammers)

Navigation: *Statistics and Trending > SAN > Slammer Protocols > Actions > Slammer Statistics Trending > Configure Trending Chart > Data Filtering*

Allows you to restrict the data used in a trending chart to data collected before or after a specified time.

Filter out statistics older than

Excludes all statistics collected before the specified date. When used in conjunction with the following filter, specifies a time range for the data displayed in the trending chart.

Filter out statistics more recent than

Excludes all statistics collected after the specified date. When used in conjunction with the previous filter, specifies a time range for the data displayed in the trending chart.

Related concepts

- [About SAN Slammer Statistics Trending Charts](#)

Related tasks

- [Configure a SAN Slammer Statistics Trending Chart](#)

Configure Trending Chart, Trend Configuration Tabs

To view details about the Slammer or LUN Configure Trending Chart, Trend Configuration tab, choose one of:

- [Configure Trending Chart, Trend Configuration Tab \(LUNs\)](#)
- [Configure Trending Chart, Trend Configuration Tab \(Slammers\)](#)

Configure Trending Chart, Trend Configuration Tab (LUNs)

Navigation: *Statistics and Trending > SAN > LUNs > Actions > LUN Statistics Trending > Configure Trending Chart > Trend Configuration*

Allows you to specify the trending chart data to display for the selected LUNs on the Pillar Axiom system.

LUNs to Trend

Name

Lists the names of the LUNs selected for trending.

Volume Group

Identifies the volume group to which each LUN selected for trending belongs.

Storage Domain

Identifies the Storage Domain to which each LUN selected for trending belongs.

Current Slammer Node

Identifies the Slammer name and control unit (CU) to which each LUN selected for trending belongs.

Add

Opens a dialog for adding new LUNs to the list.

Clear

Removes all of the LUNs from the LUNs to Trend list.

Remove

Removes the selected LUN from the LUNs to Trend list.

Slammer Control Unit Data to Trend

Add

Opens a dialog for adding Slammer control units (CUs) to the list.

Clear

Removes all of the Slammer CUs from the Slammer CU Data to Trend list.

Remove

Removes the currently selected Slammer CU from the Slammer CU Data to Trend list.

Statistics to Trend

Add

Opens a dialog for adding a statistic to the Statistics to Trend list.

Clear

Removes all of the statistics from the Statistics to Trend list.

Remove

Removes the currently selected statistic from the Statistics to Trend list.

Related concepts

- [About LUN Statistics Trending Charts](#)

Related tasks

- [Configure a LUN Statistics Trending Chart](#)

Configure Trending Chart, Trend Configuration Tab (Slammers)

Navigation: *Statistics and Trending > SAN > Slammer Protocols > Actions > Slammer Statistics Trending > Configure Trending Chart > Trend Configuration*

Allows you to specify the trending chart data to display for the selected Slammer on the Pillar Axiom system.

Ports to Trend

Add

Opens a dialog for adding new Slammer ports to the list.

Clear

Removes all of the Slammer ports from the Ports to Trend list.

Remove

Removes the selected Slammer port from the Ports to Trend list.

Slammer Control Unit Data to Trend

Add

Opens a dialog for adding Slammer control units (CUs) to the list.

Clear

Removes all of the Slammer CUs from the Slammer CU Data to Trend list.

Remove

Removes the currently selected Slammer CU from the Slammer CU Data to Trend list.

Statistics to Trend

Add

Opens a dialog for adding a statistic to the Statistics to Trend list.

Clear

Removes all of the statistics from the Statistics to Trend list.

Remove

Removes the currently selected statistic from the Statistics to Trend list.

Related concepts

- [About SAN Slammer Statistics Trending Charts](#)

Related tasks

- [Configure a SAN Slammer Statistics Trending Chart](#)

Create Chart Threshold Dialogs

To view details about the Slammer or LUN Create Chart Threshold dialogs, choose one of:

- [Create Chart Threshold Dialog \(LUNs\)](#)
- [Create Chart Threshold Dialog \(Slammers\)](#)

Create Chart Threshold Dialog (LUNs)

Navigation: *Statistics and Trending > SAN > LUNs > Actions > LUN Statistics Trending > Configure Trending Chart > Chart Thresholds > Add*

Allows you to add a new horizontal threshold line to the chart by giving it a name, specifying the statistic metric and value to use, and by specifying the color and rendering method to use when the threshold is displayed.

Name

Identifies the threshold by giving it a name. This is the name that appears in the Chart Thresholds list and on the threshold line in the trending chart.

Statistic Metric Type

Specifies the type of statistical metric to use for the threshold. This metric appears under the Scale heading in the Chart Thresholds list, and it corresponds to one of the axis scale rulers displayed on either side of the trending chart.

Available types of statistical metrics are:

Capacity (GB)	Total amount of storage use in gigabytes (GB).
IOPS per second	Number of I/O operations processed each second.
IOPS (Cumulative)	Total number of I/O operations processed.

MB per Second	Data transfer rate in megabytes (MB) each second.
----------------------	---

MB (Cumulative)	Total amount of data transferred in megabytes (MB).
------------------------	---

Occurrences per Second	Rate of occurrences each second.
-------------------------------	----------------------------------

Occurrences (Cumulative)	Total number of occurrences.
---------------------------------	------------------------------

Value

Specifies the value assigned to the threshold. This is the numeric value of the statistic metric that determines where the chart threshold line is displayed on the chart.

Requires a positive numeric value.

Color

Specifies the color used to display the threshold line in the chart.

The color distinguishes the threshold line from the trending lines in the trending chart.

Rendering Mode

Indicates whether the threshold line is only displayed when it is within the axis scale, or the axis scale is automatically adjusted to ensure that the threshold line is always displayed. Valid modes:

Adjust axis scale to always display	Ensures that the threshold line will be visible in the chart by automatically adjusting the scale of the chart.
--	---

Only display if within axis scale	Does not adjust the scale of the chart, so the threshold line does not appear in the chart if the threshold value falls outside the scale.
--	--

Related concepts

- [About LUN Statistics Trending Charts](#)

Related tasks

- [Create a Chart Threshold](#)

Create Chart Threshold Dialog (Slammers)

Navigation: *Statistics and Trending > SAN > Slammer Protocols > Actions > Slammer Statistics Trending > Configure Trending Chart > Chart Thresholds > Add*

Allows you to add a new horizontal threshold line to the chart by giving it a name, specifying the statistic metric and value to use, and by specifying the color and rendering method to use when the threshold is displayed.

Name

Identifies the threshold by giving it a name. This is the name that appears in the Chart Thresholds list and on the threshold line in the trending chart.

Statistic Metric Type

Specifies the type of statistical metric to use for the threshold. This metric appears under the Scale heading in the Chart Thresholds list, and it corresponds to one of the axis scale rulers displayed on either side of the trending chart.

Available types of statistical metrics are:

Capacity (GB)	Total amount of storage use in gigabytes (GB).
IOPS per second	Number of I/O operations processed each second.
IOPS (Cumulative)	Total number of I/O operations processed.
MB per Second	Data transfer rate in megabytes (MB) each second.
MB (Cumulative)	Total amount of data transferred in megabytes (MB).
Occurrences per Second	Rate of occurrences each second.

**Occurrences
(Cumulative)** Total number of occurrences.

Value

Specifies the value assigned to the threshold. This is the numeric value of the statistic metric that determines where the chart threshold line is displayed on the chart.

Requires a positive numeric value.

Color

Specifies the color used to display the threshold line in the chart.

The color distinguishes the threshold line from the trending lines in the trending chart.

Rendering Mode

Indicates whether the threshold line is only displayed when it is within the axis scale, or the axis scale is automatically adjusted to ensure that the threshold line is always displayed. Valid modes:

- | | |
|--|--|
| Adjust axis
scale to
always display | Ensures that the threshold line will be visible in the chart by automatically adjusting the scale of the chart. |
| Only display if
within axis
scale | Does not adjust the scale of the chart, so the threshold line does not appear in the chart if the threshold value falls outside the scale. |

Related concepts

- [About SAN Slammer Statistics Trending Charts](#)

Related tasks

- [Create a Chart Threshold](#)

Create Event Notification Dialog

Navigation: Event Notification > Actions > Create Event Notification

Use the Create Event Notification dialog to create event notices when specified events occur. When an event is triggered, the Pillar Axiom system sends a notification to the designated email recipients.

Name

Identifies the name of the event notification.

Description

Describes the event notification.

Enable Event Notification

Indicates whether the event notification is enabled. When checked, this option activates the notification when the event occurs on the Pillar Axiom system.

Event Notification Recipient Email Addresses

Identifies the email addresses of the recipients who are to receive event notifications. The email server to which the Pillar Axiom system sends notifications must be able to send messages to these email addresses.

Add

Allows you to add email recipients to the event notification.

Test Email

Sends a message to the specified email addresses to test recipient email addresses. Recipients should look for a message that is titled "[Axiom-QoS] Test email" in their email in-boxes.

Note: Allow at least 10 minutes between email tests.

Remove

Deletes the selected email address from the list.

Monitored Events

Lists events that are defined in the selected categories.

You can sort the list of events in one of two ways:

**By severity,
then category**

Sorts the list by severity with a list of event categories. The severity categories include:

	Informational	Requires no action for events that are information only.
	Warning	Requires no immediate action for minor conditions that you can address at your convenience.
	Critical	Requires prompt action to prevent system failures or offline conditions.
By category, then severity	Sorts the list by categories with a list of event severity.	
	Security	Events to notify of a security problem such as unauthorized request.
	Audit	Events that keep track of what users are doing, such as the operations that they performed.
	System	Events to notify of system problems, such as a missing Brick or Slammer.

Related references

- [Event Notification Overview Page](#)
- [System Event Severities](#)
- [Pillar Axiom System Limits](#)

Related tasks

- [Create an Event Notification](#)

Create Reporting Schedule Dialog

Navigation: *Reporting > Reporting Schedules > Create Schedule*

Use the Create Reporting Schedules dialog to create a new schedule for generating reports.

Schedule Name

Displays the name of the schedule.

If you do not specify a name, the system uses the default name of `untitled`.

Report Type

Specifies the type of report the schedule generates. Report types include:

- SAN Hosts
- Storage Performance
- Storage Use
- Storage Use per Volume
- System Configuration
- System Configuration Summary

Start Time

Specifies the date and time to begin generating reports.

Schedule Frequency

Specifies the frequency at which the schedule generates reports. Frequencies include:

- Run Once
- Hourly
- Daily
- Weekly

Recurrence

Specifies how many hours, days, or weeks to wait before generating this scheduled report again.

Related concepts

- [*About Scheduled Reports*](#)

Related tasks

- [*Create a Reporting Schedule*](#)

Download Report Dialog

Navigation: *Reporting > Generate Reports > Download Report*

Allows you to download a previously generated report to your client in a variety of formats.

Format

Available formats are:

- CSV
- Excel
- HTML
- PDF
- XML

Target Download Path

Filename and path for where to save the downloaded file.

Related tasks

- [*Download a Report*](#)

Event Log Overview Page

Navigation: **Event Logs**

Use the Event Log page to review entries in the Pillar Axiom event log. You can set a filter to display specific types of events if the list is too long.

Event

Displays the name of the event in the Pillar Axiom event log.

Severity

Displays the severity level of entries in the Pillar Axiom event log. Valid options:

Informational	Requires no action for events that are information only.
Warning	Requires no immediate action for minor conditions that you can address at your convenience.
Critical	Requires prompt action to prevent system failures or offline conditions.

Category

Identifies the type of event. Valid values:

Security	Events to notify of a security problem such as unauthorized request.
Audit	Events that keep track of what users are doing, such as the operations that they performed.
System	Events to notify of system problems, such as a missing Brick or Slammer.

Time Occurred

Identifies the time at which the event was sent to the designated recipients.

Affected Item

Provides the specific object name affected by the Event Type. For example, if the **Event** reads Brick Firmware Invalid, then the **Affected Item** column lists the Brick name that caused the event to occur. Such details provide additional information for troubleshooting purposes.

User

The name of the user logged in at the time the event occurred.

Description

Displays the event description text.

Events per Page

Indicates the number of events to display on each page. The default is 50 events.

Note: If (filtered) displays at the top of the page, it indicates that the list contains excluded items.

Refresh

Allows you to update the contents of the page.

Related references

- [*Pillar Axiom System Limits*](#)
- [*System Event Severities*](#)

Related tasks

- [*Display the Event Log*](#)
- [*Filter Event Log Entries*](#)

Event Notification Overview Page

Navigation: Event Notification

Use the Event Notification overview page to review the list of event notifications created for the Pillar Axiom system. This page provides options to create, modify, delete, and view event notifications.

Name

Lists the name of event notification. Click a name to review, modify, or delete the notification settings.

Enabled

Indicates whether the event notification is enabled.

- **Yes:** The event notification is actively collecting event information.
- **No:** The event notification is inactive and not collecting event information.

Time Last Sent

Identifies the time at which the event was sent to the designated recipients.

Number of Events

Indicates the number of events collected by the notification.

Number of Recipients

Indicates the number of email recipients subscribed to the event notification.

Description

Displays the description of the event notification.

Related references

- [*Pillar Axiom System Limits*](#)

Related tasks

- [*Display Event Notifications*](#)
- [*Create an Event Notification*](#)
- [*Modify an Event Notification*](#)
- [*View Event Notification Details*](#)
- [*Delete an Event Notification*](#)
- [*Display the Event Log*](#)

Events Properties Dialog

Navigation: Event Log > Actions > Event Properties

Use the Events Properties dialog to view detailed information about a selected event.

Copy to Clipboard

Select this option to copy the contents of the event properties to your clipboard. For example, copy the event properties to the clipboard, then paste the information to an email that you may want to send to a system administrator.

Event

Displays the name of the event in the Pillar Axiom event log.

Category

Identifies the type of event. Valid values:

Security	Events to notify of a security problem such as unauthorized request.
Audit	Events that keep track of what users are doing, such as the operations that they performed.
System	Events to notify of system problems, such as a missing Brick or Slammer.

Time Occurred

Identifies the time at which the event was sent to the designated recipients.

User

The name of the user logged in at the time the event occurred.

Affected Item

Provides the specific object name affected by the Event Type. For example, if the **Event** reads Brick Firmware Invalid, then the Affected Item column lists the Brick name that caused the event to occur. Such details provide additional information for troubleshooting purposes.

Description

Displays the event description text. The **Description** also provides additional information that the Oracle Pillar Customer Support can use to help resolve the event.

Related tasks

- [*Display the Event Properties*](#)
- [*Display the Event Log*](#)

Export Dialog

Navigation:

- *Statistics and Trending > SAN > LUNs > Actions > LUN Statistics Trending > Export*
- *Statistics and Trending > SAN > Slammer Protocols > Actions > Slammer Statistics Trending > Export*

Allows you to save the data in the displayed trending chart as a CSV or XML file on your client workstation.

Format

Specifies the format for the exported chart data. Valid formats:

CSV	Parses the information into comma-separated values (CSV) format.
XML	Parses the information into XML format.

Export to

Specifies where on your local workstation to save your formatted file.

Related concepts

- [About LUN Statistics Trending Charts](#)
- [About SAN Slammer Statistics Trending Charts](#)

Related tasks

- [Export a Trending Chart](#)

Generate Report Dialog

Navigation: *Reporting > Generated Reports > Generate Report*

Allows you to create a report by selecting from a list of predefined report types.

Type

Specifies the type of report to be generated:

SAN Hosts	Provides statistical information on the host servers and configured components currently included in your storage area network (SAN).
Storage Performance	Provides performance information about the LUNs on the Pillar Axiom system. Includes operations/second, read MB/s, and write MB/s.
Storage Use	Provides storage capacity information on the storage currently available on the Pillar Axiom system. Includes total capacity, allocated, free, and unavailable capacity, and storage use by Storage Class.
Storage Use per Volume	Provides capacity information for each logical volume on the Pillar Axiom system.
System Configuration	Provides detailed information on the configuration and status of the current Pillar Axiom system and all of its components, such as serial numbers, firmware versions, ports, and status, for the Pilot, Slammers, and Bricks.
System Configuration Summary	Provides a summary of the Pilot, Slammer, and Brick information included in the detailed System Configuration report.

Related tasks

- [Generate a Report](#)

Generated Reports Overview Page

Navigation: *Reporting > Generated Reports*

Allows you to generate a report, download a generated report to your client workstation in the format of your choice, or delete a generated report.

All reports, whether manually generated or generated by a reporting schedule, are stored on the Pillar Axiom system and listed on this page. The Generated Reports page lists the names, creation dates, and sizes of all currently available generated reports. Use the Generated Reports list to select reports for downloading in the format of your choice or to delete selected reports.

Name

Displays the name of the generated report.

Created

Displays the date and time that the report was created.

Size

Indicates the size of the raw report file in kilobytes (KB) or megabytes (MB).

Note: The size of the downloaded report will vary depending on the chosen format.

Related concepts

- [About Generated Reports](#)

Related references

- [Generate Report Dialog](#)
- [Download Report Dialog](#)

Related tasks

- [Generate a Report](#)
- [Download a Report](#)
- [Delete a Report](#)

Hardware Overview Page

Navigation: Hardware

Allows you to select options to display hardware components installed on the Pillar Axiom system. After you select a type, you can select and review the status and current configuration of a specific hardware component.

Lists hardware components by type. Click a component identifier to display details about the component:

Pilot

Allows you to review the Pilot status and properties.

Slammers

Allows you to review the Slammer status and properties.

Bricks

Allows you to review the Bricks status and properties.

UPS

Allows you to review the uninterruptible power supply (UPS) status and properties.

Component Status Overview

Briefly describes the types of hardware components in Pillar Axiom systems.

Related concepts

- [*About Hardware Replacement*](#)

Related references

- [*Pilot Overview Page*](#)
- [*Slammers Overview Page*](#)
- [*Bricks Overview Page*](#)
- [*Uninterruptible Power Supplies Overview Page*](#)
- [*Pillar Axiom System Limits*](#)

Related tasks

- [*Display Hardware Component Status*](#)
- [*Modify a Hardware Component Name*](#)
- [*Identify the Hardware Component*](#)

LUN Statistics and Trending Overview Page

Navigation: *Statistics and Trending > SAN > LUNs*

Allows you to review performance statistics for LUNs, view trending charts for LUNs, and export trending chart data.

Name

Identifies the name that is assigned to a LUN for administrative purposes.

Physical Allotted Capacity

Identifies the maximum capacity limit, in gigabytes (GB), that is assigned to the object.

Priority Level

Identifies the priority level assigned to the specified LUN.

Valid levels:

- Archive
- Low
- Medium
- High
- Premium

Average IOPs

Identifies the current performance for input (read) and output (write) operations for the LUN.

Average Throughput

Identifies the data transfer rate for inputs (reads) and outputs (writes) of the specified LUN.

Average I/O Latency

Identifies the average time to complete the read or write operations.

Average I/O Size

Identifies the average size of the read and write operations.

Collection Period

Identifies the start and end time at which information was last collected from the Pillar Axiom system.

Related concepts

- [*About LUN Statistics*](#)
- [*About LUN Statistics Trending Charts*](#)

Related references

- [*LUN Statistics Trending Dialog*](#)
- [*Pillar Axiom System Limits*](#)

Related tasks

- [*View LUN Statistics*](#)
- [*Configure a LUN Statistics Trending Chart*](#)

Manage System Alert Dialog

*Navigation: **System Alerts** > **Actions** > **Manage System Alert***

Use the Manage System Alert dialog to review details about a system alert.

Copy to Clipboard

Select this option to copy the contents of the system alert properties to your clipboard. For example, copy the alert properties to the clipboard, then paste the information to an email that you may want to send to a system administrator.

System Alert

Specifies one or more alerts that are to be addressed.

Time Occurred

Identifies the time at which the alert occurred.

Affected Object

Provides the specific object name affected by the system alert. For example, if the **System Alert** reads Missing Brick, then the Affected Item lists the Brick name that caused the alert to occur. Such details provide additional information for troubleshooting purposes.

Description

Displays the system alert description text. The **Description** also provides additional information that you can use to resolve the alert.

Remove Brick from Configuration (*Brick system alerts only*)

Allows you to remove the Brick from the hardware configuration.

Related concepts

- [About System Notifications](#)

Related references

- [System Alerts Overview Page](#)

Related tasks

- [Manage System Alerts](#)
- [Delete a System Alert](#)

Modify Brick, Components Tab

Navigation: Hardware > Bricks > Actions > Modify Name > Components

Use the Modify Brick, Components tab to review the status of Bricks. If there is a hardware failure, click the failed component. The Pillar Axiom Storage Services Manager takes you to Guided Maintenance, which helps you through the process of resolving the hardware failure.

Note: For more information on Guided Maintenance, refer to the *Pillar Axiom Service Guide*.

Brick Name

Specifies the new name that is assigned the Brick. Use a unique, meaningful name to help you easily locate specific components. The Pillar Axiom system maps the assigned name to the component's serial number and updates the map if you modify the component name.

By default, the Bricks are assigned names such as `Brick001`. This string is a logical Brick name and does not necessarily reflect the physical location of the Brick.

Serial Number

Displays the serial number of the selected Brick.

Brick ID

Displays the unique identifier (the World Wide Name) of the selected Brick.

Replaceable Unit

Displays the Brick component that is replaceable. Select a component, and then click **Replace Component** to start Guided Maintenance.

Status

Displays the current status of the hardware component. A status of Normal requires no action.

Part Number

Displays the part number of the replaceable hardware component.

Serial Number

Displays the serial number of the replaceable hardware component.

Related references

- [*Modify Brick, I/O Ports Tab*](#)
- [*Hardware Overview Page*](#)

Related tasks

- [*Display Hardware Component Status*](#)
- [*Identify the Hardware Component*](#)
- [*Replace a FRU*](#)

Modify Brick, I/O Ports Tab

Navigation: Hardware > Bricks > Actions > Modify Name > I/O Ports

Use the Modify Brick, I/O Ports tab to review the status of the Fibre Channel (FC) interfaces of Bricks.

Port

Lists by type the FC ports on a Brick:

- **RAID Controller Module** (0 or 1)
- **FC0 through FC3** or **Cascade** (FC Bricks only)

Status

Identifies the connection status of the port.

The Pillar Axiom user interfaces (the GUI and CLI) show that host Fibre Channel (FC) HBA ports are either **Connected** or **Not Connected** to the Slammer ports. The meaning of **Connected** is that the HBA port on the SAN host has logged in to the port on the Slammer using the FC protocol. In most operating systems, host ports log in to the Slammer ports immediately after the two are physically connected and enabled and remain logged in until the physical connection is broken. So, **Connected** effectively means that there is an enabled physical connection between the ports.

Note: On HP-UX platforms, however, some HBA device drivers use a different approach—they log out from the connection when there is no traffic to send. An HP-UX HBA port often shows as **Not Connected** even though there is an enabled physical connection between the ports.

Bandwidth

Displays the transmission speed of the port.

Connection Type

Identifies the types of connectors between the RAID controller and the Brick:

- **Copper:** Identifies RJ-45 copper interfaces.
- **Long Wave Optical:** Identifies longwave optical small form-factor pluggable (SFP) transceiver interfaces.
- **Short Wave Optical:** Identifies shortwave optical SFP transceiver interfaces.
- **Unknown:** Connection type cannot be determined.

SFP Status

Displays the status of the small form-factor pluggable (SFP) transceiver.

If the interface module itself should fail, the SFP status shows **Hardware Failure**.

Note: The **SFP Status** and **SFP Vendor** fields display information only when version 2 private interconnect modules (PIMs) are connected to version 2 SATA controllers using optical SFPs. In all other cases, these two fields are blank.

SFP Vendor

Displays the SFP manufacturer. If that information is not available, the field is blank or displays **Unknown**. See also the preceding note.

SFP Part Number

Displays the vendor's part number for the SFP. If that information is not available, the field is blank or displays **Unknown**. See also the preceding note.

SFP Revision

Displays the part revision number for the SFP. If that information is not available, the field is blank or displays **Unknown**. See also the preceding note.

Related references

- [Hardware Overview Page](#)
- [Modify Brick, Components Tab](#)

Related tasks

- [Display Hardware Component Status](#)

Modify Scheduled Job Dialog

Navigation: Scheduled Jobs > Actions > Modify Schedule

Allows you to change the properties of an existing scheduled job. You can also enable or disable the schedule from this page.

Schedule Name

Identifies the name of the schedule.

Data Protection Type

Identifies the type of data protection, such as clone, that is used in the schedule.

Volume Group

Allows you to assign the clone volume to an existing volume group.

Enabled

Indicates whether the schedule is enabled.

- Enable the schedule so that the operation is performed at the specified time.
- Disable the schedule so that operations are not performed. This option allows you to define a schedule before the source volume (LUN or Clone LUN) has been made available to users.

Protected Volume

Identifies the name of the volume (LUN or Clone LUN) from which a scheduled data protection will be created.

Start Time

Identifies the date and time at which the Pillar Axiom system starts a scheduled operation.

Recurrence

Identifies how often the system should perform the scheduled operation. Valid values vary based on the schedule's recurrence interval and frequency.

Related references

- [*Scheduled Jobs Overview Page*](#)
- [*View Scheduled Job Dialog*](#)

Related tasks

- [*Modify a LUN Data Protection Schedule*](#)
- [*Create LUN Data Protection Schedules*](#)

Modify Event Notification Dialog

Navigation: Event Notification > Actions > Modify Event Notification

Use the Modify Event Notification dialog to modify event notices when specified events occur. When an event is triggered, the Pillar Axiom system sends a notification to the designated recipients.

Name

Identifies the name of the event notification.

Description

Describes the event notification.

Enable Event Notification

Indicates whether the event notification is enabled. When checked, this option activates the notification when the event occurs on the Pillar Axiom system.

Event Notification Recipient Email Addresses

Identifies the email addresses of the recipients who are to receive event notifications. The email server to which the Pillar Axiom system sends notifications must be able to send messages to these email addresses.

Add

Allows you to add email recipients to the event notification.

Test Email

Sends a message to the specified email addresses to test recipient email addresses. Recipients should look for a message that is titled "[Axiom-QoS] Test email" in their email in-boxes.

Remove

Deletes the selected email address from the list.

Monitored Events

Lists events that are defined in the selected categories.

You can sort the list of events in one of two ways:

**By severity,
then category**

Sorts the list by severity with a list of event categories. The severity categories include:

	Informational	Requires no action for events that are information only.
	Warning	Requires no immediate action for minor conditions that you can address at your convenience.
	Critical	Requires prompt action to prevent system failures or offline conditions.
By category, then severity	Sorts the list by categories with a list of event severity.	
	Security	Events to notify of a security problem such as unauthorized request.
	Audit	Events that keep track of what users are doing, such as the operations that they performed.
	System	Events to notify of system problems, such as a missing Brick or Slammer.

Related references

- [Event Notification Overview Page](#)
- [System Event Severities](#)
- [Pillar Axiom System Limits](#)

Related tasks

- [Modify an Event Notification](#)

Modify Reporting Schedule Dialog

Navigation: *Reporting > Reporting Schedules > Modify Schedule*

Use the Modify Reporting Schedule dialog to make changes to the selected reporting schedule.

Schedule Name

Displays the name of the schedule.

Report Type

Specifies the type of report the schedule generates. Report types include:

- SAN Hosts
- Storage Performance
- Storage Use
- Storage Use per Volume
- System Configuration
- System Configuration Summary

Start Time

Specifies the date and time to begin generating reports.

Schedule Frequency

Specifies the frequency at which the schedule generates reports. Frequencies include:

- Run Once
- Hourly
- Daily
- Weekly

Recurrence

Specifies how many hours, days, or weeks to wait before generating this scheduled report again.

Related concepts

- [*About Scheduled Reports*](#)

Related tasks

- [*Create a Reporting Schedule*](#)
- [*Modify a Reporting Schedule*](#)

Modify Slammer, Components tab

Navigation: Hardware > Slammers > Actions > Modify Name > Components

Use the Modify Slammer, Component tab to review the status of Slammers. If there is a hardware failure, click the failed component. The Pillar Axiom Storage Services Manager takes you to the Guided Maintenance that will help you through the process of resolving the hardware failure.

Note: For more information on Guided Maintenance, refer to the *Pillar Axiom Service Guide*.

Name

Identifies the name that is assigned to a hardware component. Assign unique, meaningful component names to help you more easily locate specific components. The Pillar Axiom system maps the assigned name to the component's serial number and updates the map if you modify the component name.

Memory per CU

The amount of memory available to each control unit (CU).

Serial Number

Displays the serial number of the Slammer.

Replaceable Unit

Displays the Slammer component that is replaceable. Select a component, and then click **Replace Component** to start Guided Maintenance.

Control Unit

Identifies a specific CU in a Slammer. Each Slammer contains two CUs.

Status

Displays the current status of the hardware component. A status of Normal requires no action.

Part Number

Displays the part number of the replaceable hardware component.

Serial Number

Displays the serial number of the replaceable hardware component.

Related references

- [*Modify Slammer, I/O Ports Tab*](#)
- [*Hardware Overview Page*](#)

Related tasks

- [*Display Hardware Component Status*](#)
- [*Identify the Hardware Component*](#)
- [*Replace a FRU*](#)

Modify Slammer, I/O Ports Tab

Navigation: Hardware > Slammer > Actions > Modify Name > I/O Ports

Use the Modify Slammers, I/O Ports tab to review the status of the Fibre Channel (FC) and Internet Small Computer System Interface (iSCSI) interfaces of Slammers. You can also review the Fabric Switch interfaces, as well as the data path and management interfaces of Slammers.

Port

Lists by type the FC and iSCSI ports on a Slammer:

- **Private Interconnect Module (PIM)**
 - FC0 through FC3
 - FS0 through FS9
 - ETH0 through ETH2
- **Network Interface Module (NIM)**
 - 2-port NIM: PORT0 and PORT1
 - 4-port NIM: PORT0 through PORT3

Control Unit

Identifies a control unit (CU) of the Slammer.

Connection Type

Identifies the types of network ports for data path traffic between the customer network switches and the Pillar Axiom Slammers:

- **Copper:** Identifies RJ-45 copper interfaces.
- **Long Wave Optical:** Identifies longwave optical small form-factor pluggable (SFP) transceiver interfaces.
- **Short Wave Optical:** Identifies shortwave optical SFP transceiver interfaces.
- **Unknown:** Connection type cannot be determined.

Status

Identifies the connection status of the port.

The Pillar Axiom user interfaces (GUI and CLI) show that host Fibre Channel (FC) HBA ports are either **Connected** or **Not Connected** to the Slammer ports. The meaning of **Connected** is that the HBA port on the SAN host has logged in

to the port on the Slammer using the FC protocol. In most operating systems, host ports log in to the Slammer ports immediately after the two are physically connected and enabled and remain logged in until the physical connection is broken. So, **Connected** effectively means that there is an enabled physical connection between the ports.

Note: On HP-UX platforms, however, some HBA device drivers use a different approach—they log out from the connection when there is no traffic to send. An HP-UX HBA port often shows as **Not Connected** even though there is an enabled physical connection between the ports.

Bandwidth

Displays the transmission speed of the port.

Topology

Identifies the FC transport topology in use by the ports in the network interface module (NIM) to connect to the storage area network (SAN) employed by the customer:

- **Fabric:** means that the port is an N_Port in a switched fabric (FC-SW).
- **Loop:** means that the port is an NL_Port in an arbitrated loop (FC-AL).
- **Point-to-Point:** means that the port is an N_Port that is connected to another N_Port, back to back (FC-P2P).
- **Public Loop:** means that the port is an NL_Port that is connected to a loop in which one port in the loop is an FL_Port in the fabric (FC-FLA).

Note: The topology used by Storage System Fabric (SSF) between the Slammer PIMs and the Brick RAID controllers is private and therefore not reported.

SFP Status

Displays the status of the SFP transceiver.

- **Bypassed**
- **Bypassed-No SFP**
- **Bypassed-Incorrect Speed**
- **Bypassed-Read Error**
- **Bypassed-Incorrect Type**
- **Bypassed-Lost Sync**

If the interface module itself should fail, the SFP status shows **Hardware Failure**.

Note: The **SFP Status** and **SFP Vendor** fields display information only when version 2 private interconnect modules (PIMs) are connected to version 2 SATA controllers using optical SFPs. In all other cases, these two fields are blank.

SFP Vendor

Displays the vendor's part number for the SFP. If that information is not available, the system displays **Unknown**. See also the preceding note.

SFP Part Number

Displays the vendor's part number for the SFP. If that information is not available, the field is blank or displays **Unknown**. See also the preceding note.

SFP Revision

Displays the part revision number for the SFP. If that information is not available, the field is blank or displays **Unknown**. See also the preceding note.

Related references

- [Hardware Overview Page](#)
- [Modify Slammer, Components tab](#)

Related tasks

- [Display Hardware Component Status](#)

Pilot Overview Page

Navigation: Hardware > Pilots

Allows you to review the status of the Pilot management controller that is installed on the Pillar Axiom system.

Control Unit

Identifies the control unit (CU) of the Pilot.

Status

Displays the current status of a CU within the Pilot. A status of Normal requires no action.

Mode

Displays the current operational mode of the two CUs within the Pilot. Valid options:

Active	Indicates which CU performs all configuration tasks that administrators request.
---------------	--

Standby	Indicates which CU acts as a secondary device and does nothing unless the active CU fails over to this standby control unit.
----------------	--

OS Version

Identifies the operating system version of the Pilot.

Server Version

Identifies the software version installed on the Pillar Axiom system.

Serial Number

Identifies the serial number that is assigned to the hardware component.

Related references

- [Hardware Overview Page](#)

Related tasks

- [Identify the Hardware Component](#)

Reporting Overview Page

Navigation: *Reporting*

Use the Reporting Overview page to choose between scheduling or generating statistical reports about your network and Pillar Axiom system, or viewing statistics as trending charts.

Reports provide information about the status of your system at a point in time. You can generate a report when you need one, or you can arrange for reports to be generated at scheduled times. You can download reports in a variety of textual formats.

The Pillar Axiom system collects statistical information about the LUNs and the Slammer storage controllers in your storage network. You can view this information in tables or in trending charts. Trending charts provide a graphical display of statistics collected over time. You can use trending charts to visually monitor or compare the displayed values of these statistics.

Scheduled Reports

Opens the Reporting Schedules overview page.

Generated Reports

Opens the Generated Reports overview page.

Related concepts

- [*About Generated Reports*](#)
- [*About Scheduled Reports*](#)

Related references

- [*Generated Reports Overview Page*](#)
- [*Reporting Schedules Overview Page*](#)

Related tasks

- [*Generate a Report*](#)
- [*Create a Reporting Schedule*](#)

Reporting Schedules Overview Page

Navigation: *Reporting > Scheduled Reports*

Use the Reporting Schedules page to create a new reporting schedule, view or modify an existing reporting schedule, or delete an existing reporting schedule. When you create a reporting schedule, it is listed on this page.

Name

Displays the name of the schedule.

Report Type

Specifies the type of report the schedule generates. Report types include:

- SAN Hosts
- Storage Performance
- Storage Use
- Storage Use per Volume
- System Configuration
- System Configuration Summary

Start Time

Specifies the date and time to begin generating reports.

Frequency

Specifies the frequency at which the schedule generates reports. Frequencies include:

- Run Once
- Hourly
- Daily
- Weekly

Enabled

Specifies whether this schedule is enabled.

If a schedule is not enabled, you can modify the schedule at a later time to enable it.

Related concepts

- [*About Scheduled Reports*](#)

Related references

- [*Create Reporting Schedule Dialog*](#)
- [*Modify Reporting Schedule Dialog*](#)
- [*View Reporting Schedule Dialog*](#)

Related tasks

- [*Create a Reporting Schedule*](#)
- [*Modify a Reporting Schedule*](#)
- [*View a Reporting Schedule*](#)
- [*Delete a Reporting Schedule*](#)

SAN Slammer Protocol Statistics and Trending Overview Page

Navigation: *Statistics and Trending > SAN > Slammer Protocols*

Allows you to review statistics for storage area network (SAN) protocols and create trending charts from SAN protocol statistics.

Slammer

Identifies the name of the Slammer that contains TCP/IP statistics.

Control Unit

Identifies the control unit (CU) of the Slammer that contains the statistics.

Network Interface

Identifies the physical port on the CU.

Port Type

Identifies the Slammer port connection type, Fibre Channel (FC) or Internet Small Computer System Interface (iSCSI).

Negotiated Link Speed

Displays the transmission speed in gigabits/second for the port.

Average Throughput (per Second)

Displays the average throughput in MB/second.

- **Read:** The average read throughput in MB/second.
- **Write:** The average write throughput in MB/second.

Average I/O Latency

Identifies the average time to complete the read or write operations.

Average I/O Size

Identifies the average size of the read and write operations.

Commands Received (per Second)

Displays the number of read and write commands received each second over the last sampling period.

Channel Errors Since Activated

Displays the cumulative number of errors that have occurred on the channel since the Slammer control unit was started.

Collection Period

Identifies the start and end times at which information was last collected from the Pillar Axiom system.

Related concepts

- [*About SAN Slammer Statistics*](#)
- [*About SAN Slammer Statistics Trending Charts*](#)

Related references

- [*View Details Dialog \(FC Slammers\)*](#)
- [*View Details Dialog \(iSCSI Slammers\)*](#)
- [*Slammer Statistics Trending Dialog*](#)
- [*Pillar Axiom System Limits*](#)

Related tasks

- [*View SAN Slammer Statistics*](#)
- [*Configure a SAN Slammer Statistics Trending Chart*](#)

SAN Statistics and Trending Overview Page

Navigation: *Statistics and Trending > SAN*

Use the SAN Statistics and Trending Overview page to select the type of SAN statistics to display.

LUNs

Opens the LUN Statistics and Trending Overview page, where you can view LUN statistics, create trending charts, and export trending chart data.

Slammer Protocols

Opens the SAN Slammer Protocol Statistics and Trending Overview page, where you can view SAN protocol statistics, create trending charts, and export trending chart data.

Related references

- [*LUN Statistics and Trending Overview Page*](#)
- [*SAN Slammer Protocol Statistics and Trending Overview Page*](#)

Related tasks

- [*Configure a LUN Statistics Trending Chart*](#)
- [*Configure a SAN Slammer Statistics Trending Chart*](#)

Scheduled Jobs Overview Page

Navigation: Scheduled Jobs

Allows you to review a list of scheduled jobs that are actions performed at the specified time or at regular intervals. The Actions drop-down menu allows you to view, modify, and delete scheduled jobs.

Name

Identifies the name of a scheduled operation.

Start Time

The date and time the task is scheduled to start.

Type

Identifies the type of data protection used in the schedule.

Enable

Identifies whether the scheduled replication is enabled.

Enabled

Indicates that the scheduled event performs at the specified time.

Disabled

Indicates that the operation will not perform as scheduled.

Related references

- [View Scheduled Job Dialog](#)
- [Modify Scheduled Job Dialog](#)

Related tasks

- [View a Job Schedule](#)
- [Schedule the Software Update](#)
- [Cancel a Scheduled Software Update](#)
- [Delete a LUN Data Protection Schedule](#)
- [Create LUN Data Protection Schedules](#)

Set Event Log Filter Dialog

Navigation: Event Log > Actions > Set Event Log Filter

Use the Set Event Log Filter dialog to create and modify the event filters that are configured on the Pillar Axiom system.

Event Categories

Identifies a list of event categories. Choose from:

Security	Events to notify of a security problem such as unauthorized request.
Audit	Events that keep track of what users are doing, such as the operations that they performed.
System	Events to notify of system problems, such as a missing Brick or Slammer.

Event Severities

Identifies a list of event types. Choose from:

Informational	Requires no action for events that are information only.
Warning	Requires no immediate action for minor conditions that you can address at your convenience.
Critical	Requires prompt action to prevent system failures or offline conditions.

Event Date Range

Indicates whether to filter events by occurrence date.

Display Events that occur in a date range	Enable this option to activate the Beginning date and Ending date options. Disable this option so that events are filtered by type and severity only.
Beginning date	Specifies the date so that events that occurred on or after this date, and that match the selected filters, are displayed.
Ending date	Specifies the date so that events that occurred on or before this date, and that match the selected filters, are displayed.

Reset to Defaults

Resets the page to default values. Selecting this option enables all of the Event Severities and Event Categories, and clears any set date range.

Related references

- [*Event Log Overview Page*](#)

Related tasks

- [*Filter Event Log Entries*](#)
- [*Display the Event Log*](#)
- [*Display the Event Properties*](#)

Slammers Overview Page

Navigation: Hardware > Slammers

Allows you to review the Slammers that are a part of the Pillar Axiom system. Options available from this page allow you to rename the Slammers, run diagnostics, locate Slammer on the Pillar Axiom system, and view Slammer details.

Slammer Name

Lists the names of hardware components. Click a name to display details about that hardware component.

Type

Lists the type of Slammer.

Control Unit

Identifies a control unit (CU) of the Slammer.

CU Status

Displays the current status of the CU. A status of Normal requires no action.

Temperature

Displays the temperature status of the Slammer.

Chassis

Displays the current status of the Slammer Chassis.

Motherboard Assembly

Displays the current status of the Slammer Motherboard Assembly.

Power Supplies

Displays the current status of the Slammer power supplies.

Fans

Displays the current status of the Slammer fans.

Batteries

Displays the current status of the Slammer batteries.

Private Interconnect Module

Displays the current status of the Slammer Private Interconnect Module (PIM).

Network Interface Module

Displays the current status of the Slammer Network Interface Module (NIM).

Related references

- [*Hardware Overview Page*](#)
- [*View Slammer, Components Tab*](#)
- [*View Slammer, I/O Ports Tab*](#)

Related tasks

- [*Display Hardware Component Status*](#)
- [*Modify a Hardware Component Name*](#)
- [*Identify the Hardware Component*](#)
- [*Replace a FRU*](#)

Statistics and Trending Overview Page

Navigation: *Statistics and Trending*

Use the Statistics and Trending Overview page to select performance statistics and trending charts that are available on the Pillar Axiom system.

SAN Statistics

Opens the SAN Statistics page, where you can choose LUN Statistics and Trending or Slammer Protocols Statistics and Trending.

Related references

- [SAN Statistics and Trending Overview Page](#)
- [Pillar Axiom System Limits](#)

Related tasks

- [View LUN Statistics](#)
- [View SAN Slammer Statistics](#)
- [Configure a LUN Statistics Trending Chart](#)
- [Configure a SAN Slammer Statistics Trending Chart](#)

Statistics Trending Dialogs

To view details about the Slammer or LUN Statistics Trending dialogs, choose one of:

- [LUN Statistics Trending Dialog](#)
- [Slammer Statistics Trending Dialog](#)

LUN Statistics Trending Dialog

Navigation: *Statistics and Trending > SAN > LUNs > Actions > LUN Statistics Trending*

Use the LUN Statistics Trending dialog to configure, display, or print a trending chart, or to export a previously configured trending chart.

Configure Trending Chart

Opens the Configure Trending Chart page, where you can specify the Pillar Axiom objects and statistics to chart.

Export

Opens the Export page, where you can choose a file format and location for exporting the data in a trending chart to a file on your workstation.

Related concepts

- [About LUN Statistics Trending Charts](#)

Related references

- [Configure Trending Chart, Trend Configuration Tab \(LUNs\)](#)
- [Configure Trending Chart, Chart Thresholds Tab \(LUNs\)](#)
- [Configure Trending Chart, Data Filtering Tab \(LUNs\)](#)
- [Export Dialog](#)

Related tasks

- [Configure a LUN Statistics Trending Chart](#)
- [Export a Trending Chart](#)
- [Print a Trending Chart](#)

Slammer Statistics Trending Dialog

Navigation: *Statistics and Trending > SAN > Slammer Protocols > Actions > Slammer Statistics Trending*

Use the Slammer Statistics Trending dialog to configure, display, or print a trending chart, or to export a previously configured trending chart.

Configure Trending Chart

Opens the Configure Trending Chart page, where you can specify the Pillar Axiom objects and statistics to chart.

Export

Opens the Export page, where you can choose a file format and location for exporting the data in a trending chart to a file on your workstation.

Related concepts

- [*About SAN Slammer Statistics Trending Charts*](#)

Related references

- [*Configure Trending Chart, Trend Configuration Tab \(Slammers\)*](#)
- [*Configure Trending Chart, Chart Thresholds Tab \(Slammers\)*](#)
- [*Configure Trending Chart, Data Filtering Tab \(Slammers\)*](#)
- [*Export Dialog*](#)

Related tasks

- [*Configure a SAN Slammer Statistics Trending Chart*](#)
- [*Export a Trending Chart*](#)
- [*Print a Trending Chart*](#)

Summary of System Status Overview Page

Navigation: Status Summary

Use the Summary of System Status overview page to review the status and health of the Pilot, Slammers, and Bricks that are installed on the Pillar Axiom system.

Pilots

The Pilots table lists the following information:

Control Unit

Identifies a control unit (CU) in a hardware component.

Mode

Displays the current operational mode of the two CUs within the Pilot.

- **Active:** Indicates which CU performs all configuration tasks that administrators request.
- **Standby:** Indicates which CU acts as a secondary device and does nothing unless the active CU fails over to this standby control unit.

Status

Displays the current status of a CU within the Pilot. A status of Normal requires no action.

Slammers

The Slammers table lists the following information:

Slammer Name

Lists the names of hardware components.

Type

Lists the type of Slammer.

CU0 Status

Identifies the status for control unit 0 (CU0).

CU1 Status

Identifies the status for control unit 1 (CU1).

UPSs

The uninterruptible power supply (UPS) table lists the following information:

UPS Name

Identifies the name assigned to the external UPS device.

Power Source

Identifies the source of the UPS power. Valid sources:

- AC (alternating current)
- Battery
- Unknown

Battery Status

Identifies the current status of the UPS batteries. Valid values:

- Normal
- Warning
- Critical
- Unknown

Bricks

The Bricks table lists the following information:

Brick Name

Lists the names of hardware components.

Status

Identifies the status of the hardware components.

Event Log

The Event Log table lists the following information:

Severity

The event log severity lists the following event types:

- Informational
- Critical
- Warning

Number of Events

The number of events that have occurred on the Pillar Axiom system.

Event Notification

The Event Notification table lists the following information:

- **Enabled Email Subscriptions:** Indicates the number of event notifications that are currently enabled.
- **Number of Monitored system Events:** Indicates the number of monitored events.
- **Disabled Email Subscriptions:** Indicates the number of event notifications that are currently disabled.
- **Number of Recipients:** Indicates the total number of email recipients.

Refresh

Updates the page with current data.

Related references

- [*System Alerts Overview Page*](#)
- [*Event Log Overview Page*](#)
- [*Event Notification Overview Page*](#)
- [*Hardware Overview Page*](#)

System Alerts Overview Page

*Navigation: **System Alerts***

Use the System Alerts overview page to manage alerts that are generated when specific events occur. You can copy the system alert information to your workstation clipboard or remove the alert as necessary.

Alert

Identifies item that caused the system alert.

Time Occurred

Indicates the date and time the system alert occurred.

Affected Items

Identifies the name of the system object that caused the system alert.

Description

Provides a brief description of the system alert.

Related concepts

- [*About Managing Event Notifications*](#)

Related tasks

- [*Manage System Alerts*](#)
- [*Display System Alerts*](#)
- [*Display Hardware Component Status*](#)

System Event Severities

The Pillar Axiom system generates events and classifies them by severity.

Table 27 Pillar Axiom event severities

Severity	Explanation
Critical	Access to data is compromised.
Warning	Administrator action is required to prevent a soft error from becoming a hard error or critical event.
Informational	A configuration change has been detected or another non-error event has occurred.

View Brick, Components Tab

Navigation: Hardware > Bricks > Actions > View Details > Components

Use the View Brick, Component tab to review the status of Bricks. If there is a hardware failure, click the failed component. The Pillar Axiom Storage Services Manager takes you to Guided Maintenance which will help you through the process of resolving the hardware failure.

Note: For more information on Guided Maintenance, refer to the *Pillar Axiom Service Guide*.

Brick Name

Identifies the name that is assigned to a hardware component. Assign unique, meaningful component names to help you more easily locate specific components. The Pillar Axiom system maps the assigned name to the component's serial number and updates the map if you modify the component name.

Serial Number

Displays the serial number of the selected Brick.

Brick ID

Displays the World Wide Name (WWN) of the selected Brick.

By default, the Bricks are assigned names such as /Brick001, based on a simple sort of the component's internal Fibre Channel WWN. This is the logical Brick name and is not necessarily the same as the physical Brick location. You can assign any name to a Brick.

Firmware Number

Identifies the drive firmware version number.

Replaceable Unit

Displays the Brick component that is replaceable. Select a component, and then click **Replace Component** to start Guided Maintenance.

Status

Displays the current status of a hardware component. A status of Normal requires no action.

Part Number

Displays the part number of a hardware component.

Serial Number

Displays the serial number of a hardware component.

Related references

- [*View Brick, I/O Ports Tab*](#)
- [*Hardware Overview Page*](#)

Related tasks

- [*Display Hardware Component Status*](#)
- [*Identify the Hardware Component*](#)
- [*Replace a FRU*](#)

View Brick, I/O Ports Tab

Navigation: Hardware > Bricks > Actions > View Details > I/O Ports

Use the View Brick, I/O Ports tab to review the status of the Fibre Channel (FC) interfaces of Bricks.

Port

Lists by type the FC ports on a Brick:

- **RAID Controller Module** (0 or 1)
- **FC0 through FC3** or **Cascade** (FC Bricks only)

Status

Identifies the connection status of the port.

The Pillar Axiom user interfaces (the GUI and CLI) show that host Fibre Channel (FC) HBA ports are either **Connected** or **Not Connected** to the Slammer ports. The meaning of **Connected** is that the HBA port on the SAN host has logged in to the port on the Slammer using the FC protocol. In most operating systems, host ports log in to the Slammer ports immediately after the two are physically connected and enabled and remain logged in until the physical connection is broken. So, **Connected** effectively means that there is an enabled physical connection between the ports.

Note: On HP-UX platforms, however, some HBA device drivers use a different approach—they log out from the connection when there is no traffic to send. An HP-UX HBA port often shows as **Not Connected** even though there is an enabled physical connection between the ports.

Bandwidth

Displays the transmission speed of the port.

Connection Type

Identifies the types of connectors between the RAID controller and the Brick:

- **Copper:** Identifies RJ-45 copper interfaces.
- **Long Wave Optical:** Identifies longwave optical small form-factor pluggable (SFP) transceiver interfaces.
- **Short Wave Optical:** Identifies shortwave optical SFP transceiver interfaces.
- **Unknown:** Connection type cannot be determined.

SFP Status

Displays the status of the small form-factor pluggable (SFP) transceiver.

If the interface module itself should fail, the SFP status shows **Hardware Failure**.

Note: The **SFP Status** and **SFP Vendor** fields display information only when version 2 private interconnect modules (PIMs) are connected to version 2 SATA controllers using optical SFPs. In all other cases, these two fields are blank.

SFP Vendor

Displays the SFP manufacturer. If that information is not available, the field is blank or displays **Unknown**. See also the preceding note.

SFP Part Number

Displays the vendor's part number for the SFP. If that information is not available, the field is blank or displays **Unknown**. See also the preceding note.

SFP Revision

Displays the part revision number for the SFP. If that information is not available, the field is blank or displays **Unknown**. See also the preceding note.

Related references

- [View Brick, Components Tab](#)
- [Hardware Overview Page](#)

Related tasks

- [Display Hardware Component Status](#)

View Scheduled Job Dialog

Navigation Scheduled Jobs > Actions > View Schedule

Allows you to review the properties of a selected scheduled job.

Schedule Name

Identifies the unique name of a scheduled operation, which is an action to be performed at the specified time or at regular intervals.

Data Protection Type

Identifies the type of data protection, such as clone, that is used in the schedule.

Volume Group

Identifies the volume group to which the clone is assigned.

Protected Volume

Identifies the name of the volume (LUN or Clone LUN) from which a scheduled data protection will be created.

Enabled

Indicates whether the schedule is enabled.

- Enable the schedule so that the operation is performed at the specified time.
- Disable the schedule so that operations are not performed. This option allows you to define a schedule before the source volume (LUN or Clone LUN) has been made available to users.

Start Time

Identifies the date and time at which the Pillar Axiom system starts a scheduled operation.

Recurrence

Identifies how often the system should perform the scheduled operation. Valid values vary based on the schedule's recurrence interval and frequency.

Related references

- [*Scheduled Jobs Overview Page*](#)
- [*Modify Scheduled Job Dialog*](#)

Related tasks

- [*View a LUN Data Protection Schedule*](#)
- [*Create LUN Data Protection Schedules*](#)

View Details Dialog (LUNs)

Navigation: *Statistics and Trending > SAN > LUNs > Actions > View Details*

Allows you to see detailed information about the LUN you have selected on the SAN LUN Statistics and Trending page.

Name

Identifies the name of the selected LUN.

Axiom Performance

Specifies the continued load, over two minute sample periods, that is placed on the selected LUN.

Read Throughput	Identifies the data transfer rate for data inputs (reads) of the specified LUN.
Write Throughput	Identifies the data transfer rate for data outputs (writes) of the specified LUN.
Total Throughput	Indicates the average data transfer rate for data read and write operations of the specified LUN.
Read IOPS	Indicates the average number of read (input) I/O operations per second.
Write IOPS	Indicates the average number of write (output) I/O operations per second.
Total IOPS	Identifies the combined for input and output I/O operations per second.

System Load

Specifies the performance of the LUN while processing I/O requests.

Read Throughput	Identifies the data transfer rate for data inputs (reads) of the specified LUN.
Write Throughput	Identifies the data transfer rate for data outputs (writes) of the specified LUN.
Total Throughput	Indicates the average data transfer rate for data read and write operations of the specified LUN.

Read IOPS	Indicates the average number of read (input) I/O operations per second.
Write IOPS	Indicates the average number of write (output) I/O operations per second.
Total IOPS	Identifies the combined for input and output I/O operations per second.

I/O Latency

Specifies the average time to complete a read or write operation (in milliseconds) and the average operation size (in KB).

Read Response Time	Identifies the average time to perform a read operation in the last sample period.
Write Response Time	Identifies the average time to perform a write operation in the last sample period.
Combined Response Time	Identifies the average time to perform a read or write operation in the last sample period.
Read Operation Size	Identifies the average size of a read operation in the last sample period.
Write Operation Size	Identifies the average size of a write operation in the last sample period.

General

Specifies the I/O activity of the cache usage.

Cache Flushes per Second	Identifies the rate that the cache lines were flushed-to-disk for each second in the last sample period.
Cache Hit Ratio	Identifies the percentage of read operations that were serviced from the Read Cache (also called cache hits) in the last sample period.
Read-Ahead IOPS	Identifies the average I/Os for each second spent on read-ahead fetching based on the read access behavior in the last sample period.
Non-Optimized IOPS	Identifies the average I/Os for each second that pass through non-optimized data paths in the last sample period.

Related concepts

- [About LUN Statistics](#)

Related tasks

- [View LUN Statistics](#)

View Details Dialog (FC Slammers)

Navigation: *Statistics and Trending > SAN > Slammer Protocols > Actions > View Details*

Allows you to see detailed information about the Fibre Channel (FC) Slammer port you have selected on the SAN Slammer Protocol Statistics and Trending page.

Name

Identifies the name of the Slammer port.

Control Unit

Identifies the number of the Slammer control unit (CU).

Slammer Node Port Name

Identifies the name of the Slammer port node.

Port Type

Identifies the type of Slammer port (FC or iSCSI).

General Information

Read Throughput	Identifies the data transfer rate for data inputs (reads).
Write Throughput	Identifies the data transfer rate for data outputs (writes).
Total Throughput	Identifies the average combined input and output data transfer rates (reads and writes).
Total IOPS	Identifies the total number of I/O operations per second.

Performance

Max Read Throughput	Identifies the maximum input data transfer rate (reads).
Max Write Throughput	Identifies the maximum output data transfer rate (writes).
Max Total Throughput	Identifies the maximum combined input and output data transfer rate (reads and writes).
Max Read IOPS	Identifies the maximum number of input (read) I/O operations per second.

Max Write IOPS	Identifies the maximum number of output (write) I/O operations per second.
Max Total IOPS	Identifies the maximum total number of input and output (read and write) I/O operations per second.

SCSI Task Management Operations

Abort Task	Indicates the number of abort task commands processed on the selected port.
Abort Task Set	Indicates the number of commands to abort a task set processed on the selected port. A task set is a group of tasks.
Clear ACA	Indicates the number of Clear ACA (Auto Contingent Allegiance) commands processed on the selected port.
Clear Task Set	Indicates the number of commands to clear a task set processed on the selected port.
Logical Unit Reset	Indicates the number of commands to reset a logical unit processed on the selected port.
Target Reset	Indicates the number of commands to reset a target processed on the selected port.

I/O Latency

Specifies the average time to complete a read or write operation (in milliseconds) and the average operation size (in KB).

Read Response Time	Identifies the average time to perform a read operation in the last sample period.
Write Response Time	Identifies the average time to perform a write operation in the last sample period.
Combined Response Time	Identifies the average time to perform a read or write operation in the last sample period.
Read Operation Size	Identifies the average size of a read operation in the last sample period.

Write Operation Size	Identifies the average size of a write operation in the last sample period.
Channel Errors	
Total Channel Errors	Indicates the total number of channel error associated with this port.
Command Timeout Errors	Indicates the number of command timeout errors that have occurred on the channel associated with this port.
DMA Errors	Indicates the number of Direct Memory Access (DMA) errors that have occurred on the channel associated with this port.
Invalid RXID Errors	Indicates the number of invalid receiver exchange identifier (RXID) errors that have occurred on the channel associated with this port.
Loop Init Errors	Indicates the number of loop initialization errors that have occurred on the channel associated with this port.
Overflow Errors	Indicates the number of overflow errors that have occurred on the channel associated with this port.
PCI Errors	Indicates the number of Peripheral Component Interconnect (PCI) errors that have occurred on the channel associated with this port.
Port Unavailable Errors	Indicates the number of port unavailable errors that have occurred on the channel associated with this port.
Reselection Timeout Errors	Indicates the number of re-selection timeout errors that have occurred on the channel associated with this port.
RND Errors	Indicates the number of RND errors that have occurred on the channel associated with this port. A faulty SPF on an FC switch might cause these errors.
System Errors	Indicates the number of system errors that have occurred on the channel associated with this port.
Unacknowledged Host Event Errors	Indicates the number of unacknowledged host event errors that have occurred on the channel associated with this port.
Underrun Errors	Indicates the number of underrun errors that have occurred on the channel associated with this port.

Transfer Errors

Indicates the number of data transfer errors that have occurred on the channel associated with this port.

Loop Activity

LIPs

Indicates the number of loop initialization primitive (LIP) activities taking place on this port.

Loop Ups

Indicates the number of loop up activities taking place on this port.

Loop Downs

Indicates the number of loop down activities taking place on this port.

Related concepts

- [About SAN Slammer Statistics](#)

Related references

- [SAN Slammer Protocol Statistics and Trending Overview Page](#)

Related tasks

- [View SAN Slammer Statistics](#)

View Details Dialog (iSCSI Slammers)

Navigation: *Statistics and Trending > SAN > Slammer Protocols > Actions > View Details*

Allows you to see detailed information about the iSCSI Slammer port you have selected on the SAN Slammer Protocol Statistics and Trending page.

Name

Identifies the name of the Slammer port.

Control Unit

Identifies the number of the Slammer control unit (CU).

Slammer Node Port Name

Identifies the name of the Slammer port node.

Port Type

Identifies the type of Slammer port (FC or iSCSI).

General Information

Read Throughput	Identifies the data transfer rate for data inputs (reads).
Write Throughput	Identifies the data transfer rate for data outputs (writes).
Total Throughput	Identifies the average combined input and output data transfer rates (reads and writes).

Performance

Max Read Throughput	Identifies the maximum input data transfer rate (reads).
Max Write Throughput	Identifies the maximum output data transfer rate (writes).
Max Total Throughput	Identifies the maximum combined input and output data transfer rate (reads and writes).
Max Read IOPS	Identifies the maximum number of input (read) I/O operations per second.
Max Write IOPS	Identifies the maximum number of output (write) I/O operations per second.

Max Total IOPS	Identifies the maximum total number of input and output (read and write) I/O operations per second.
-----------------------	---

SCSI Task Management Operations

Abort Task	Indicates the number of abort task commands processed on the selected port.
Abort Task Set	Indicates the number of commands to abort a task set processed on the selected port. A task set is a group of tasks.
Clear ACA	Indicates the number of Clear ACA (Auto Contingent Allegiance) commands processed on the selected port.
Clear Task Set	Indicates the number of commands to clear a task set processed on the selected port.
Logical Unit Reset	Indicates the number of commands to reset a logical unit processed on the selected port.
Target Reset	Indicates the number of commands to reset a target processed on the selected port.

I/O Latency

Specifies the average time to complete a read or write operation (in milliseconds) and the average operation size (in KB).

Read Response Time	Identifies the average time to perform a read operation in the last sample period.
Write Response Time	Identifies the average time to perform a write operation in the last sample period.
Combined Response Time	Identifies the average time to perform a read or write operation in the last sample period.
Read Operation Size	Identifies the average size of a read operation in the last sample period.
Write Operation Size	Identifies the average size of a write operation in the last sample period.

iSCSI Port Errors

Underrun Errors	Indicates the number of underrun errors during the collection period.
Overrun Errors	Indicates the number of overrun errors during the collection period.
Command Timeout Errors	Indicates the number of command timeout errors during the collection period.
DMA Errors	Indicates the number of Direct Memory Access (DMA) errors during the collection period.
Transport Errors	Indicates the number of transport errors during the collection period.
Device Unavailable Errors	Indicates the number of device unavailable errors during the collection period.
Data Digest Errors	Indicates the number of data digest errors during the collection period.
Header Digest Errors	Indicates the number of header digest errors during the collection period.
Invalid Snack Errors	Indicates the number of invalid snack errors during the collection period.
Unsolicited Data Errors	Indicates the number of unsolicited data errors during the collection period.
Unexpected Data SN Errors	Indicates the number of unexpected data storage network (SN) errors during the collection period.
Initiator Task Tag Errors	Indicates the number of initiator task tag errors during the collection period.
System Errors	Indicates the number of system errors during the collection period.
MAC CRC Errors	Indicates the number of Media Access Control Cyclic Redundancy Check (MAC CRC) errors during the collection period.
MAC Encoding Errors	Indicates the number of MAC encoding errors during the collection period.

iSNS Errors	Indicates the number of Internet storage name service (iSNS) errors during the collection period.
Command PDUs Rejected	Indicates the number of command Protocol Data Unit (PDUs) rejected during the collection period.
Connection Failures	Indicates the number of connection failures during the collection period.
Session Login Failures	Indicates the number of session login failures during the collection period.
FW Dump Errors	Indicates the number of firmware (FW) dump errors during the collection period.

iSCSI Port Requests

Reinitialize Requests	Indicates the number of re-initialization requests during the collection period.
Target Cold Reset Requests	Indicates the number of cold target reset requests during the collection period.
Task Reassign Requests	Indicates the number of task reassign requests during the collection period.
iSNS Messages	Indicates the number of iSNS messages during the collection period.

iSCSI Port Events

Link Up Events	Indicates the number of link up events during the collection period.
Link Down Events	Indicates the number of link down events during the collection period.
IP Address Change Events	Indicates the number of IP address change events during the collection period.
Duplicate IP Address Events	Indicates the number of duplicate IP address events during the collection period.

Related concepts

- [*About SAN Slammer Statistics*](#)

Related references

- [*SAN Slammer Protocol Statistics and Trending Overview Page*](#)

Related tasks

- [*View SAN Slammer Statistics*](#)

View Event Notification Dialog

Navigation: Event Notification > Actions > View Event Notification

Use the View Event Notification dialog to review event notices. When an event is triggered, the Pillar Axiom system sends a notification to the designated email recipients.

Name

Identifies the name of the event notification.

Description

Describes the event notification.

Enable Event Notification

Indicates whether the event notification is enabled. When checked, this option activates the notification when the event occurs on the Pillar Axiom system.

Event Notification Recipient Email Addresses

Identifies the email addresses of the recipients who are to receive event notifications. The email server to which the Pillar Axiom system sends notifications must be able to send messages to these email addresses.

Monitored Events

Lists events that are defined in the selected categories.

Note: Although you can make changes to the Monitored Events list, you cannot save your changes.

Related references

- [Event Notification Overview Page](#)
- [System Event Severities](#)
- [Pillar Axiom System Limits](#)

Related tasks

- [View Event Notification Details](#)
- [Create an Event Notification](#)

View Reporting Schedule Dialog

Navigation: *Reporting > Reporting Schedules > View Schedule*

Use the View Reporting Schedules dialog to review details of the selected reporting schedule.

Schedule Name

Displays the name of the schedule.

Report Type

Specifies the type of report the schedule generates. Report types include:

- SAN Hosts
- Storage Performance
- Storage Use
- Storage Use per Volume
- System Configuration
- System Configuration Summary

Start Time

Specifies the date and time to begin generating reports.

Schedule Frequency

Specifies the frequency at which the schedule generates reports. Frequencies include:

- Run Once
- Hourly
- Daily
- Weekly

Recurrence

Specifies how many hours, days, or weeks to wait before generating this scheduled report again.

View Slammer, Components Tab

Navigation: Hardware > Slammers > Actions > View Details > Components

Use the View Slammer, Components tab to review the status of Slammers. If there is a hardware failure, click the failed component. The Pillar Axiom Storage Services Manager takes you to the Guided Maintenance that will help you through the process of resolving the hardware failure.

Note: For more information on Guided Maintenance, refer to the *Pillar Axiom Service Guide*.

Slammer Name

Identifies the name that is assigned to a hardware component. Assign unique, meaningful component names to help you more easily locate specific components. The Pillar Axiom system maps the assigned name to the component's serial number and updates the map if you modify the component name.

Memory per CU

The amount of memory available to each control unit (CU).

Serial Number

Displays the serial number of the Slammer.

Replaceable Unit

Displays the Slammer component that is replaceable. Select a component, and then click **Replace Component** to start Guided Maintenance.

Control Unit

Identifies a specific control unit (CU) in a Slammer. Each Slammer contains two CUs.

Status

Displays the current status of a hardware component. A status of Normal requires no action.

Part Number

Displays the part number of a hardware component.

Serial Number

Displays the serial number of a hardware component.

Related references

- [*View Slammer, I/O Ports Tab*](#)
- [*Hardware Overview Page*](#)

Related tasks

- [*Display Hardware Component Status*](#)
- [*Identify the Hardware Component*](#)
- [*Replace a FRU*](#)

View Slammer, I/O Ports Tab

Navigation: Hardware > Slammer > Actions > View Details > I/O Ports

Use the View Slammers, I/O Ports tab to review the status of the Fibre Channel (FC) and Internet Small Computer System Interface (iSCSI) interfaces of Slammers. You can also review the Fabric Switch interfaces, as well as the data path and management interfaces of Slammers.

Port

Lists by type the FC and iSCSI ports on the Slammer.

Private Interconnect Module (PIM)	FC0 through FC2 FS0 through FS9 ETH0 through ETH2
Network Interface Module	2-port NIM: PORT0 and PORT1 4-port NIM: PORT0 through PORT3

Control Unit

Identifies a control unit (CU) of the Slammer.

Connection Type

Identifies the types of network ports for data path traffic between the customer network switches and the Pillar Axiom Slammers.

Copper	Identifies RJ-45 copper interfaces.
Long Wave Optical	Identifies longwave optical small form-factor pluggable (SFP) transceiver interfaces.
Short Wave Optical	Identifies shortwave optical SFP transceiver interfaces.
Unknown	Connection type cannot be determined.

Status

Identifies the connection status of the port.

The Pillar Axiom user interfaces (the GUI and CLI) show that host Fibre Channel (FC) HBA ports are either **Connected** or **Not Connected** to the Slammer ports. The meaning of **Connected** is that the HBA port on the SAN host has logged in to the port on the Slammer using the FC protocol. In most operating systems, host ports log in to the Slammer ports immediately after the two are physically connected and enabled and remain logged in until the physical connection is broken. So, **Connected** effectively means that there is an enabled physical connection between the ports.

Note: On HP-UX platforms, however, some HBA device drivers use a different approach—they log out from the connection when there is no traffic to send. An HP-UX HBA port often shows as **Not Connected** even though there is an enabled physical connection between the ports.

Bandwidth

Displays the transmission speed of the port.

Topology

Identifies the FC transport topology in use by the ports in the network interface module (NIM) to connect to the storage area network (SAN) employed by the customer:

Fabric	Indicates that the port is an N_Port in a switched fabric (FC-SW).
Loop	Indicates that the port is an NL_Port in an arbitrated loop (FC-AL).
Point-to-Point	Indicates that the port is an N_Port that is connected to another N_Port, back to back (FC-P2P).
Public Loop	Indicates that the port is an NL_Port that is connected to a loop in which one port in the loop is an FL_Port in the fabric (FC-FLA).

Note: The topology used by Storage System Fabric (SSF) between the Slammer PIMs and the Brick RAID controllers is private and therefore not reported.

SFP Status

Displays the status of the small form-factor pluggable (SFP) transceiver.

- **Bypassed**
- **Bypassed-No SFP**
- **Bypassed-Incorrect Speed**
- **Bypassed-Read Error**
- **Bypassed-Incorrect Type**
- **Bypassed-Lost Sync**

If the interface module itself should fail, the SFP status shows **Hardware Failure**.

Note: The **SFP Status** and **SFP Vendor** fields display information only when version 2 private interconnect modules (PIMs) are connected to version 2 SATA controllers using optical SFPs. In all other cases, these two fields are blank.

SFP Vendor

Displays the vendor's part number for the SFP. If that information is not available, the system displays **Unknown**. See also the preceding note.

SFP Part Number

Displays the vendor's part number for the SFP. If that information is not available, the field is blank or displays **Unknown**. See also the preceding note.

SFP Revision

Displays the part revision number for the SFP. If that information is not available, the field is blank or displays **Unknown**. See also the preceding note.

Related references

- [View Slammer, Components Tab](#)
- [Hardware Overview Page](#)

Related tasks

- [Display Hardware Component Status](#)

Uninterruptible Power Supplies Overview Page

Navigation: Hardware > UPS

Allows you to review the current status of the uninterruptible power supply (UPS) battery and power. The Pillar Axiom system retrieves information from each device using Simple Network Management Protocol (SNMP) over the Pilot Ethernet connection to monitor and report status. This page provides options to create and manage the UPS devices connected to the Pillar Axiom system.

Name

Identifies the name assigned to the external UPS device.

IP Address

Identifies the IP address that is assigned to the external UPS device.

Model

Identifies the model number of the UPS device.

Power Source

Identifies the source of the UPS power. Valid sources:

- AC (alternating current)
- Battery
- Unknown

Battery Status

Identifies the current status of the UPS batteries. Valid values:

- Normal
- Warning
- Critical
- Unknown

Related references

- [*Create UPS Dialog*](#)
- [*Modify UPS Dialog*](#)
- [*Hardware Overview Page*](#)
- [*Summary of System Status Overview Page*](#)
- [*SNMP Hosts Overview Page*](#)

Related tasks

- [*Create a UPS Device*](#)
- [*Modify a UPS Device*](#)
- [*View a UPS Device*](#)
- [*Delete a UPS Device*](#)

Create UPS Dialog

Navigation: Hardware > UPS > Actions > Create UPS

Allows you to connect an uninterruptible power supply (UPS) device to the Pillar Axiom system using a simple network management protocol (SNMP).

Name

Identifies the name of the UPS device. UPS names must be unique across the Pillar Axiom system and must be 256 or fewer UTF-8 characters.

IP Address

Identifies the IP address that is assigned to the external UPS device.

SNMP Community

Identifies a community for which a specific trap host should receive traps that the Pillar Axiom system generates. You can specify different community strings for each trap host so that multiple administrators can receive specific types of SNMP traps. The default community string is **public** (lower case).

Related references

- [Uninterruptible Power Supplies Overview Page](#)
- [Modify UPS Dialog](#)
- [Hardware Overview Page](#)
- [Summary of System Status Overview Page](#)

Related tasks

- [Create a UPS Device](#)
- [Modify a UPS Device](#)
- [View a UPS Device](#)
- [Delete a UPS Device](#)

Modify UPS Dialog

Navigation: Hardware > UPS > Actions > Modify UPS

Allows you to change the properties of a selected uninterruptible power supply (UPS) device. For example, you can assign the UPS device to an alternate simple network management protocol (SNMP) community string.

Name

Identifies the name of the UPS device. UPS names must be unique across the Pillar Axiom system and must be 256 or fewer UTF-8 characters.

IP Address

Identifies the IP address that is assigned to the external UPS device.

SNMP Community

Identifies a community for which a specific trap host should receive traps that the Pillar Axiom system generates. You can specify different community strings for each trap host so that multiple administrators can receive specific types of SNMP traps. The default community string is **public** (lower case).

Current Status

Provides read-only details and status about the UPS device.

Model

Identifies the model number of the UPS device.

Firmware Revision

Identifies the firmware version that is installed on the UPS device.

Serial Number

Identifies the serial number of the UPS device.

Power Source

Identifies the source of the UPS power. Valid sources:

- AC (alternating current)
- Battery
- Unknown

Battery Status

Identifies the current status of the UPS batteries. Valid values:

- Normal

- Warning
- Critical
- Unknown

Related references

- [*Uninterruptible Power Supplies Overview Page*](#)
- [*Create UPS Dialog*](#)
- [*Hardware Overview Page*](#)
- [*Summary of System Status Overview Page*](#)

Related tasks

- [*Modify a UPS Device*](#)
- [*Delete a UPS Device*](#)

View UPS Dialog

Navigation: Hardware > UPS > Actions > View UPS

Allows you to review the properties of a selected uninterruptible power supply (UPS) device.

Name

Identifies the name of the UPS device. UPS names must be unique across the Pillar Axiom system and must be 256 or fewer UTF-8 characters.

IP Address

Identifies the IP address that is assigned to the external UPS device.

SNMP Community

Identifies a community for which a specific trap host should receive traps that the Pillar Axiom system generates. You can specify different community strings for each trap host so that multiple administrators can receive specific types of SNMP traps. The default community string is **public** (lower case).

Current Status

Provides read-only details and status about the UPS device.

Model

Identifies the model number of the UPS device.

Firmware Revision

Identifies the firmware version that is installed on the UPS device.

Serial Number

Identifies the serial number of the UPS device.

Power Source

Identifies the source of the UPS power. Valid sources:

- AC (alternating current)
- Battery
- Unknown

Battery Status

Identifies the current status of the UPS batteries. Valid values:

- Normal

- Warning
- Critical
- Unknown

Related references

- [*Uninterruptible Power Supplies Overview Page*](#)
- [*Create UPS Dialog*](#)
- [*Modify UPS Dialog*](#)
- [*Hardware Overview Page*](#)
- [*Summary of System Status Overview Page*](#)

Related tasks

- [*View a UPS Device*](#)
- [*Modify a UPS Device*](#)

APPENDIX D

Protect Tab Reference Pages

Data Protection Overview Page

Navigation: Data Protection

Allows you to access data protection tasks to manage clones and clone schedules.

Protection Schedules

Opens the Protection Schedules overview page where you can create and manage data protection schedules.

LUN Protection

Opens the LUN Protection overview page where you can create an immediate Clone LUN, restore a LUN from a clone, and enable or disable the data path for a LUN.

Related references

- [Protection Schedules Overview Page](#)
- [SAN LUN Protection Overview Page](#)

Protection Schedules Overview Page

Navigation: Data Protection > Protection Schedules

Allows you to review a summary of the data protection schedules. You can review the schedule names, the date and time for the schedule to start, and the protected volume (LUN or Clone LUN). This page provides options to create and manage the data protection schedules.

Name

Identifies the name of a schedule. Select a schedule name and use the Actions menu to review or modify the schedule settings.

Start Time

Identifies the time and date on which the Pillar Axiom system started a schedule recurrence.

Frequency

Identifies the interval at which the Pillar Axiom system starts a recurrent schedule.

Protected Volume/LUN

Identifies the name of the protected volume from which a Clone LUN was created.

Enabled

Identifies whether the data protection schedule is enabled.

- Yes: Indicates that the schedule is actively cloning the protected volumes.
- No: Indicates that the schedule is not cloning the protected volumes.

Related concepts

- [About Data Replicas and System Capacity](#)

Related references

- [Pillar Axiom System Limits](#)

Related tasks

- [View Protection Schedules](#)
- [Create LUN Data Protection Schedules](#)
- [Modify a LUN Data Protection Schedule](#)
- [View a LUN Data Protection Schedule](#)
- [Delete a LUN Data Protection Schedule](#)

Create Data Protection Schedule Dialog

Navigation: Data Protection > Protection Schedules > Create Schedule

Allows you to create a data replication (clone) schedule on a selected volume (LUN or Clone LUN).

Schedule Name

Identifies the unique name of a scheduled operation, which is an action to be performed at the specified time or at regular intervals.

Data Protection Type

Identifies the type of data protection, such as clone, that is used in the schedule.

Enable

Identifies whether the scheduled replication is enabled.

Enabled

Indicates that the scheduled event performs at the specified time.

Disabled

Indicates that the operation will not perform as scheduled.

Volume to Replicate

Identifies the name of the volume (LUN or Clone LUN) from which a scheduled data protection will be created.

Number of Existing Clones

Identifies the number of child Clone LUNs associated with the existing LUN.

Used Capacity Allocated for Clones

Displays the amount of space allocated for Clone LUNs.

Maximum Capacity Allocated for Clones

Displays the maximum space allocated for Clone LUNs.

Start Time

Specifies the date and time to begin scheduling replication.

Schedule Frequency

Specifies the frequency at which the scheduled replication runs. Frequencies include:

- Run Once

- Hourly
- Daily
- Weekly

Recurrence

Identifies how often the system should perform the scheduled operation. Valid values vary based on the schedule's recurrence interval and frequency.

Related concepts

- [*About Managing Clone LUNs*](#)

Related references

- [*Pillar Axiom System Limits*](#)

Related tasks

- [*Create LUN Data Protection Schedules*](#)
- [*Create an Immediate Clone LUN*](#)

Modify Data Protection Schedule Dialog (Protect tab)

Navigation: Data Protection > Protection Schedules > Actions > Modify Schedule

Allows you to manage the properties of an existing data protection schedule. You can also enable or disable the schedule from this page.

Schedule Name

Identifies the name of the schedule.

Data Protection Type

Identifies the type of data protection, such as clone, that is used in the schedule.

Enabled

Specifies whether the scheduled replication is enabled.

Enabled	Indicates that the scheduled event performs at the specified time.
----------------	--

Disabled	Indicates that the operation will not perform as scheduled. Disable the schedule, for example, when the source volume (LUN or Clone LUN) has not been made available to users.
-----------------	--

Protected Volume

Identifies the name of the volume (LUN or Clone LUN) from which a scheduled data protection will be created.

Schedule

Specifies the date and time to begin scheduling replication.

Specifies the frequency at which the scheduled replication runs. Frequencies include:

- Run Once
- Hourly
- Daily
- Weekly

Recurrence

Specifies how many hours, days, or weeks to wait before generating this scheduled job again.

Valid values are listed in the following table.

Table 28 Job schedule recurrence intervals

Recurrence interval	Valid values
Hourly	1 through 24
Daily	1 through 7
Weekly	1 through 4

Related concepts

- [About Managing Clone LUNs](#)

Related references

- [Protection Schedules Overview Page](#)
- [Pillar Axiom System Limits](#)

Related tasks

- [View a LUN Data Protection Schedule](#)
- [Modify a LUN Data Protection Schedule](#)
- [Delete a LUN Data Protection Schedule](#)
- [View Protection Schedules](#)

View Data Protection Schedule Dialog

Navigation: Data Protection > Protection Schedules > View Schedule

Allows you to review the data protection schedule properties.

Schedule Name

Identifies the name of the scheduled job.

Data Protection Type

Identifies the type of data protection, such as clone, that is used in the schedule.

Volume Group

Identifies the volume group to which the clone is assigned.

Enabled

Specifies whether the scheduled replication is enabled.

Enabled

Indicates that the scheduled event performs at the specified time.

Disabled

Indicates that the operation will not perform as scheduled. Disable the schedule, for example, when the source volume (LUN or Clone LUN) has not been made available to users.

Protected Volume

Identifies the name of the volume (LUN or Clone LUN) from which a scheduled data protection will be created.

Schedule

Identifies the schedule of the data protection.

Recurrence

Identifies the interval by which the scheduled job occurs.

Related concepts

- [*About Managing Clone LUNs*](#)

Related references

- [*Protection Schedules Overview Page*](#)

Related tasks

- [*View Protection Schedules*](#)
- [*Modify a LUN Data Protection Schedule*](#)
- [*Delete a LUN Data Protection Schedule*](#)
- [*Create an Immediate Clone LUN*](#)

SAN LUN Protection Overview Page

Navigation: Data Protection > LUN Protection

Allows you to review the volume (LUN or Clone LUN) properties that have been defined on the Pillar Axiom system. This page provides options to create an immediate clone, delete volumes, restore a LUN from a selected Clone LUN, and enable or disable the volume from the SAN host data path.

Name

Identifies the name that is assigned to a LUN for administrative purposes.

Status

Identifies the current status of each LUN. Valid types:

Online	Indicates that the LUN is fully accessible.
Offline	Indicates that the LUN is not accessible.
Inactive	Indicates that the LUN cannot be accessed from the data path.
Partial Offline	Indicates that the actual redundancy level may be different from the redundancy level with which the volume was configured.
Degraded	Indicates that all of the copies of a redundant volume are not available. If one copy is missing, it is not fully redundant. This can happen when a write to one copy of the array fails (which may be a 30 second time-out).
Conservative	Indicates that write-back cache has been disabled so journaling has slowed.

Host Access

Identifies the SAN host mapping status associated with the LUN. Valid types:

- Mapped
- No Mappings
- Inactive
- All

Protocol Access

Identifies the access protocol used to map the LUN to the Slammer.
Protocols include:

- FC only
- iSCSI only
- No Access
- All

Groups

Displays which volume group or storage domain to which the logical volumes belongs.

Volume Group	Lists the name of the volume group where the logical volume is located.
---------------------	---

Storage Domain	Specifies the name of the Storage Domain.
-----------------------	---

Logical Capacity (GB)

Displays the storage requirements for the logical volumes.

Allocated	Identifies the initial capacity that is assigned to the logical volume. This value is a soft limit, which means that data can be stored in a logical volume until the maximum capacity is reached.
------------------	--

Addressable	Identifies the maximum capacity to which the logical volume can grow. For a clone, this field identifies how much addressable space will be available.
--------------------	--

Logical Distribution	Identifies a graphical representation of the initial capacity that is assigned to the logical volume. This value is a soft limit, which means that data can be stored in a logical volume until the maximum capacity is reached.
-----------------------------	--

Physical Capacity for Clone LUNs

Displays the physical storage usage for the Clone LUNs.

Logical Maximum	Identifies the amount of storage that was requested for the clone repository.
------------------------	---

Physical Used	Identifies the current volume capacity usage of the object.
Physical Allocated	Identifies the total amount of storage capacity that is reserved on the system.
Physical Maximum	Identifies the maximum capacity to which the logical volume can grow. For clones, this field identifies how much addressable space is available.

Total Physical Capacity (GB)

Displays the total physical storage capacity for the logical volumes and Clone LUNs.

Redundancy	Identifies how many mirror copies of the original data are stored online.
Disk Protection	Indicates the RAID drive data protection method.
LUN Overhead	Identifies the physical and logical storage capacity that is required to meet the LUN Quality of Service (QoS) settings.
Allocated	Specifies the amount of raw capacity in gigabytes (GB) that has been assigned and designated to this logical volume.
Maximum	Identifies the maximum capacity for the volume group. The maximum capacity of the logical volumes and nested volume groups that are associated with the volume group cannot exceed this value. A value of 0 (zero) identifies that the volume group is configured with unlimited capacity. You can increase the maximum capacity of associated logical volumes and nested volume groups without constraints.
Physical Distribution	A graphical representation of the capacity used compared to the maximum allocated.

Priority Level

Identifies the assigned priority level when the volume was created.

- Premium

- High
- Medium
- Low
- Archive

Global LUN Number

Identifies the globally unique identifier of the LUN.

LUID

Identifies the unique identifier of the LUN.

Related concepts

- [*About Managing Clone LUNs*](#)
- [*About Creating LUNs*](#)

Related references

- [*Pillar Axiom System Limits*](#)

Related tasks

- [*Create an Immediate Clone LUN*](#)
- [*Delete a LUN*](#)
- [*Delete All Clone LUNs*](#)
- [*Restore a LUN from a Clone LUN*](#)
- [*Enable the Data Path of a LUN*](#)
- [*Disable the Data Path of a LUN*](#)

Replication Engines Overview Page

Navigation: Replication Engines

Allows you to view the status of the available Replication Engines registered with the Pillar Axiom system. You can access the Pillar Axiom MaxRep interface for the Replication Engine from this page.

Agent Status

Identifies the communication status of the Pillar Axiom 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 version of Pillar Axiom MaxRep software running on the Replication Engine.

Related tasks

- [*Manage a Replication Engine*](#)

APPENDIX E

Support Tab Reference Pages

Add RAID Controller to Clear History Dialog

Navigation: Tools > System Logs > Delete Log Bundles > Add

Use the Add RAID Controller to Clear History dialog to select the specific RAID controller for which you want to delete system logs.

Brick

Select from the drop-down list the Brick that contains the RAID controller for which you want to delete system logs.

Raid Group

Select from the drop-down list the name of the RAID controller whose system logs you want to delete.

Related references

- [Delete Log Bundles Dialog](#)
- [Create Log Bundle Dialog](#)

Create Log Bundle Dialog

Navigation: Tools > System Logs > Actions > Create Log Bundle

Use the Create Log Bundle dialog to specify the scope of the system information for the Pillar Axiom system that you want to collect.

Collection Reason

Provides information about the system logs collection. This information may be used to communicate the purpose of the logs or specify to the recipient a timestamp or log of interest. The Pillar Axiom system saves this information in the header of the Call-Home log files.

Component or Item

Provides a list of available hardware components and system events for data collection.

- **Collect:** Indicates whether the object is selected for data collection.
- **Name:** Indicates the name of the object for data collection.

Select buttons

Use the select buttons to specify all or a group of system components.

- **Select All:** Sets all hardware and system events in the list to **Yes**. This selection provides a record of all events on the system.
- **Deselect All:** Resets the available hardware and system events in the list to **No** so that no logs are collected.
- **Select All Slammers:** Sets all Slammers in the list to **Yes**. This selection provides a record of events that have occurred on the Slammers. This button only affects Slammers.
- **Select All Bricks:** Sets all Bricks in the list to **Yes**. This selection provides a record of performance, capacity usage, and system health information. This button only affects Bricks.

Collection Period

Controls the extent of information coverage for each selected source:

- **Most Recent Logs:** Indicates the age of the collected data logs. For example, a setting of 4 hours means that the logs are less than 4 hours old.
- **All Logs:** Indicates that the data collection logs are continually updated.

SAN Host Log Selection

Allows you to select the SAN host for log collection:

Number of hosts selected for log collection	Indicates the number of hosts selected for log collection.
Select Hosts	<p>Opens a dialog that allows you to select recognized SAN hosts on the system for log collection.</p> <ul style="list-style-type: none">■ Collect: Indicates whether the host is selected for data collection■ SAN host: Indicates the name of the SAN host for data collection

Automatically send log bundle to Call-Home server

Sends the data logs collection as a .tar file bundle to the Call-Home server.

Related references

- [System Logs Overview Page](#)
- [Pillar Axiom System Limits](#)

Related tasks

- [Create a Log Bundle](#)
- [Send Logs to Call-Home Server](#)

Data Consistency Overview Page

Navigation: Tools > Data Consistency

Allows you to review the data consistency test results for the Pillar Axiom Bricks. You can perform the data consistency test from this page.

Brick Name

Identifies the name of the Brick.

Status

Identifies the state of the Brick. Valid states:

- Normal
- Warning
- Critical
- Unknown

Date of Result

Specifies the date and time when the data consistency test was completed.

Consistency Result

Specifies the result of the data consistency test. Valid results:

- Pass
- Fail

Errors Found

Identifies the number of consistency test errors.

Errors Fixed

Identifies the number of errors corrected during the test.

Related concepts

- [About Data Consistency](#)

Related tasks

- [Verify Data Consistency](#)

Delete Log Bundles Dialog

Navigation: Tools > System Logs > Actions > Delete Log Bundles

Use the Delete Log Bundles dialog to clear the system logs from the Pillar Axiom system. You may select which system logs to remove: All or specific Brick logs, Slammer logs, or log collections.

Note: Deleting system logs requires support administrator login privileges. Contact Pillar Data Systems Technical Support before proceeding.

Slammer Logs

Selects all Slammer logs on the system.

Brick Logs

Selects all Brick logs on the system.

Log Collections

Selects all logs on the system.

RAID Controller History to Clear

Brick

Identifies the Brick names selected for deletion.

Raid Group

Identifies the RAID Group associated with the selected brick that is selected for deletion.

Add

Opens the Add Raid Controller to Clear History dialog, which allows you to select the specific Brick RAID controller to clear.

Remove

Removes the selected object from the list of pending log deletions.

Clear

Removes all selected objects from the list of pending log deletions.

Related references

- [Add RAID Controller to Clear History Dialog](#)

Related tasks

- [Delete Log Bundles](#)
- [Create a Log Bundle](#)

Drive Firmware Overview Page

Navigation: Tools > Drive Firmware

Allows you to upload, install, and remove the drive firmware for the Pillar Axiom system.

Summary

Provides the version number of the available drive firmware and information about the Drive Firmware feature.

Staged Package

Identifies the version of the drive firmware package uploaded (staged) on the Pillar Axiom system.

Pending Drive Firmware Updates

Provides information about the drives that match the specifications for the firmware update.

Brick

Identifies the name of the Brick.

Drive Number

Identifies the number of the drive for firmware update.

Current Firmware Version

Identifies the drive firmware version number.

Pending Firmware Version

Identifies the version number of the drive firmware installed for update.

Related concepts

- [*About the Drive Firmware Update*](#)

Related tasks

- [*Upload the Drive Firmware Package*](#)
- [*Update the Drive Firmware*](#)
- [*Remove the Drive Firmware Package*](#)

Manage Halt Points Dialog

Navigation: Tools > System Halt Points > Manage Halt Points

Manages the system halt points that are available on the Pillar Axiom system. A halt point on a particular software component causes the system to pause the startup sequence at some step associated with that component so that troubleshooting and diagnostic actions can be performed.



Caution

System halt points are to be used for recovery purposes only. They are used to gather information or to clear conditions that cannot otherwise be accomplished. Halt points should never be set or cleared without assistance from the Oracle Pillar Customer Support. Management of system halt points can only be performed by the Primary administrator and the Support administrator.

Active

Indicates whether the startup process is to halt at the indicated step for this software component.

Order

Identifies where in the startup sequence the software component step is to be executed.

Current

Indicates whether the software component step is currently halted.

Component Name

Identifies the name of the software component that is associated with the system halt point.

Step

Identifies the name of the software component step where the halt point is to occur.

Clear

Click this button to disable all system halt points. See the **Current** field for a list of affected halt points.

Related concepts

- [About System Halt Points](#)

Related tasks

- [Manage System Halt Points](#)

Reset System Dialog

Navigation: Tools > System Trouble > Actions > Reset System

Use the Reset System dialog to reset your system configuration as directed by the Oracle Pillar Customer Support.

Resetting the system configuration, performs the following actions:

- Deletes all data stored on the Pillar Axiom system.
- Resets the configuration to an initial state.
- Resets the system serial number.



Caution

Because this action deletes all user data along with the system configuration, the system prompts you to confirm the operation. Be absolutely sure you want to take this action, because all data in your system will be lost.

Browse [...]

Allows you to select the filename and folder location for the encryption file provided by the Oracle Pillar Customer Support.

Related tasks

- [Reset Pillar Axiom System](#)

Software Modules Page

Navigation: Software Modules

Use the Software Modules page to install new versions of firmware and software on the Pillar Axiom system, schedule a software update, and view the current software versions or upgrade paths for the system.

Software Update Scheduled

Note: The Software Update Scheduled information appears if there is an active software update schedule.

Task Name

Identifies the type of scheduled task: Software Update.

Scheduled Start Time

Indicates the date and time of the schedule software update.

Cancel Scheduled Update

Allows you to remove the scheduled software update.

Installed Software

Package Version

Identifies the version number of a software module after the software update is complete.

Compatibility Matrix Version

Identifies what software components are supported and compatible with specific hardware component versions in the system.

Module

Identifies the name of a software or firmware module that is installed on the Pillar Axiom system.

Table 29 Software module types

Name	Description
Pilot OS	Operating system for the Pilot.
Pilot Software	Software that runs on the Pilot, such as the GUI interface and web server, online help, Simple

Table 29 Software module types (continued)

Name	Description
	Network Management Protocol (SNMP), and Network Data Management Protocol (NDMP).
Slammer PROM, AX600	Programmable ROM (PROM), which includes BIOS and netboot code, for storage area network (SAN) Slammers. Pillar Axiom 600 systems display the <i>AX600</i> suffix.
Slammer Software, AX600	SAN software that runs on Slammers. Pillar Axiom 600 systems display the <i>AX600</i> suffix.
Brick SATA2 Firmware	RAID firmware for serial ATA (SATA) Bricks. Pillar Axiom systems that contain version 2 SATA controllers display the <i>SATA2 Firmware</i> suffix. Note: Version 2 SATA RAID controllers have 16 ports to support the Storage System Fabric (SSF). Version 1 SATA controllers have 13 such ports.
Brick FC Firmware	RAID firmware for Fibre Channel (FC) Bricks.
Brick Disk Drive Firmware	Drive firmware for Bricks.

Version

Identifies the version number of a software module. A value of *unsupported* indicates that an individual software module was upgraded or downgraded.

Applies to Current Hardware (*Support roles only*)

Indicates that the affected hardware component uses the software module.

Staged Software**Package Version**

Identifies the version number of a software module after the software update is complete.

Can Upgrade to Staged Version

Indicates that an upgrade path is available based on the installed software module version and the staged software package.

Upload Software Package

Permits you to navigate to and select a software update package so that you can:

- Copy the package from its distribution media to the staged packages that are available for installation.
- Install the package components on the Pillar Axiom system.

Related references

- [*Pillar Axiom System Limits*](#)

Related tasks

- [*Download Firmware and Software Updates*](#)
- [*Update the Pillar Axiom Software*](#)
- [*Schedule the Software Update*](#)
- [*Cancel a Scheduled Software Update*](#)

System Halt Points Overview Page

Navigation: Tools > System Halt Points

Allows the administrator to view the halt points, if any, that have been enabled on the Pillar Axiom system.

Order

Identifies where in the startup sequence the software component step is to be executed.

Current

Indicates whether the software component step is currently halted.

Component Name

Identifies the name of the software component that is associated with the system halt point.

Step

Identifies the name of the software component step where the halt point is to occur.

Related concepts

- [About System Halt Points](#)

Related tasks

- [Manage System Halt Points](#)

System Logs Overview Page

Navigation: Tools > System Logs

Use the System Logs overview page to review collected system information and run the collection tools that are available on a Pillar Axiom system.

Content

Lists the name of the bundle file (compressed tar filename) containing the collected system information.

Time Collected

Identifies the time and date at which the download bundle was collected from the Pillar Axiom system.

Collection Type

Indicates the method by which the system logs are collected:

Manual	Indicates user initiated system logs.
Event Generated	Indicates event triggered system logs.
Periodic	Indicates occasional Call-Home. system logs.

Target

Identifies the types of system information that have been collected and are included in the current download bundle.

Size

Identifies the size of the download bundle.

Reason

Provides information about the system logs collection.

Related references

- [Create Log Bundle Dialog](#)
- [Pillar Axiom System Limits](#)

Related tasks

- [Create a Log Bundle](#)
- [Delete Log Bundles](#)
- [Send Logs to Call-Home Server](#)

System Trouble Overview Page

Navigation: Tools > System Trouble

Use the System Trouble Overview page to review the status and health of the Slammers that are installed on the Pillar Axiom system. The **Actions** menu options allow you to test the connectivity between the Pillar Axiom system and the customer network as well as reset the system to an initial state.

Slammer Name

Identifies the name of the Slammer for which you want to test connectivity.

Type

Identifies if the type of Slammer attached to Pillar Axiom system.

Control Unit

Identifies the Slammer control unit (CU) number and the physical network port in the network interface module on that Slammer CU.

CU Status

Displays the status of the Slammer CU.

Network Interface Module

Displays the status of the Network Interface Module (NIM).

Related concepts

- [About Pillar Axiom Diagnostics](#)
- [About Responding to System Alerts](#)

Related references

- [Tools Overview Page](#)
- [Test Connectivity Dialog](#)
- [Run PITMAN Diagnostics Dialog](#)
- [Pillar Axiom System Limits](#)

Related tasks

- [Reset Pillar Axiom System](#)
- [Test System Connectivity](#)

Test Connectivity Dialog

Navigation: Tools > System Trouble > Actions > Test Connectivity

Use the Test Connectivity Dialog to help resolve a connectivity issue between the specified Slammer and the customer network.

Slammer

Identifies the Slammer for which you want to resolve connectivity issues.

Control Unit

Identifies a specific control unit (CU) in a Slammer and the physical network port in the network interface module on that Slammer CU.

Command Line

Identifies a command to perform to resolve a connectivity issue between the specified Slammer and the customer network.

Environment Variables

Identifies the space-delimited pairs of environment variables and values to use while executing the command.

Execute

Performs the specified command.

Command Output

Displays the results of the command line that was run to resolve a connectivity issue. The command output cannot be saved to a file.

Related concepts

- [About Pillar Axiom Diagnostics](#)

Related references

- [Slammer Connectivity Commands](#)
- [Pillar Axiom System Limits](#)

Related tasks

- [Test System Connectivity](#)

Tools Overview Page

Navigation: Tools

Use the Tools Overview page to select any of the types of support tools that are available on a Pillar Axiom system. After you select a type, you can select and perform the specified support operation to help diagnose and resolve system issues.

Data Consistency

Select this option to perform data consistency tests on selected Bricks.

System Logs

Select this option to create, view, download, and send the system logs to the Call-Home server.

System Trouble

Select this option to view the status and health of the installed Slammers. This option allows you to test the system connectivity and reset the system serial number and configuration.

System Halt Points

Select this option to view the active halt points on the Pillar Axiom system. This option allows you to manage system halt points for diagnostic purposes.

Note: Working with system halt points is intended for Oracle Pillar Customer Support personnel.

Related concepts

- [About Pillar Axiom Diagnostics](#)

Related references

- [System Logs Overview Page](#)
- [System Trouble Overview Page](#)
- [Manage Halt Points Dialog](#)
- [Pillar Axiom System Limits](#)

Run PITMAN Diagnostics Dialog

Navigation: Tools > System Trouble > Actions > Run PITMAN Diagnostics

Allows you to troubleshoot Storage System Fabric (SSF) faults.

Command Parameter

Identifies PITMAN commands to be performed on the Slammer control unit (CU).

[Table 30: PITMAN commands](#) describes the PITMAN commands.

Execute

Performs the specified PITMAN command.

Command Output

Displays the results of the PITMAN command. The command output cannot be saved to a file.

Table 30 PITMAN commands

Command	Command and syntax
SetAutoModeOn	<p>SetAutoModeOn</p> <p>Sets the operational state to Automatic mode.</p> <p>When in this mode, PITMAN actively monitors link errors and automatically starts diagnostic cycles, if link errors are detected.</p> <p>Note: PITMAN rejects any manual commands when it is running in the Automatic mode.</p> <p>Note: The default runtime mode for PITMAN is Automatic for the Slammer CU.</p>
SetAutoModeOff	<p>SetAutoModeOff</p> <p>Sets the operation state to Manual mode.</p> <p>When in this mode, PITMAN stops any automatic diagnostic cycles in progress and stops monitoring link errors. PITMAN takes no action even if link errors are detected.</p> <p>Note: The default runtime mode for PITMAN is Automatic for the Slammer CU.</p>
GetPitmanStatus	GetPitmanStatus

Table 30 PITMAN commands (continued)

Command	Command and syntax
	Queries the current mode and state of PITMAN and displays the results in the Command Output field in the Run PITMAN Diagnostic dialog.
GetMarksDb	<p>GetMarksDb RecordCount={<i>x</i> <i>all</i>}</p> <p>x Displays the specified number of records from the MARKS database.</p> <p>all Displays all the records from the MARKS database.</p> <p>Note: This command displays the specified number of latest records from the MARKS database and is different from log collection using different Call-Home methods.</p> <p>Example:</p> <p>GetMarksDb RecordCount=10</p> <p>GetMarksDb RecordCount=all</p> <p>The contents of the specified number of records of the MARKS database is displayed in the Run PITMAN Diagnostic dialog.</p>
GetMarksDb Summary	<p>GetMarksDb Summary</p> <p>Displays a summary of the content of the MARKS database in the Run PITMAN Diagnostic dialog.</p>
PushMarksDbToPilot	<p>PushMarksDbToPilot</p> <p>Directs the content in the MARKS database to the Pilot to collect logs for the Call-Home feature since the MARKS database is too large to be held in the GUI or CLI output buffer.</p>
TrafficGenOn	<p>TrafficGenOn mode={<i>manual</i> <i>auto</i>} peer={<i>nodename</i> <i>all</i>} initiator=<i>portname</i> target=<i>portname</i></p> <p>mode>manual If the mode is Manual, the traffic generator uses the specified initiator and target ports.</p> <p>mode=auto If the mode is Automatic, the traffic generator automatically selects the initiator and target ports to equally distribute the generated traffic through a particular FC network.</p>

Table 30 PITMAN commands (continued)

Command	Command and syntax
	<p>peer=all Indicates that all Slammers and Bricks that own the ports of the FC network are being tested.</p> <p>peer=nodename Indicates that all Slammers and Bricks that own the ports of the FC network are being tested. In a 4-Slammer system, where one FC network is shared by two Private Interconnect Module (PIMs), either Slammer CUs that contain the PIMs can be specified.</p> <p>initiator=portname Slammer ports are identified by the Slammer name, CU number, and the port label name printed on the metal cage of the Slammer. Brick ports are identified by the Brick name, RC number, and the port label name printed on the Brick.</p> <p>target=portname</p> <p>Generates traffic between the specified ports of the Bricks and Slammers.</p> <p>Note: This command is only available when PITMAN is operating in the Manual mode.</p> <p>Example:</p> <p>TrafficGenOn mode=auto peer=all</p> <p>TrafficGenOn mode=auto peer=0x2008000b080459a2</p> <p>TrafficGenOn mode=manual initiator=FC0 target=FC3</p> <p>Note: The traffic generation between the ports does not interfere with the customer data traffic. Also, after running for two consecutive hours, the traffic generator automatically shuts down. If another TrafficGenOn command is issued within these two hours, the timer is reset. The traffic generator is automatically switched off, when the mode of PITMAN is changed from one mode to another.</p>
TrafficGenOff	<p>TrafficGenOff</p> <p>Stops the traffic generation between the ports of the Bricks and Slammers.</p> <p>Note: This command is only available when PITMAN is operating in the Manual mode.</p>

Table 30 PITMAN commands (continued)

Command	Command and syntax
StartRecordingStats	<p>StartRecordingStats interval=<i>x</i> duration=<i>y</i></p> <p>interval Specifies the time intervals at which the statistics of the link devices on the FC network must be collected.</p> <p>duration Specifies the time duration for which the statistics of the link devices on the FC network must be collected.</p> <p>Periodically queries link devices on all FC loops for statistics at the specified time interval. At each specified time interval, the statistics delta is calculated and recorded in the MARKS database. This command is used to check the health of the FC network in a newly installed Pillar Axiom system.</p> <p>Note: This command is only available when PITMAN is operating in the Manual mode.</p> <p>Example:</p> <p>StartRecordingStats interval=30 duration=180</p> <p>Collects statistics of the link devices on the FC network at 30 second intervals for 180 seconds.</p>
StopRecordingStats	<p>StopRecordingStats</p> <p>Stops recording statistics for link devices in the FC network.</p> <p>Note: This command is only available when PITMAN is operating in the Manual mode.</p>
ClearStats	<p>ClearStats</p> <p>Causes the Bricks and Slammers to clear all statistics that were gathered before traffic generation between the ports and statistics collection on the SSF network.</p> <p>Note: This command is only available when PITMAN is operating in the Manual mode.</p>
GetStatsSessionInfo	<p>GetStatsSessionInfo</p> <p>Displays information on the statistics session by summarizing the status of traffic generation and statistics recording undertaken by PITMAN.</p>
CtrlSlmDev	<p>CtrlSlmDev wwn=<i>node name</i> connlabel=<i>label name</i> op={enable disable}</p>

Table 30 PITMAN commands (continued)

Command	Command and syntax
	<p>wwn=<i>node name</i> The World Wide Name (WWN) of the desired Slammer CU.</p> <p>connlabel=<i>label name</i> Connector label name on the field replaceable unit (FRU) located below each port.</p> <p>Example: connlabel=FC0.</p> <p>For Pillar Axiom 300 systems, the values of connlabel can be FC0 to FC6.</p> <p>For Pillar Axiom systems with version 1 PIMs, the values of connlabel can be FC0 to FC3 and FS0 to FS9.</p> <p>For Pillar Axiom systems with version 2 PIMs, the values of connlabel can be FC0 to FC3 and FS0 to FS11.</p> <p>op=enable Enables the specified link device or FRU in the FC network.</p> <p>op=disable Disables the specified link device or FRU in the FC network.</p> <p>Note: This command is only available when PITMAN is operating in the Manual mode.</p> <p>Example:</p> <pre>CtrlSlmDev wwn=0x2008000b08041b12 connlabel=FC0 op=enable</pre>
ResetSlmSwitch	<p>ResetSlmSwitch wwn=<i>node name</i> unit=<i>switch subcomponent</i></p> <p><i>nodename</i> The World Wide Name (WWN) of the desired Slammer CU.</p> <p><i>switch subcomponent</i> Valid values:</p> <ul style="list-style-type: none"> ○ fc: Refers to the Fiber Channel (FC)switch chip that resides in the private interconnect module (PIM) ○ mgmt: Refers to the Fiber Channel (FC) Management Controller chip that resides in the private interconnect module (PIM)

Table 30 PITMAN commands (continued)

Command	Command and syntax
	<ul style="list-style-type: none">○ pim: Refers to the Ethernet switch chip that resides in the private interconnect module (PIM) <p>Resets the specified Slammer switch.</p> <p>Note: This command is only available when PITMAN is operating in the Manual mode.</p>

Related concepts

- [About PITMAN Diagnostic Tool](#)

Related tasks

- [Run PITMAN Diagnostics](#)

Update Software, Details Tab

Navigation: Software Modules > Actions > Update Software > Details

Allows you to review the scheduled software and firmware updates on the Pillar Axiom system.

The update process affects all software modules and firmware on the Pillar Axiom system. To control the affects of the update on individual modules, login as support administrator.

Important! When logged into the system as a support administrator you can select individual components to upgrade or downgrade from the software module package. Such action is not recommended and may affect system performance. Contact the Oracle Pillar Customer Support before installing individual software components.

Install Action (*Support roles only*)

Identifies the action to perform on the selected module during the software update. The support administrator role allows you to select individual software packages to install.

Note: When you selectively update the software modules, the Pillar Axiom system cannot determine the current software module version and will display *unsupported* as the installed software version.

The choices include:

Do not install	Select this option to keep the existing module version.
Install if newer version	Select this option to upgrade the existing module only if the update is a later version.
Force Install	Select this option to force the update to the module.

Note: The Force Install option may cause an upgrade or downgrade to the currently installed module version.

Module

Identifies the name of a software or firmware module that is installed on the Pillar Axiom system.

Installed Version

Identifies the version number of a software module. A value of *unsupported* indicates that an individual software module was upgraded or downgraded.

Staged Version

Identifies the version number of the staged software module.

Software Update Options

The following options provide additional control of the software module update. These options apply to all software modules that are ready for update.

Ignore compatibility (not recommended)	During the update process, the Pillar Axiom system verifies that the version of the staged module is compatible with existing hardware and software. Select this option to omit the compatibility check.
Shutdown Slammer	Select this option to force the software update to shutdown all Slammer software components regardless of any failures that may be encountered during the shutdown process.
Ignore hardware status (except for Pilot)	Select this option to force the software update regardless of any critical or warning issues that may exist on the Slammer or Brick hardware.
Ignore current requests	Select this option to proceed with the software upgrade regardless of pending system requests.
Override failed software update	Select this option to overwrite an existing, failed software update.

Related references

- [Update Software, Schedule Tab](#)
- [Upgrade Paths from Installed Package Dialog](#)
- [Upgrade Paths to Staged Package Dialog](#)
- [Pillar Axiom System Limits](#)

Related tasks

- [Update the Pillar Axiom Software](#)
- [Display Software Versions](#)
- [Schedule the Software Update](#)

Update Software, Schedule Tab

Navigation: Software Modules > Actions > Update Software > Schedule

Allows you to schedule software and firmware updates on the Pillar Axiom system.

Schedule software update to occur at a later time

Identifies whether the schedule **Software Update Option** is enabled.

Schedule Software Update

Note: This option is enabled when **Schedule software update to occur at a later time** is enabled.

Identifies the time at which the Pillar Axiom system starts a scheduled operation.

Note: The pop-up calendar that is used to set the software update schedule is limited to the next 72-hours. You will notice that not all of the drop-down lists and other features of this calendar are functional. This behavior is normal.

Related references

- [Update Software, Details Tab](#)
- [Upgrade Paths from Installed Package Dialog](#)
- [Upgrade Paths to Staged Package Dialog](#)
- [Pillar Axiom System Limits](#)

Related tasks

- [Update the Pillar Axiom Software](#)
- [Display Software Versions](#)
- [Schedule the Software Update](#)

Upgrade Paths from Installed Package Dialog

Navigation: Software Modules > Actions > View Upgrade Paths from Installed Package

Allows you to review the staged software packages to which you can upgrade. The information indicates if the upgrades will cause Pilot or data disruption. If the list shows more than one upgrade version, install the earliest software version first, followed by the subsequent versions.

Package Version

Indicates the version of the staged package to which you are upgrading.

Pilot Disruption Required

Indicates if the upgrade will disrupt activities on the Pilot.

Data Disruption Required

Indicates if the upgrade will disrupt data path. The field will display one of:

- Yes: Indicates that the upgrade will interrupt data transmission and possible data loss may occur.
- No: Indicates that the software upgrade will not disrupt data transmission.

Pilot Software and OS

Indicates the supported software package to which you can upgrade.

Slammer Software and PROM

Indicates the supported software package to which you can upgrade.

Brick Firmware

Indicates the supported software package to which you can upgrade.

Drive Firmware

Indicates the supported software package to which you can upgrade.

Related references

- [Software Modules Page](#)
- [Update Software, Details Tab](#)
- [Upgrade Paths to Staged Package Dialog](#)

Related tasks

- [Confirm the Upgrade Paths](#)
- [Upload the Software Package](#)
- [Update the Pillar Axiom Software](#)

Upgrade Paths to Staged Package Dialog

Navigation: Software Modules > Actions > View Upgrade Paths to Staged Package

Allows you to review the software packages from which you can upgrade. The information indicates if the upgrades will cause Pilot or data disruption. If the list shows more than one upgrade version, install the earliest software version first, followed by the subsequent versions.

Package Version

Indicates the version of the staged package from which are you are upgrading.

Pilot Disruption Required

Indicates if the upgrade will disrupt activities on the Pilot.

Data Disruption Required

Indicates if the upgrade will disrupt data path. The field will display one of:

- Yes: Indicates that the upgrade will interrupt data transmission and possible data loss may occur.
- No: Indicates that the software upgrade will not disrupt data transmission.

Pilot Software and OS

Indicates the supported software package to which you can upgrade.

Slammer Software and PROM

Indicates the supported software package to which you can upgrade.

Brick Firmware

Indicates the supported software package to which you can upgrade.

Drive Firmware

Indicates the supported software package to which you can upgrade.

Related references

- [Software Modules Page](#)
- [Update Software, Details Tab](#)

Related tasks

- [Confirm the Upgrade Paths](#)
- [Upload the Software Package](#)
- [Update the Pillar Axiom Software](#)

Utilities Overview Page

Navigation: Utilities

Use the Utilities Overview page to download the following Pillar Axiom 600 utilities:

- Pillar Axiom CLI
- Pillar Axiom Statistics Tools (Statistics Tools)
- Pillar Axiom Virtual Disk Service Provider (VDS Provider)
- Pillar Axiom Volume Shadow Copy Service Provider (VSS Provider)

Pillar Axiom CLI

The Pillar Axiom Command Line Interface (CLI) is a client-based application that enables you to perform administrative actions by means of commands from a shell session.

The Pillar Axiom CLI supports automation through customer scripting using standard shells, Perl, Python, and so forth.

Download the Pillar Axiom CLI program for your operating system:

- RHEL/CENTOS/OEL 5 x86
- RHEL/CENTOS/OEL 4 x86
- SLES 11 x86
- Citrix 5.6 XenServer x86
- Solaris 9 SPARC
- Solaris 10 SPARC
- Solaris 10 x86
- Mac OS/X x86
- Windows 32-bit
- Windows 64-bit

Statistics Tools

The Pillar Axiom Statistics Tools allows you to collect Pillar Axiom system statistics and to parse the information into comma-separated values (CSV) files for use in report generators.

Download the statistics tool for your operating system:

- Linux
- Windows

Pillar Axiom VDS Provider

Download the VDS provider plug-in to manage Pillar Axiom storage devices.

Pillar Axiom VSS Provider

Download the VSS provider plug-in to manage VSS-enabled backup applications.

Related references

- [*Virtual Disk Service \(VDS\) Page*](#)
- [*Volume Shadow Copy Service \(VSS\) Page*](#)

Related tasks

- [*Download and Install the Pillar Axiom VDS Provider*](#)
- [*Download and Install the VSS Provider Plug-In*](#)

Virtual Disk Service (VDS) Page

Use the Virtual Disk Service (VDS) page to download the Pillar Axiom VDS Provider plug-in to your administrative workstation.

The VDS API provides you with a method to manage storage devices and allows you to:

- Create, delete, and extend LUNs
- Mask and unmask LUNs
- Obtain status of storage devices (Slammers, Bricks, disk drives, and LUNs)

VDS runs on the Windows 2003 platform.

- See the Microsoft *Virtual Service Technical Reference*

Related references

- [Pillar Axiom System Limits](#)

Related tasks

- [Download and Install the Pillar Axiom VDS Provider](#)

Volume Shadow Copy Service (VSS) Page

Use the Volume Shadow Copy Service (VSS) page to download the Pillar Axiom VSS Provider plug-in to your administrative workstation.

VSS allows you to create and maintain shadow copies of volumes and files, including open files.

During backups:

- Applications continue to write data.
- Open files are included in the backup.
- Users are not locked out.

VSS runs on the Windows 2003/2008 platforms.

- See the Microsoft *Volume Shadow Copy Service Technical Reference*

Related references

- [Pillar Axiom System Limits](#)

Related tasks

- [Download and Install the VSS Provider Plug-In](#)

APPENDIX F

Pillar Axiom MaxMan

Manage the List of Axiom Systems Dialog

Navigation: Axiom > Manage Axiom List

Allows you to add and remove Pillar Axiom systems that are managed by the Pillar Axiom MaxMan system.

Axiom

Provides a drop-down list of recently added Pillar Axiom systems. You can select systems from this list or enter the name of a system you want to monitor.

Add

Adds the Pillar Axiom system to the monitored list of systems.

Host

Identifies the name of the monitored Pillar Axiom system.

Port

Identifies the port number of the monitored Pillar Axiom system.

Status

Identifies the connection status of the monitored Pillar Axiom system. Valid options:

- Connected
- Lost Connectivity

Remove

Removes the selected Pillar Axiom system from the monitored list.

Related concepts

- [About Managing Configuration Files](#)

Related tasks

- [Add Systems to the Monitored List](#)
- [Create a Configuration File](#)

Configuration Tab Reference Pages

Storage Overview Page

*Navigation: **Storage***

Allows you to display SAN storage information for the Pillar Axiom MaxMan application.

SAN

Opens the SAN Storage overview page where you can access options to view LUNs and SAN Hosts.

Related concepts

- [About Pillar Axiom MaxMan](#)

Related references

- [SAN Storage Overview Page](#)
- [SAN LUNs Overview Page](#)
- [SAN Hosts Overview Page](#)

Related tasks

- [Manage a Specific Pillar Axiom System](#)

SAN Storage Overview Page

*Navigation: **Storage > SAN***

Allows you to select options to review the storage area network (SAN) logical units (LUNs) and hosts that are configured on each of the Pillar Axiom systems connected to the Pillar Axiom MaxMan application.

LUNs

Allows your to review the SAN LUN properties associated with each system.

Hosts

Allows you to review SAN Host properties associated with each system.

Related concepts

- [About Pillar Axiom MaxMan](#)

Related references

- [SAN LUNs Overview Page](#)
- [SAN Hosts Overview Page](#)

SAN LUNs Overview Page

Navigation: Storage > SAN > LUNs

Allows you to review the LUN and Clone LUN properties for each Pillar Axiom system connected to the Pillar Axiom MaxMan application.

Axiom

Identifies the name of the Pillar Axiom system.

Name

Identifies the name that is assigned to a LUN for administrative purposes.

Status

Identifies the current status of each LUN. Valid types:

Online	Indicates that the LUN is fully accessible.
Offline	Indicates that the LUN is not accessible.
Inactive	Indicates that the LUN cannot be accessed from the data path.
Partial Offline	Indicates that the actual redundancy level may be different from the redundancy level with which the volume was configured.
Degraded	Indicates that all of the copies of a redundant volume are not available. If one copy is missing, it is not fully redundant. This can happen when a write to one copy of the array fails (which may be a 30 second time-out).
Conservative	Indicates that write-back cache has been disabled so journaling has slowed.

Host Access

Identifies the SAN host mapping status associated with the LUN. Valid types:

- Mapped
- No Mappings
- Inactive
- All

Protocol Access

Identifies the access protocol used to map the LUN to the Slammer.
Protocols include:

- FC only
- iSCSI only
- No Access
- All

Groups

Displays which volume group or storage domain to which the logical volumes belongs.

Volume Group	Lists the name of the volume group where the logical volume is located.
---------------------	---

Storage Domain	Specifies the name of the Storage Domain.
-----------------------	---

Logical Capacity (GB)

Displays the storage requirements for the logical volumes.

Allocated	Identifies the initial capacity that is assigned to the logical volume. This value is a soft limit, which means that data can be stored in a logical volume until the maximum capacity is reached.
------------------	--

Addressable	Identifies the maximum capacity to which the logical volume can grow. For a clone, this field identifies how much addressable space will be available.
--------------------	--

Logical Distribution	Identifies a graphical representation of the initial capacity that is assigned to the logical volume. This value is a soft limit, which means that data can be stored in a logical volume until the maximum capacity is reached.
-----------------------------	--

Capacity (GB) for Clone LUNs

Displays the physical storage usage for the Clone LUNs.

Logical Maximum	Identifies the amount of storage that was requested for the clone repository.
Physical Used	Identifies the current volume capacity usage of the object.
Physical Allocated	Identifies the total amount of storage capacity that is reserved on the system.
Physical Maximum	Identifies the maximum capacity to which the logical volume can grow. For clones, this field identifies how much addressable space is available.

Total Physical Capacity (GB)

Displays the total physical storage capacity for the logical volumes and Clone LUNs.

Redundancy	Identifies how many mirror copies of the original data are stored online.
Disk Protection	Indicates the RAID drive data protection method.
LUN Overhead	Identifies the physical and logical storage capacity that is required to meet the LUN Quality of Service (QoS) settings.
Allocated	Specifies the amount of raw capacity in gigabytes (GB) that has been assigned and designated to this logical volume.
Maximum	Identifies the maximum capacity for the volume group. The maximum capacity of the logical volumes and nested volume groups that are associated with the volume group cannot exceed this value. A value of 0 (zero) identifies that the volume group is configured with unlimited capacity. You can increase the maximum capacity of associated logical volumes and nested volume groups without constraints.
Physical Distribution	A graphical representation of the capacity used compared to the maximum allocated.

Priority Level

Identifies the assigned priority level when the volume was created.

- Premium
- High
- Medium
- Low
- Archive

Global LUN Number

Identifies the globally unique identifier of the LUN.

LUID

Identifies the unique identifier of the LUN.

Related concepts

- [About Pillar Axiom MaxMan](#)

Related references

- [SAN Storage Overview Page](#)

SAN Hosts Overview Page

*Navigation: **Storage > SAN > Hosts***

Allows you to review the storage area network (SAN) hosts for each Pillar Axiom system connected to the Pillar Axiom MaxMan application.

Axiom

Identifies the name of the Pillar Axiom system.

Host

Identifies the SAN host information. Valid options:

Host Name	Identifies the name of the SAN host.
Number of LUNs Mapped	Identifies the number of LUNs that are mapped to that particular SAN host either because of specific mapping or because the LUN is available to all SAN hosts.

Pillar Axiom Path Manager

Identifies certain global characteristics associated with the Pillar Axiom Path Manager (APM). Valid options:

Status	Identifies whether or not the APM driver is communicating, or if it is not registered. If the driver is not registered, install a path manager, such as the Pillar Axiom Path Manager.
Version	Identifies the version of the APM host driver, if it has been installed, that is running on the SAN host.
Host IP Address	Identifies the IP address of the SAN host. The system uses this address to exchange management requests and responses with the Pillar Axiom Path Manager (APM) that is installed on the host. If APM is not installed, this field displays <i>N/A</i> .

HBA

HBA Alias Name	Identifies the HBA alias name.
-----------------------	--------------------------------

Related concepts

- [About Pillar Axiom MaxMan](#)

Related tasks

- [Manage a Specific Pillar Axiom System](#)

Replication Engines Overview Page

Navigation: Replication Engines

Allows you to view the status of the available Replication Engines registered with each Pillar Axiom system that is managed by the Pillar Axiom MaxMan application.

Axiom

Identifies the name of the Pillar Axiom system.

Agent Status

Identifies the communication status of the Pillar Axiom 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 version of Pillar Axiom MaxRep software running on the Replication Engine.

Related concepts

- [About Pillar Axiom MaxMan](#)

Related tasks

- [Manage a Specific Pillar Axiom System](#)

Software Modules Page

*Navigation: **Software Modules***

Allows you to review the installed software and firmware versions for each Pillar Axiom system connected to the Pillar Axiom MaxMan application.

Axiom

Identifies the name of the Pillar Axiom system.

Module

Identifies the name of a software or firmware module that is installed on the Pillar Axiom system.

Table 31 Software module types

Name	Description
Pilot OS	Operating system for the Pilot.
Pilot Software	Software that runs on the Pilot, such as the GUI interface and web server, online help, Simple Network Management Protocol (SNMP), and Network Data Management Protocol (NDMP).
Slammer PROM, AX600	Programmable ROM (PROM), which includes BIOS and netboot code, for storage area network (SAN) Slammers. Pillar Axiom 600 systems display the <i>AX600</i> suffix.
Slammer Software, AX600	SAN software that runs on Slammers. Pillar Axiom 600 systems display the <i>AX600</i> suffix.
Brick SATA2 Firmware	RAID firmware for serial ATA (SATA) Bricks. Pillar Axiom systems that contain version 2 SATA controllers display the <i>SATA2 Firmware</i> suffix. Note: Version 2 SATA RAID controllers have 16 ports to support the Storage System Fabric (SSF). Version 1 SATA controllers have 13 such ports.
Brick FC Firmware	RAID firmware for Fibre Channel (FC) Bricks.
Brick Disk Drive Firmware	Drive firmware for Bricks.

Version

Identifies the version number of a software module. A value of *unsupported* indicates that an individual software module was upgraded or downgraded.

Related concepts

- [About Pillar Axiom MaxMan](#)
- [About Updating the Pillar Axiom Software](#)

Related tasks

- [Manage a Specific Pillar Axiom System](#)

Administrator Accounts Overview Page

Navigation: Administrator Accounts

Allows you to review the administrator accounts available on each Pillar Axiom system connected to the Pillar Axiom MaxMan

Axiom

Identifies the name of the Pillar Axiom system.

Login Name

Lists administrator login, or user names. Click a name to review or modify the administrator account.

Role

Identifies the role that is assigned to the administrator account. A role defines which permissions are granted to the administrator.

- Primary Administrator
- Administrator 1
- Administrator 2
- Monitor
- Support
- Pillar support

Disabled

Identifies whether the administrator account is disabled.

No	Indicates that the account is active. Administrators whose accounts are enabled can log in to the Pillar Axiom system.
Yes	Indicates that the account is inactive. Administrators whose accounts are disabled cannot log in.

Full Name

Identifies the first and last name associated with the administrator account.

Email Address

Identifies the email address of the recipient. The email server to which the Pillar Axiom system sends alerts must be able to receive messages at this address. The system does not validate this address.

Phone Number

Identifies the phone number associated with the administrator account. The Pillar Axiom system does not verify the validity of this entry.

Related concepts

- [*About Pillar Axiom MaxMan*](#)
- [*About Creating Administrator Accounts*](#)

Related tasks

- [*Manage a Specific Pillar Axiom System*](#)

Health Tab Reference Pages

Alerts and Events Overview Page

Navigation: Alerts and Events

Allows you to select options to display system alerts and event notifications for all of the Pillar Axiom systems connected to the Pillar Axiom MaxMan.

System Alerts

Allows you to review Pillar Axiom system alerts.

Recent System Events

Allows you to review Pillar Axiom event logs.

Event Notification

Allows you to review the Pillar Axiom event notifications.

Related concepts

- [About Pillar Axiom MaxMan](#)

Related references

- [System Alerts Overview Page](#)
- [Recent Events Overview Page](#)
- [Event Notification Overview Page](#)

Related tasks

- [Manage a Specific Pillar Axiom System](#)

Axioms Overview Page

Navigation: Hardware > Axioms

Allows you to review the status and system information of each Pillar Axiom system connected to the Pillar Axiom MaxMan application.

Axiom

Identifies the name of the Pillar Axiom system.

Overall Status

Identifies the status of the Pillar Axiom system. Valid status:

- Normal

- Warning
- Critical
- Booting
- Upgrading
- Shutdown

Pilot Status

Identifies the current status of a control unit (CU) within the Pilot. A status of Normal requires no action.

Slammer Status

Identifies the current status of the CU of the Slammer.

Brick Status

Identifies the current status of the Bricks.

System Summary

Model

Displays the model number of Pillar Axiom system.

Slammer Types

Displays the type of Slammers installed the system.

Brick Types

Displays the type of Bricks installed the system.

Number of Slammers

Displays the number of Slammers installed the system.

Number of Bricks

Displays the number of Bricks installed the system.

Location

Displays the system location as defined by the system administrator.

Pilot Management Interface

IP Address

Identifies the public IP address that is assigned to the Pilot. This IP address is what the administrator uses to access the Pillar Axiom Storage Services manager over the management interface.

Netmask

Identifies the subnet mask for the public IP address that is permanently assigned to the Pilot.

Gateway

Identifies the IP address of the gateway server in the subnet of which the Pillar Axiom system (the Pilot) is a member.

Pilot CU 0/1 Interface

IP Address

Identifies the IP addresses that are permanently assigned to the ports on the CUs in the Pilot.

Netmask

Identifies the subnet mask for the public IP address that is permanently assigned to the Pillar Axiom system.

Gateway

Identifies the public IP address of the gateway server in the subnet of which the Pillar Axiom system is a member.

DHCP

Identifies whether Dynamic Host Configuration Protocol (DHCP) is enabled.

Email Notification

Identifies whether email is enabled to notify recipients of system events.

Call-Home

Indicates whether event-triggered Call-Home is enabled.

Asset Number

Displays the system asset number as defined by the system administrator.

Serial Number

Identifies the system serial number (SSN) that is assigned to the Pillar Axiom system.

Related concepts

- [About Pillar Axiom MaxMan](#)
- [About Managing Configuration Files](#)

Related tasks

- [Manage a Specific Pillar Axiom System](#)
- [Manage a Specific Pillar Axiom System](#)

Bricks Overview Page

Navigation: Hardware > Bricks

Allows you to review the Bricks status for each Pillar Axiom system connected to the Pillar Axiom MaxMan.

Axiom

Identifies the name of the Pillar Axiom system.

Brick Name

Lists the names of the Bricks. Click a name to display details about that hardware component.

Note: When you move the mouse cursor over a name, the fully qualified name (FQN) for that Brick is displayed.

Enclosure Type

Lists the type of RAID controller installed in the Brick chassis. Valid types:

- Unknown
- SATA
- SATA V2
- FC
- FC V2

Media Type

Lists the type of drives installed within the Brick enclosure. Valid types:

- SATA
- FC
- SSD SLC (solid state drive, single-level cell)

Brick Status

Displays the current status of the hardware components. A status of Normal requires no action. Valid options:

Overall	Displays the summary status of the Brick.
Temperature	Displays the status of the Brick temperature.

Chassis	Displays the status of the Brick chassis.
ES Module	Displays the status of the enclosure services (ES) module, which monitors the fan speed, power supply temperature, drive status, and RAID controller status.
RAID Controller	Displays the status of the RAID controller within the Brick.
Power Supply and Fans	Displays the status of the power supplies and fans within the Brick.
Disks	Displays the status of the drives within the Brick.
Spare Disk	Displays the status of the spare drive within the Brick.

Details

Displays the current capacity of the Brick and the name of the Storage Domain within which the Brick resides. Valid options:

Total Capacity	Displays the total raw capacity for the Brick. This value does not include the capacity of the spare drive.
Storage Domain	Displays the name of the Storage Domain associated with the Brick.

Related concepts

- [About Pillar Axiom MaxMan](#)

Related references

- [Axioms Overview Page](#)

Related tasks

- [Manage a Specific Pillar Axiom System](#)

Event Notification Overview Page

Navigation: Alerts and Events > Event Notification

Allows you to review the list of event notifications created for each Pillar Axiom 600 system connected to the Pillar Axiom MaxMan application.

Axiom

Identifies the name of the Pillar Axiom system.

Name

Lists the name of event notification. Click a name to review, modify, or delete the notification settings.

Enabled

Indicates whether the event notification is enabled. Valid options:

Yes The event notification is actively collecting event information.

No The event notification is inactive and not collecting event information.

Time Last Sent

Identifies the time at which the event was sent to the designated recipients.

Number of Events

Indicates the number of events collected by the notification.

Number of Recipients

Indicates the number of email recipients subscribed to the event notification.

Description

Displays the description of the event notification.

Related concepts

- [About Pillar Axiom MaxMan](#)

Related references

- [Alerts and Events Overview Page](#)

Related tasks

- [Manage a Specific Pillar Axiom System](#)

Generated Reports Overview Page

Navigation: *Generated Reports*

Allows you to review generated reports for each Pillar Axiom 600 system connected to the Pillar Axiom MaxMan application.

Axiom

Identifies the name of the Pillar Axiom system.

Name

Displays the name of the generated report.

Created

Displays the date and time that the report was created.

Size

Indicates the size of the raw report file in kilobytes (KB) or megabytes (MB).

Note: The size of the downloaded report will vary depending on the chosen format.

Related concepts

- [About Pillar Axiom MaxMan](#)

Related references

- [Axioms Overview Page](#)

Related tasks

- [Manage a Specific Pillar Axiom System](#)

Hardware Overview Page

Navigation: Hardware

Allows you to select options to display hardware components for all of the Pillar Axiom 600 systems connected to the Pillar Axiom MaxMan application.

Axioms

Allows you to review the status and properties of the Pillar Axiom 600 system.

Pilots

Allows you to review the status and properties of the Pilot control units (CUs).

Slammers

Allows you to review the status and properties of the Slammer CUs.

Bricks

Allows you to review the status and properties of the Brick CUs.

UPS

Allows you to review the status and properties of the Uninterruptible Power Supply (UPS) devices.

Related concepts

- [About Pillar Axiom MaxMan](#)

Related references

- [Axioms Overview Page](#)
- [Pilot Overview Page](#)
- [Slammers Overview Page](#)
- [Bricks Overview Page](#)
- [Uninterruptible Power Supplies Overview Page](#)

Related tasks

- [Manage a Specific Pillar Axiom System](#)

Pilot Overview Page

Navigation: Hardware > Pilots

Allows you to review the status of the Pilot management controller for each Pillar Axiom system connected to the Pillar Axiom MaxMan application.

Axiom

Identifies the name of the Pillar Axiom system.

Control Unit

Identifies the control unit (CU) of the Pilot.

Status

Displays the current status of a CU within the Pilot. A status of Normal requires no action.

Mode

Displays the current operational mode of the two CUs within the Pilot. Valid options:

Active Indicates which CU performs all configuration tasks that administrators request.

Standby Indicates which CU acts as a secondary device and does nothing unless the active CU fails over to this standby control unit.

OS Version

Identifies the operating system version of the Pilot.

Server Version

Identifies the software version installed on the Pillar Axiom system.

Serial Number

Identifies the serial number that is assigned to the hardware component.

Related concepts

- [About Pillar Axiom MaxMan](#)

Related references

- [Axioms Overview Page](#)

Related tasks

- [Manage a Specific Pillar Axiom System](#)

Recent Events Overview Page

Navigation: Alerts and Events > Recent Events

Allows you to review the event logs for each Pillar Axiom system connected to the Pillar Axiom MaxMan.

Axiom

Identifies the name of the Pillar Axiom system.

Event

Displays the name of the event in the Pillar Axiom event log.

Severity

Displays the severity level of entries in the Pillar Axiom event log. Valid options:

Informational	Requires no action for events that are information only.
Warning	Requires no immediate action for minor conditions that you can address at your convenience.
Critical	Requires prompt action to prevent system failures or offline conditions.

Category

Identifies the type of event. Valid values:

Security	Events to notify of a security problem such as unauthorized request.
Audit	Events that keep track of what users are doing, such as the operations that they performed.
System	Events to notify of system problems, such as a missing Brick or Slammer.

Time Occurred

Identifies the time at which the event was sent to the designated recipients.

Affected Item

Provides the specific object name affected by the Event Type. For example, if the **Event** reads Brick Firmware Invalid, then the Affected Item column lists the Brick name that caused the event to occur. Such details provide additional information for troubleshooting purposes.

User

The name of the user logged in at the time the event occurred.

Description

Displays the event description text.

Events per Page

Indicates the number of events to display on each page. The default is 50 events.

Note: If (filtered) displays at the top of the page, it indicates that the list contains excluded items.

Refresh

Allows you to update the contents of the page.

Related concepts

- [About Pillar Axiom MaxMan](#)

Related references

- [Alerts and Events Overview Page](#)

Related tasks

- [Manage a Specific Pillar Axiom System](#)

LUN Statistics and Trending Overview Page

Navigation: *Statistics > SAN > LUNs*

Allows you to review performance statistics for LUNs, view trending charts for LUNs, and export trending chart data for each Pillar Axiom system connected to the Pillar Axiom MaxMan.

Axiom

Identifies the name of the Pillar Axiom system.

Name

Identifies the name that is assigned to a LUN for administrative purposes.

Physical Allotted Capacity

Identifies the maximum capacity limit, in gigabytes (GB), that is assigned to the object.

Priority Level

Identifies the priority level assigned to the specified LUN.

Valid levels:

- Archive
- Low
- Medium
- High
- Premium

Average IOPs

Identifies the current performance for input (read) and output (write) operations for the LUN.

Average Throughput

Identifies the data transfer rate for inputs (reads) and outputs (writes) of the specified LUN.

Average I/O Latency

Identifies the average time to complete the read or write operations.

Average I/O Size

Identifies the average size of the read and write operations.

Collection Period

Identifies the start and end time at which information was last collected from the Pillar Axiom system.

Related concepts

- [About Pillar Axiom MaxMan](#)

Related references

- [Axioms Overview Page](#)

Related tasks

- [Manage a Specific Pillar Axiom System](#)

SAN Slammer Protocol Statistics and Trending Overview Page

Navigation: *Statistics > SAN > Slammer Protocols*

Allows you to review statistics for storage area network (SAN) protocols and create trending charts from SAN protocol statistics for each Pillar Axiom system connected to the Pillar Axiom MaxMan.

Axiom

Identifies the name of the Pillar Axiom system.

Slammer

Identifies the name of the Slammer that contains TCP/IP statistics.

Control Unit

Identifies the control unit (CU) of the Slammer that contains the statistics.

Network Interface

Identifies the physical port on the CU.

Port Type

Identifies the Slammer port connection type, Fibre Channel (FC) or Internet Small Computer System Interface (iSCSI).

Negotiated Link Speed

Displays the transmission speed in gigabits/second for the port.

Average Throughput (per Second)

Displays the average throughput in MB/second.

- **Read:** The average read throughput in MB/second.
- **Write:** The average write throughput in MB/second.

Average I/O Latency

Identifies the average time to complete the read or write operations.

Average I/O Size

Identifies the average size of the read and write operations.

Commands Received (per Second)

Displays the number of read and write commands received each second over the last sampling period.

Channel Errors Since Activated

Displays the cumulative number of errors that have occurred on the channel since the Slammer control unit was started.

Collection Period

Identifies the start and end times at which information was last collected from the Pillar Axiom system.

Related concepts

- [About Pillar Axiom MaxMan](#)

Related references

- [Axioms Overview Page](#)

Related tasks

- [Manage a Specific Pillar Axiom System](#)

SAN Statistics and Trending Overview Page

Navigation: *Statistics > SAN*

Allows you to select the type of SAN statistics to display for the Pillar Axiom MaxMan

LUNs

Opens the LUN Statistics and Trending Overview page, where you can view LUN statistics, create trending charts, and export trending chart data.

Slammer Protocols

Opens the SAN Slammer Protocol Statistics and Trending Overview page, where you can view SAN protocol statistics, create trending charts, and export trending chart data.

Related concepts

- [About Pillar Axiom MaxMan](#)

Related references

- [Axioms Overview Page](#)
- [Statistics and Trending Overview Page](#)

Related tasks

- [Manage a Specific Pillar Axiom System](#)

Scheduled Jobs Overview Page

Navigation: Scheduled Tasks

Allows you to review a list of scheduled jobs for each Pillar Axiom system connected to the Pillar Axiom MaxMan application.

Axiom

Identifies the name of the Pillar Axiom system.

Name

Identifies the name of a scheduled operation.

Start Time

The date and time the task is scheduled to start.

Type

Identifies the type of data protection used in the schedule.

Enable

Identifies whether the scheduled replication is enabled.

Enabled	Indicates that the scheduled event performs at the specified time.
----------------	--

Disabled	Indicates that the operation will not perform as scheduled.
-----------------	---

Enabled

Specifies whether the scheduled task is enabled.

Related concepts

- [About Pillar Axiom MaxMan](#)

Related references

- [Axioms Overview Page](#)

Related tasks

- [Manage a Specific Pillar Axiom System](#)

Slammers Overview Page

Navigation: Hardware > Slammers

Allows you to review the status of the Slammers for each Pillar Axiom system connected to the Pillar Axiom MaxMan application.

Axiom

Identifies the name of the Pillar Axiom system.

Slammer Name

Lists the names of hardware components. Click a name to display details about that hardware component.

Type

Lists the type of Slammer.

Control Unit

Identifies a control unit (CU) of the Slammer.

CU Status

Displays the current status of the CU. A status of Normal requires no action.

Temperature

Displays the temperature status of the Slammer.

Chassis

Displays the current status of the Slammer Chassis.

Motherboard Assembly

Displays the current status of the Slammer Motherboard Assembly.

Power Supplies

Displays the current status of the Slammer power supplies.

Fans

Displays the current status of the Slammer fans.

Batteries

Displays the current status of the Slammer batteries.

Private Interconnect Module

Displays the current status of the Slammer Private Interconnect Module (PIM).

Network Interface Module

Displays the current status of the Slammer Network Interface Module (NIM).

Related concepts

- [About Pillar Axiom MaxMan](#)

Related references

- [Axioms Overview Page](#)

Related tasks

- [Manage a Specific Pillar Axiom System](#)

Statistics and Trending Overview Page

Navigation: *Statistics and Trending*

Allows you to select performance statistics and trending pages for each Pillar Axiom system connected to the Pillar Axiom MaxMan application.

SAN

Opens the SAN Statistics page, where you can choose LUN Statistics and Trending or Slammer Protocols Statistics and Trending.

Related concepts

- [About Pillar Axiom MaxMan](#)

Related references

- [Axioms Overview Page](#)

Related tasks

- [Manage a Specific Pillar Axiom System](#)

System Alerts Overview Page

Navigation: *Alerts and Events > System Alerts*

Allows you to review the system alerts for each Pillar Axiom system connected to the Pillar Axiom MaxMan application.

Axiom

Identifies the name of the Pillar Axiom system.

Alert

Identifies item that caused the system alert.

Time Occurred

Indicates the date and time the system alert occurred.

Affected Items

Identifies the name of the system object that caused the system alert.

Description

Provides a brief description of the system alert.

Related concepts

- [About Pillar Axiom MaxMan](#)
- [About Pillar Axiom MaxMan](#)

Related tasks

- [Manage a Specific Pillar Axiom System](#)

Uninterruptible Power Supplies Overview Page

*Navigation: **Hardware** > **UPS***

Allows you to review the current status of the uninterruptible power supply (UPS) that is installed on the Pillar Axiom system, which is connected to the Pillar Axiom MaxMan application.

Axiom

Identifies the name of the Pillar Axiom system.

Name

Identifies the name assigned to the external UPS device.

IP Address

Identifies the IP address that is assigned to the external UPS device.

Model

Identifies the model number of the UPS device.

Power Source

Identifies the source of the UPS power. Valid sources:

- AC (alternating current)
- Battery
- Unknown

Battery Status

Identifies the current status of the UPS batteries. Valid values:

- Normal
- Warning
- Critical
- Unknown

Related concepts

- [*About Pillar Axiom MaxMan*](#)
- [*About Pillar Axiom MaxMan*](#)

Related tasks

- [*Manage a Specific Pillar Axiom System*](#)

Index

A

accept

- a Brick 186

- a drive 182

Accept Brick Dialog

- field definitions 437

access bias

- description 95

- effect on performance 97

accessing the Pillar Axiom system

- description 30

Account Security controls 386, 403

add

- a Brick 186

- administrator accounts (Axiom system) 60

- Pillar Axiom systems (Pillar Axiom MaxMan) 272

Add RAID Controller to Clear History Log Files

- dialog 551

additional resources 19

administrator account

- how to

- create (Axiom system) 60

Administrator Account

- Create 304

administrator accounts

- about account creation 59

- about account modification 62

- how to

- change passwords 62, 63

- delete 64

- display 61

- modify 62

- limits

- full names 278

- login attempts 276

- number of accounts 276

- number of sessions 276

- passwords 278

- user names 278

- security description 51

Administrator Accounts overview

- field definitions 280

Administrator Accounts overview (Pillar Axiom MaxMan)

- field definitions 591

alerts

- how to

- delete 204

- display 204

- limits

- descriptions 278

- name length 277

Alerts and Events (Pillar Axiom MaxMan)

- field definitions 593

application packages

- download formats 26

archive files

- how to

- extract 28

ASM performance profile

- description 106

asset information, system

- how to

- modify 40

Associate Hosts

- field definitions 282

associated hosts

- definition 135

- how to

- create host-to-HBA association 140

automatic screen updates

- how to

- disable 35

Axiom Performance controls 512

B

Backup Storage Profile settings 101

battery-backed memory (BBM) 205

binding drive to Bricks 182

branding, drive 181

Brick console

- description 227

- how to

- run Brick commands 229

- view RAID output 228
- Brick hardware components
 - drive insertion 181
 - foreign drives 181
- Brick storage enclosure
 - how to
 - accept a drive 182
- Brick storage enclosures
 - effects on Storage Domains 77
 - error recovery 227
 - foreign 187
 - how to
 - accept 186
 - reassign to another Storage Domain 188
 - remove 189
 - run Brick commands 229
 - view RAID output 228
 - limits
 - name length 277
 - overhead 90
 - prerequisites for removal 189
 - RAID commands 227
 - reassigning to a different Storage Domain 188
 - stripes 106
 - unassigned Storage Domain status 75
 - virtual capacity 91
- Bricks Overview
 - field definitions 438
- Bricks Overview (Pillar Axiom MaxMan)
 - field definitions 596

C

- cache, write, LUN 205
- Call-Home 45
- Call-Home Configuration controls 372
- Call-Home feature
 - description 44
 - how to
 - configure 46
 - modify 47
 - send system logs 218
 - test 46
 - upload a new matrix 48
 - logs (MIB object) 53
 - transmission methods 44
- Call-Home Triggering controls 370
- capacity
 - description 85
 - overhead 90
 - parity in reported capacities 91
 - reclaimed 91
 - reserved for in-filling 90
- capacity usage
 - as an MIB object 54
 - consumption by replica type 149
 - depends on Brick type 91
 - free capacity, insufficient to create a volume 87
 - how to
 - display 65
 - categories, event 194
 - change
 - administrator passwords 62, 63
 - Channel Errors, FC controls 517
 - CHAP secrets
 - about configuring 48
 - limits
 - data type and length 279
 - chart threshold
 - how to
 - create 262
 - Chart Thresholds controls
 - field definitions 441, 443
 - Citrix XenServer Storage Profiles 104
 - clearing pinned data 204
 - ClearStats PITMAN command 570
 - client application packages
 - download formats 26
 - client logs, UI
 - how to
 - view 215
 - client software
 - how to
 - download 26
 - install 27
 - client software packages
 - description 24
 - Clone LUN Capacity 291
 - Clone LUN replicas
 - capacity usage 149
 - homing 149
 - how to
 - create 153
 - delete 154, 155
 - increase allocated capacity 125
 - modify protection schedule 159
 - restore LUNs 156
 - limits
 - number of 276
 - monitor capacity usage 54
 - clone LUNs
 - how to
 - display 155
 - Clone LUNs Capacity 317, 383, 430
 - Clone SAN LUN
 - Data Protection
 - field definitions 291
 - Clone Schedules 291, 302, 318, 384, 431

- collect
 - log bundles 215
 - statistics 216
- community strings
 - limits
 - data type and length 279
- compressed files
 - download formats 26
- configuration files
 - how to
 - reset a Pillar Axiom system 239
 - quantity range 275
- configuration files (Pillar Axiom MaxMan)
 - contents 272
 - extension, psdmac 272
 - how to
 - add Pillar Axiom systems 272
 - create 272
 - modify 274
 - open 273
 - opening 272
- Configuration Trending Chart
 - Data Filtering Tab 445
 - field definitions 445
- configure
 - account security settings 52
 - Call-Home settings 46
 - email settings 44
 - interfaces
 - management 42
 - iSCSI system settings 49
 - system time 39
- Configure Trending Chart Dialog
 - Chart Threshold Tab 262
- Configure Trending Chart, Trend Configuration Tab (LUNs)
 - field definitions 447
- Configure Trending Chart, Trend Configuration Tab (Slammers)
 - field definitions 448
- connectivity
 - about network interfaces 41
 - Slammer test description 220
- Connectivity and Communication controls 366
- connectivity, Slammer
 - command reference 223
 - how to
 - test 224
- contact information 20
- contacts, Oracle 20
- conventions
 - typographical 20
- copy
 - LUNs 132

- Copy SAN LUN 298
 - Data Protection
 - field definitions 301
- create
 - a Storage Profile 108
 - administrator accounts (Axiom system) 60
 - Clone LUN schedules 122
 - data protection schedules 158
 - event notifications 199
 - immediate Clone LUNs 153
 - log bundles 215
 - logical volume, when insufficient space exists 87
 - LUNs
 - define data protection 121
 - define mapping by host 117
 - define mapping by LUN number 119
 - define Quality of Service 115
 - SNMP hosts 55
 - Storage Domains 78
 - volume groups 67, 69
- Create Administrator Account
 - field definitions 304
- Create Chart Thresholds controls
 - field definitions 450, 452
- Create Job Schedule
 - field definitions 306
- Create Log Bundle
 - field definitions 552
- Create Reporting Schedules dialog 456
 - field definitions 456
- Create SAN LUN 288, 314
 - Data Protection
 - field definitions 317
 - membership
 - field definitions 348
- Create SNMP Host
 - field definitions 320, 433
- Create Uninterruptible Power Supplies overview
 - field definitions 533
- critical severity level (system event) 505
- CtrlSImDev PITMAN command 570
- Current status controls 534, 536
- customer support 20

D

- data consistency
 - about 212
 - how to
 - verify 213
- Data Consistency overview
 - field definitions 554
- data migration
 - effects created by Storage Domain creation 78

- data paths
 - how to
 - disable for a LUN *133*
 - enable for a LUN *133*
- data protection
 - how to
 - create Clone LUN schedules *122, 158*
 - delete schedules *160*
 - display schedule details *161*
 - display schedules *152*
 - modify a Clone LUN schedule *159*
 - jobs
 - description *206*
 - schedule description *158*
- Data Protection Schedule
 - View *544*
- data replica capacities *149*
- data type and length ranges *277*
- debugging
 - how to
 - collect log bundles *215*
 - delete log bundles *218*
 - isolate PI errors *226*
 - test connectivity issues *224*
- default log in values *30*
- delete
 - a Storage Profile *110*
 - administrator account *64*
 - alerts *204*
 - Clone LUN replicas *154, 155*
 - data protection schedule *160*
 - event log entries *195*
 - event notifications *201*
 - job schedules *208*
 - log bundles *218*
 - LUNs *134*
 - reporting schedule *248*
 - reports *243*
 - SAN host names *140*
 - SNMP hosts *56*
 - Storage Domains *80*
 - volume groups *70*
- Delete Log Bundles
 - field definitions *555*
- diagnostics
 - description of system tools *209*
 - how to
 - clear system halt points *237*
 - continue system startup after a halt *238*
 - diagnose Slammer issues *221*
 - set halt points *237*
 - test connectivity *224*
 - view Slammer diagnostic results *222*
 - on Slammers *220*
 - PITMAN tool *225*
- Disk Drive Firmware overview
 - field definitions *556*
- display
 - account summaries *61*
 - alerts *204*
 - capacity usage *65*
 - clone LUN details *155*
 - data protection *152*
 - data protection details *161*
 - event logs *195*
 - event notification details *200*
 - event notifications *198*
 - event properties *196*
 - hardware component status
 - overview *176*
 - hardware FRU details *177*
 - LUN details *124*
 - Pillar Axiom software versions *166*
 - reporting schedules *247*
 - SAN host settings *136*
 - Slammer diagnostic results *222*
 - Storage Profiles *108*
 - system alerts *203*
- Distributed RAID geometry *98*
- DNS domains
 - limits
 - name length
- DNS Settings controls *365, 390*
- documentation *20*
 - feedback *20*
- Domain Name Server (DNS)
 - how to
 - configure IP addresses *43*
 - limits
 - name length *278*
 - purpose *41*
- download
 - Pillar Axiom firmware updates *167*
 - client software *26*
 - generated reports *242*
 - log bundles *217*
 - Pillar Axiom MIB table *58*
 - Pillar Axiom software updates *167*
 - VDS Provider *147*
 - VSS Provider *164*
- Download Report
 - field definitions *458*
- drive firmware
 - about *173*
 - how to
 - download the package *167*
 - remove the installed package *175*
 - update the staged firmware *174*

upload the package *173*

drive, disk

how to

accept *182*

drives, Brick

binding to a Brick *182*

branding *181*

E

education programs *20*

email notifications

how to

configure *44*

limits

email address *278*

Email Notifications controls *370*

error severity level (system event) *505*

Event Log overview

field definitions *459*

Event Log overview (Pillar Axiom MaxMan)

field definitions *601*

event logs

description *194*

how to

delete entries *195*

test the Call-Home feature *46*

event notifications

description *198*

how to

configure email server *44*

create *199*

delete *201*

display *198*

display details *200*

modify *201*

types of *43*

events

as MIB objects *53*

how to

display logs *195*

display properties *196*

filter log entries *196*

responding to *203*

severities *505*

Events overview page

field definitions *461*

Events overview page (Pillar Axiom MaxMan)

field definitions *597*

Events Properties dialog

field definitions *462*

Export Dialog

field definitions *464*

F

FC Port Information controls *358, 420*

FC protocol

connection status icons *112*

features, optional premium *37*

feedback, documentation *20*

field definitions

Accept Brick Dialog *437*

Account Security controls *386, 403*

Administrator Accounts overview *280*

Administrator Accounts overview (Pillar Axiom MaxMan) *591*

Alerts and Events (Pillar Axiom MaxMan) *593*

Associate Hosts *282*

Axiom Performance *512*

Bricks Overview *438*

Bricks Overview (Pillar Axiom MaxMan) *596*

Call-Home Configuration controls *372*

Call-Home Triggering controls *370*

Channel Errors, FC *517*

Chart Thresholds controls *441, 443*

Clone LUN Capacity *291, 317*

Clone LUNs Capacity *383, 430*

Clone SAN LUN

Data Protection *291*

Clone Schedules *291, 302, 318, 384, 431*

Configure Trending Chart

Data Filtering Tab *445*

Configure Trending Chart, Trend Configuration Tab (LUNs) *447*

Configure Trending Chart, Trend Configuration Tab (Slammers) *448*

Connectivity and Communication controls *366*

Copy SAN LUN

Data Protection *301*

mapping *298*

Create Administrator Account *304*

Create Chart Thresholds controls *450, 452*

Create Job Schedule *306*

Create Log Bundle *552*

Create Reporting Schedules dialog *456*

Create SAN LUN

Data Protection *317*

mapping *288, 314*

membership *348*

Create SNMP Host *320, 433*

Create UPS *533*

Current status controls *534, 536*

Data Consistency overview *554*

Delete Log Bundles *555*

DNS Settings controls *365, 390*

Download Report *458*

Drive Firmware overview *556*

Email Notifications controls *370*

Event Log overview *459*

Event Log overview (Pillar Axiom MaxMan) *601*

Events overview page 461
Events overview page (Pillar Axiom MaxMan) 597
Events Properties dialog 462
Export Dialog 464
FC Port Information controls 358, 420
General Information, FC 515
General Information, iSCSI 519
General, LUNs 513
Generate Report Dialog 465
Generated Reports overview (Pillar Axiom MaxMan) 598
Global Settings Overview 322
Groups Overview 324
Hardware overview page 467
Hardware overview page (Pillar Axiom MaxMan) 599
Host Information controls 354, 417
Host to LUN Mapping overview page 325, 327
I/O Latency, FC 516
I/O Latency, iSCSI 520
I/O Latency, LUN 513
Installed Software controls 559
Installed Software controls (Pillar Axiom MaxMan) 589
iSCSI Connectivity and Communication controls 391
iSCSI Host Specific Settings controls 356, 419
iSCSI Port Errors 521
iSCSI Port Events 522
iSCSI Port Information controls 358, 420
iSCSI Port Requests 522
iSCSI Security controls 392
iSNS Server Registration 367
iSNS Server Registration controls 49
iSNS Settings controls 392
Login Screen Message controls 386, 403
Loop Activity, FC 518
LUN Mapping 289, 299, 315, 381, 428
LUN Slammer Control Unit Assignment controls 288, 298, 314, 380, 427
LUN Statistics and Trending page 468
LUN Statistics and Trending page (Pillar Axiom MaxMan) 603
LUN Statistics Trending dialog 499
Manage SAN Host Groups
 Groups Tab 328
 Hosts Tab 329
Manage Storage Domains, Bricks Tab 330, 334
Manage Storage Domains, Storage Domains Tab 332
Manage Storage Profiles 336
Manage Storage Profiles overview page 342
Manage System Alert dialog 470
Manage the List of Axiom Systems 582
Manage Volume Groups
 Volume Groups 344
 Volumes 346
Management Interface controls 364, 390
Modify Administrator Account 350
Modify Asset Information 352
Modify Brick
 Components 471
 I/O Ports 473
Modify Event Notification 477
Modify Host
 Advanced 353
Modify iSCSI Port Settings 360
modify Job Schedule 362
Modify Reporting Schedule dialog 479
modify SAN LUN
 Data Protection 383
Modify SAN LUN
 mapping 380
Modify Scheduled Job 475
Modify Slammer
 Components 481
 I/O Ports 483
Modify SNMP Host 387
Modify System Time 389
Modify UPS 534
Notification controls 391
Path Manager Settings controls 354, 417
Performance, FC 515
Performance, iSCSI 519
Physical Capacity controls 330
 logical volumes 334
Pilot CU 0/0 Interface controls (Pillar Axiom MaxMan) 595
Pilot Management Interface controls (Pillar Axiom MaxMan) 594
Pilot overview 486
Pilot overview (Pillar Axiom MaxMan) 600
Ports Masked for this LUN controls 289, 299, 315, 381, 428
Protection Schedules overview page 539
quantity ranges for 275
Replication Engines overview 550
Replication Engines overview (Pillar Axiom MaxMan) 588
Reporting Overview Page 487
Reporting Schedules Overview Page 488
Reset System 558
Run PITMAN Diagnostics 567
SAN Hosts Overview 393
SAN Hosts Overview (Pillar Axiom MaxMan) 587
SAN LUNs Overview page 395, 546

SAN LUNs Overview page (Pillar Axiom MaxMan) 584

SAN Protocol Statistics and Trending Overview Page 490

SAN Protocol Statistics and Trending Overview Page (Pillar Axiom MaxMan) 604

SAN Slammer Ports overview 399

SAN Statistics 492

SAN Statistics (Pillar Axiom MaxMan) 605

SAN Storage overview 402

SAN Storage overview (Pillar Axiom MaxMan) 583

Scheduled Jobs overview 493

Scheduled Jobs overview (Pillar Axiom MaxMan) 606

SCSI Task Management Operations

- FC Slammer details 516
- iSCSI Slammer details 520

Security controls 367

Security Settings overview 403

Set Event Log Filter 494

Slammer Statistics Trending dialog 500

Slammers overview 496

Slammers overview (Pillar Axiom MaxMan) 607

SNMP Hosts overview 404

Software Update Scheduled controls 559

Staged Software controls 560

Statistics Overview page 498

Statistics Overview page (Pillar Axiom MaxMan) 608

status bar components 33

Storage Domains Overview Page 405

Storage Overview 408

Storage Overview (Pillar Axiom MaxMan) 583

Summary Overview 410

System Alerts overview 504

System Alerts overview (Pillar Axiom MaxMan) 609

System Load 512

System Logs overview 563

System Status overview 501

System Summary 411

System Summary controls (Pillar Axiom MaxMan) 594

System Time Overview 413

System Trouble overview 564

Test Connectivity 565

Tools overview 566

Uninterruptible Power Supplies overview 531

Uninterruptible Power Supplies overview (Pillar Axiom MaxMan) 609

usage graphs 409

Utilities overview 578

View Administrator Account 414

View Brick

- Components 506
- I/O Ports 508

View Details Dialog (FC Slammers) 515

View Details Dialog (iSCSI Slammers) 519

View Details Dialog (LUNs) 512

View Event Notification 524

View Host

- Advanced 416

View Reporting Schedule dialog 525

view SAN LUN

- Data Protection 430

View SAN LUN

- mapping 427

View Scheduled Job 510

View Slammer

- Components 526
- I/O Ports 528

View UPS 536

Volume Groups overview page 434

field limits 277

filter

- event log entries 196

firmware updates

- how to
- download firmware package 167

firmware, drive

- about 173
- how to
- remove the installed package 175
- update the staged firmware 174
- upload the package 173

foreign Bricks 181

- definition 187

formats, download

- application packages 26

free capacity

- insufficient 87
- reclaimed 91

FRUs

- about replacement 179
- how to
- replace 180

G

General Information, FC controls 515

General Information, iSCSI controls 519

general purpose Storage Profile settings 105

General, LUNs controls 513

Generate Report Dialog

- field definitions 465

generated reports 240

- how to

- create 241
 - schedule 245
- Generated Reports overview (Pillar Axiom MaxMan)
 - field definitions 598
- Generic Logs Storage Profile settings 105
- GetMarksDb PITMAN command
 - RecordCount 568
 - Summary 568
- GetPitmanStatus PITMAN command 567
- GetStatsSessionInfo PITMAN command 570
- global settings
 - system-wide parameters 38
- Global Settings Overview
 - field definitions 322
- graphical user interface (GUI)
 - how to
 - run Pillar Axiom MaxMan 268
- Groups Overview
 - field definitions 324, 408
- growth increments 89
- GUI
 - status bar 33
- GUI application
 - how to
 - download 26
 - install using MSI 27
 - install using the command line 28
 - log in 31
 - log out 35
- GUI pages
 - Accept Brick 437
 - Administrator Accounts overview 280
 - Administrator Accounts overview (Pillar Axiom MaxMan) 591
 - Alerts and Events (Pillar Axiom MaxMan) 593
 - Associate Hosts 282
 - Axioms overview page (Pillar Axiom MaxMan) 593
 - Bricks Overview 438
 - Bricks Overview (Pillar Axiom MaxMan) 596
 - Clone SAN LUN
 - quality of service 284
 - Configure Trending Chart
 - Chart Thresholds Tab (LUNs) 441
 - Chart Thresholds Tab (Slammers) 442
 - Data Filtering Tab 445
 - Trend Configuration Tab (LUNs) 447
 - Trend Configuration Tab (Slammers) 448
 - Copy SAN LUN
 - mapping 298
 - quality of service 293
 - Create Administrator Account 304
 - Create Chart Threshold Dialog 450, 452
 - Create Data Protection Schedule 540

- Create Event Notification 454
- Create Job Schedule 306
- Create Log Bundle 552
- Create LUN Map 308
- Create Reporting Schedules dialog 456
- Create SAN CloneLUN
 - mapping 288
- Create SAN LUN
 - mapping 314
 - Quality of Service tab 309
- Create SNMP Host 320
- Create Uninterruptible Power Supplies dialog 533
- Create UPS dialog 533
- Data Consistency overview 554
- Data Protection overview page 538
- Delete Log Bundles 555
- Drive Firmware overview 556
- Event Log overview 459
- Event Log overview (Pillar Axiom MaxMan) 601
- Events overview page 461
- Events overview page (Pillar Axiom MaxMan) 597
- Events Properties dialog 462
- Export Dialog 464
- Generate Report Dialog 465
- Generated Reports Overview 466
- Generated Reports overview (Pillar Axiom MaxMan) 598
- Global Settings Overview 322
- Groups Overview 324
- Hardware overview page 467
- Hardware overview page (Pillar Axiom MaxMan) 599
- Host to LUN Mapping overview page 325
- LUN Statistics and Trending page 468
- LUN Statistics and Trending page (Pillar Axiom MaxMan) 602
- LUN Statistics Trending 499
- LUN to Host Mapping overview page 327
- Manage SAN Host Groups
 - Groups Tab 328
 - Hosts Tab 329
- Manage Storage Domains
 - Bricks 330
 - Storage Domains 332
 - Volumes 334
- Manage Storage Profiles 336
- Manage Storage Profiles overview page 342
- Manage System Alert dialog 470
- Manage the List of Axiom Systems 582
- Manage Volume Groups 348
 - Volume Groups 344
 - Volumes 346
- Modify Administrator Account 350

Modify Asset Information *352*

Modify Brick

- Components *471*
- I/O Ports *473*

Modify Data Protection Schedule *542*

Modify Event Notification *477*

Modify Host

- Advanced *353*
- iSCSI Access *356*
- Pillar Axiom Path Manager *354*
- Ports *358*

Modify iSCSI Port Settings *360*

Modify LUN Number page *363*

Modify Network Settings

- Interfaces *364*
- Notification *370*

Modify Reporting Schedule dialog *479*

Modify SAN LUN

- mapping *380*
- Quality of Service tab *375*

Modify Scheduled Job *475*

Modify Security Settings *386*

Modify Slammer

- Components *481*
- I/O Ports *483*

Modify SNMP Host *387*

Modify System Time *389*

Modify Uninterruptible Power Supplies dialog *534*

Modify UPS dialog *534*

Networking Overview *390*

Pilot overview *486*

Pilot overview (Pillar Axiom MaxMan) *600*

Replication Engine overview page (Pillar Axiom MaxMan) *588*

Replication Engines overview page *550*

Reporting Overview Page *487*

Reporting Schedules Overview *488*

Reset System *558*

Run PITMAN Diagnostics *225, 567*

SAN Hosts Overview *393*

SAN Hosts Overview (Pillar Axiom MaxMan) *587*

SAN Protocol Statistics and Trending Overview page *490*

SAN Protocol Statistics and Trending Overview page (Pillar Axiom MaxMan) *604*

SAN Slammer Ports overview *399*

SAN Statistics *492*

SAN Statistics (Pillar Axiom MaxMan) *605*

SAN Storage overview *402*

SAN Storage overview (Pillar Axiom MaxMan) *583*

Scheduled Jobs overview *493*

Scheduled Jobs overview (Pillar Axiom MaxMan) *606*

Security Settings overview *403*

Set Event Log Filter *494*

Slammer Statistics Trending *499*

Slammers overview *496*

Slammers overview (Pillar Axiom MaxMan) *607*

SNMP Hosts overview *404*

Software Modules page *559*

Software Modules page (Pillar Axiom MaxMan) *589*

Statistics Overview page *498*

Statistics Overview page (Pillar Axiom MaxMan) *608*

Storage Domains Overview *405*

Storage Overview *408*

Storage Overview (Pillar Axiom MaxMan) *583*

Storage Usage overview page *409*

Summary Overview *410*

System Alerts overview *504*

System Alerts overview (Pillar Axiom MaxMan) *608*

System Logs overview *563*

System Status overview *501*

System Time Overview *413*

System Trouble overview *564*

Test Connectivity *565*

Tools overview *566*

Uninterruptible Power Supplies overview *531*

Uninterruptible Power Supplies overview (Pillar Axiom MaxMan) *609*

UPS overview *531*

UPS overview (Pillar Axiom MaxMan) *609*

Utilities overview *578*

View Administrator Account *414*

View Brick

- Components *506*
- I/O Ports *508*

View Details Dialog (FC Slammers) *515*

View Details Dialog (iSCSI Slammers) *519*

View Details Dialog (LUNs) *512*

View Event Notification *524*

View Host

- Advanced *416*
- iSCSI Access *419*
- Pillar Axiom Path Manager *417*
- Ports *420*

View Reporting Schedule dialog *525*

View SAN LUN

- mapping *427*
- Quality of Service tab *422*

View Scheduled Job *510*

View Slammer

- Components *526*
- I/O Ports *528*

View SNMP Host *433*

- View Uninterruptible Power Supplies dialog *536*
- View UPS dialog *536*
- Virtual Disk Service (VDS) *580*
- Volume Groups overview page *434*
- Volume Shadow Copy Service (VSS) *581*

H

- halt points, system
 - description *236*
 - how to
 - clear *237*
 - continue startup *238*
 - manage *237*
 - Manage Halt Points dialog *557*
 - overview page *562*
 - use of *236*
- hardware components
 - about replacement *179*
 - how to
 - identify *179*
 - modify names *178*
 - replace *180*
- Hardware overview page
 - field definitions *467*
- Hardware overview page (Pillar Axiom MaxMan)
 - field definitions *599*
- homing logical volumes *149*
- host groups
 - description *141*
 - how to
 - create *144*
 - delete *145*
 - modify *144*
 - managing *143*
- Host Information controls *354, 417*
- Host to LUN Mapping overview page
 - field definitions *325, 327*
- hosts, SAN
 - how to
 - associate with HBAs *140*
 - delete host names *140*
 - display APM driver details *136*
 - install VSS Provider *164*
 - map to LUNs *117, 119*
 - modify APM settings *138*
 - modify HP-UX compatibility mode *137*
 - modify iSCSI Access Settings *138*
 - modify load balancing settings *138*
 - modify LUN mapping *126*
 - modify mapping *128*
 - modify port settings *139*
 - limits
 - names *277*

- management *135*
- HP-UX compatibility mode
 - how to
 - enable *137*

I

- I/O bias
 - description *96*
 - effect on performance *97*
- I/O Latency, FC controls *516*
- I/O Latency, iSCSI controls *520*
- I/O Latency, LUN controls *513*
- identify
 - hardware components *179*
- in-fill reserve capacity *90*
- informational event severity (system event) *505*
- initiators, iSCSI
 - maximum for each iSCSI port *276*
- install
 - GUI application
 - using MSI *27*
 - using the command line *28*
 - VDS Provider *147*
 - VSS Provider *164*
- Installed Software controls *559*
- Installed Software controls (Pillar Axiom MaxMan) *589*
- interfaces, customer
 - setting port speed and duplex mode *364*
- interfaces, management
 - how to
 - configure *42*
- IP addresses
 - how to
 - configure SNMP trap hosts *55*
 - configure the iSCSI ports *139*
 - configure the Pilot IP addresses *42*
 - limits
 - data type and length *278*
 - management interface (Pilot) *41*
 - Pilot *32*
- iSCSI Connectivity and Communication controls *391*
- iSCSI Host Specific Settings controls *356, 419*
- iSCSI page *366*
- iSCSI Port Errors controls *521*
- iSCSI Port Events controls *522*
- iSCSI Port Information controls *358, 420*
- iSCSI Port Requests controls *522*
- iSCSI protocol
 - about iSCSI settings *48*
 - connection status icons *112*
 - how to
 - configure system settings *49*

- modify port settings *139*
- maximum objects *276*
- iSCSI Security controls *392*
- iSNS Server Registration *367*
- iSNS Server Registration controls *49*
- iSNS Settings controls *392*

J

- Job Schedule
 - Create *306*
 - Modify *362*
- jobs, scheduled
 - description *206*
 - how to
 - cancel software updates *172*
 - delete *208*
 - modify *207*
 - view details *206*

L

- licensing optional premium features *37*
- limits
 - field input *277*
 - system objects *275*
- limits for field definitions *275*
- load balancing
 - how to
 - modify settings *138*
- log bundles
 - description *214*
 - how to
 - create *215*
 - download *217*
 - send to Call-Home server *218*
- log in *31*
 - default values *30*
- log out *35*
- login attempts
 - limits *276*
- Login Screen Message *403*
- Login Screen Message controls *386*
- login time-out period *276*
- logs
 - collections, as MIB objects *53*
 - how to
 - delete *218*
 - display (events) *195*
 - display event properties *196*
 - filter (events) *196*
- Loop Activity, FC controls *518*
- loopbacks
 - for SAN Slammer control units *220*
- LUN Map

- Create *308*
- LUN mapping
 - for a specific host *117*
 - for all hosts *119*
- LUN Mapping *289, 299, 315, 381, 428*
- LUN Slammer Control Unit Assignment controls *288, 298, 314, 380, 427*
- LUN Statistics and Trending page
 - field definitions *468*
- LUN Statistics and Trending page (Pillar Axiom MaxMan)
 - field definitions *603*
- LUN Statistics Trending dialog
 - field definitions *499*
- LUNs
 - about capacity attributes *85*
 - about LUN creation *113*
 - about managing *111*
 - different volume group assignment *71*
 - effects on Storage Domains *77*
 - homing *149*
 - how to
 - configure statistics trending charts *254*
 - copy *132*
 - define data protection *121*
 - define Quality of Service *115*
 - delete *134*
 - disable data path *133*
 - display *124*
 - display data protection details *161*
 - enable data path *133*
 - map to a specific host *117*
 - map to all hosts *119*
 - modify *125*
 - modify mapping *126, 128*
 - move to another Slammer CU *126*
 - move to another Storage Domain *130*
 - move to another volume group *71*
 - prevent access through a port *119, 120, 127, 128*
 - remove access *133*
 - restore from a Clone LUN *156*
 - view performance statistics *251*
 - limits
 - names *277*
 - number of *275*
 - size *275*
 - performance statistics *250*
 - thinly provisioned *86*

M

- Manage SAN Host Groups
 - Groups Tab

- field definitions 328
- Hosts Tab
 - field definitions 329
- Manage Storage Domains, Bricks Tab
 - field definitions 330, 334
- Manage Storage Domains, Storage Domains Tab
 - field definitions 332
- Manage Storage Profiles
 - field definitions 336
- Manage Storage Profiles overview page
 - field definitions 342
- Manage System Alert dialog
 - field definitions 470
- Manage the List of Axiom Systems
 - field definitions 582
- Manage Volume Groups
 - field definitions 344, 346
 - Volume Groups 344
 - Volumes 346
- Management Interface controls 364, 390
- management interfaces
 - how to
 - configure 42
 - IP addresses 41
 - setting port speed and duplex mode 364
- mapping
 - a LUN to a specific host 117
 - a LUN to all hosts 119
 - Copy SAN LUN 298
 - Create SAN LUN 288, 314
 - field definitions 288, 298, 314, 380, 427
 - Modify SAN LUN 380
 - View SAN LUN 427
- MARKS database 225
- mask status, Slammer port
 - fully masked port 113
- masks, port
 - how to
 - prevent LUN access 119, 120, 127, 128
- MaxRep Storage Profile settings 104
- MIB table, Pillar Axiom
 - description 53
 - how to
 - download 58
 - objects 53
- Microsoft Exchange Server Storage Profiles 102
- Microsoft SQL Server Storage Profiles 102
- migration, data
 - effects created by Storage Domain creation 78
- mobile devices
 - how to
 - download system status 211
- modify
 - account security settings 52
 - administrator account 62
 - Call-Home settings 47
 - data protection schedule 159
 - email configuration 44
 - event notifications 201
 - hardware component names 178
 - iSCSI port settings 139
 - job schedules 207
 - LUN mapping 126, 128
 - LUNs 125
 - port settings 139
 - reporting schedules 247
 - SAN host settings
 - HP-UX compatibility mode 137
 - iSCSI Access Settings 138
 - Pillar Axiom Path Manager settings 138
 - scheduled software update 171
 - SNMP hosts 56
 - Storage Domains 80
 - system asset descriptions 40
 - volume group attributes 69
- Modify Administrator Account
 - field definitions 350
- Modify Asset Information
 - field definitions 352
- Modify Brick
 - Components
 - field definitions 471
 - I/O Ports
 - field definitions 473
- Modify Event Notification
 - field definitions 477
- Modify iSCSI Port Settings
 - field definitions 360
- modify Job Schedule
 - field definitions 362
- Modify Reporting Schedule dialog
 - field definitions 479
- modify SAN LUN
 - Data Protection
 - field definitions 383
- Modify Scheduled Job
 - field definitions 475
- Modify Slammer
 - Components
 - field definitions 481
 - I/O Ports
 - field definitions 483
- Modify SNMP Host
 - field definitions 387
- Modify System Time
 - field definitions 389
- Modify Uninterruptible Power Supplies overview
 - field definitions 534

- monitored lists (Pillar Axiom MaxMan)
 - how to
 - add Pillar Axiom systems 269
 - modify 274
 - remove Pillar Axiom systems 270
- monitoring system components 44
- move
 - LUNs to another Slammer CU 126
 - volumes to another volume group 71
- msi
 - file type explained 26
- MSSQL Storage Profile settings 102
- MSXchg Storage Profile settings 102

N

- network interfaces
 - about connectivity 41
- Network Time Protocol (NTP)
 - how to
 - configure 39
- NIS naming service
 - limits
 - domain name length
- Notification controls 391
- notifications, event
 - description 198
 - how to
 - configure email server 44
 - create 199
 - delete 201
 - modify 201
 - types of 43

O

- online help 20
- operating limits, system 275
- optional premium features 37
- Oracle ASM performance profile
 - description 106
- Oracle ASM Storage Profile settings 105
- Oracle Database Platform Storage Profiles 103
- Oracle Technical Network (OTN) 20
- Oracle Universal Content Management Storage Profiles 103
- OracleDB Storage Profile settings 103
- OracleUCM Storage Profile settings 103
- over-committed
 - See thinly provisioned volumes
- over-committed volumes
 - See thinly provisioned volumes

P

- parity

- physical capacity 91
- parity data
 - how to
 - verify 213
- passwords, administrator
 - how to
 - change 62, 63
 - recover from forgotten password 30
- Path Manager Settings controls 354, 417
- pds-axiomgui-selfContainedJar.jar
 - explained 28
- perf Slammer command
 - for SAN Slammers 223
- performance
 - how to
 - collect statistics 216
 - Storage Profiles
 - comparisons 99
- Performance Benchmark Storage Profile settings 105
- Performance, FC controls 515
- Performance, iSCSI controls 519
- physical capacity
 - actual amount needed 87
 - used by thinly provisioned volumes 86
 - used for parity 91
- Physical Capacity controls 330, 334
- Pillar Axiom GUI software
 - client software location 27
- Pillar Axiom MaxMan application
 - client software description 24
 - how to
 - run 268
 - information 266
 - monitored components 266
- Pillar Axiom Path Manager
 - how to
 - display driver details 136
 - limits
 - number of data paths 276
 - number of HBA ports 276
 - number of Pillar Axiom systems 276
 - purpose 135
- Pillar Axiom Storage Services Manager
 - description 22
 - how to
 - install 27
 - log in 31
 - log out 35
 - run 31
 - status bar 33
 - Windows shortcut 27
- Pillar Axiom system
 - about accessing 30

-
- capacity usage by replica type *149*
 - client software package
 - description *24*
 - description of status bar *33*
 - how to
 - display software versions *166*
 - display status *211*
 - download software updates *167*
 - identify hardware *179*
 - modify asset descriptions *40*
 - reset the serial number *239*
 - reset the system configuration *239*
 - restart *233*
 - stage the software updates *169*
 - update the software *170*
 - limits
 - length of object names *277*
 - name length *277*
 - log bundles *214*
 - monitoring system components *44*
 - notifications *43*
 - software updates *167*
 - startup *234*
 - Pillar Axiom systems (Pillar Axiom MaxMan)
 - how to
 - add *269, 272*
 - manage *271*
 - remove *270*
 - Pillar Axiom Virtual Disk Service (VDS) Provider
 - how to
 - download *147*
 - Pillar Axiom VSS Provider
 - description *163*
 - how to
 - download and install *164*
 - pillar_eula_text.rtf
 - explained *28*
 - Pilot CU 0/1 Interface controls (Pillar Axiom MaxMan) *595*
 - Pilot management controllers
 - default IP *30*
 - how to
 - upload custom Call-Home matrix *48*
 - upload software updates *169*
 - IP address *32*
 - Pilot Management Interface controls (Pillar Axiom MaxMan) *594*
 - Pilot overview
 - field definitions *486*
 - Pilot overview (Pillar Axiom MaxMan)
 - field definitions *600*
 - pinned data
 - about clearing *204*
 - PITMAN utility
 - how to
 - run *226*
 - Ports Masked for this LUN controls *289, 299, 315, 381, 428*
 - ports, management interface
 - setting *364*
 - ports, Slammer
 - connections status *112*
 - mask status *113*
 - primary Storage Domains
 - definition *76*
 - how to
 - transfer primary status to another domain *82*
 - priority band
 - See priority levels
 - priority levels
 - description *93*
 - private interface (PI) errors
 - how to
 - troubleshoot *226*
 - product support *20*
 - Protection Schedules Overview *539*
 - PushMarksDbToPilot PITMAN command *568*
- ## Q
- Quality of Service (QoS)
 - access bias *95*
 - I/O bias *96*
 - priority levels *93*
 - re-homing of logical volumes *149*
 - redundancy *94*
 - settings for Storage Profiles *101*
 - storage class *92*
 - queue priority
 - definition *93, 286, 295, 311, 336, 377, 424*
- ## R
- RAID arrays
 - geometries *98*
 - stripes *106*
 - virtual capacity *91*
 - RAID commands
 - description *227*
 - how to
 - run *229*
 - view output *228*
 - RAID configuration
 - effects by access and I/O biases *97*
 - RAID controller
 - data consistency tests *212*
 - RAID groups
 - definition *94*
 - optimum number *94*
-

- random write QoS setting
 - enhanced performance 98
 - RAID configuration 97
- ranges for field definitions 275
- re-homing
 - LUNs 126
- read-ahead property 97
- reboot
 - See restart.
- redundancy
 - description 94
- refresh screen content 35
- related documentation 19
- remove
 - a Brick 189
 - a Storage Profile 110
- replace
 - a FRU 180
- replicas
 - capacity usage 149
 - data synchronization differences 150
 - trees 149
- replication engine
 - how to
 - manage 162
- Replication Engines overview
 - field definitions 550
- Replication Engines overview (Pillar Axiom MaxMan)
 - field definitions 588
- Reporting Overview Page
 - field definitions 487
- reporting schedules
 - how to
 - delete 248
 - modify 247
 - view 247
- Reporting Schedules Overview Page
 - field definitions 488
- reports
 - generated 240
 - how to
 - delete 243
 - download 242
 - generate 240, 241
 - schedule 245
 - scheduled 245
- reset
 - system configuration 239
 - system serial number 239
- Reset System
 - field definitions 558
- ResetSImSwitch PITMAN command 571
- restart
 - Pillar Axiom system 233

- restore
 - from a Clone LUN 156
- Run PITMAN Diagnostics
 - field definitions 567
- runAxiomStorageManager.bat
 - explained 28
- runAxiomStorageManager.sh
 - explained 28
- runAxiomStorageManagerEnterprise.bat
 - explained 29
- runAxiomStorageManagerEnterprise.sh
 - explained 29

S

- sales information 20
- SAN hosts
 - how to
 - associate with HBAs 140
 - delete host names 140
 - display APM driver details 136
 - install VSS Provider 164
 - map to LUNs 117, 119
 - modify APM settings 138
 - modify HP-UX compatibility mode 137
 - modify iSCSI Access Settings 138
 - modify load balancing settings 138
 - modify LUN mapping 126
 - modify mapping 128
 - modify port settings 139
 - limits
 - names 277
 - management 135
 - modifying 136
- SAN Hosts Overview
 - field definitions 393
- SAN Hosts Overview (Pillar Axiom MaxMan)
 - field definitions 587
- SAN LUNs Overview page 395, 546
 - field definitions 395, 546
- SAN LUNs Overview page (Pillar Axiom MaxMan)
 - 584
 - field definitions 584
- SAN Protocol Statistics and Trending Overview Page
 - field definitions 490
- SAN Protocol Statistics and Trending Overview Page (Pillar Axiom MaxMan)
 - field definitions 604
- SAN Slammer Ports overview
 - field definitions 399
- SAN Statistics
 - field definitions 492
- SAN Statistics (Pillar Axiom MaxMan)

- field definitions 605
- SAN Storage overview
 - field definitions 402
- SAN Storage overview (Pillar Axiom MaxMan)
 - field definitions 583
- SAN storage parameters
 - how to
 - delete host names 140
 - display host settings 136
 - modify APM settings 138
 - modify HP-UX compatibility mode 137
 - modify iSCSI Access Settings 138
- scheduled jobs
 - how to
 - delete 208
 - modify 207
- Scheduled Jobs overview
 - field definitions 493
- Scheduled Jobs overview (Pillar Axiom MaxMan)
 - field definitions 606
- scheduled reports 245
- scheduled software updates
 - how to
 - cancel 172
 - modify 171
 - limits
 - name length 277
- scheduled tasks (MIB object) 54
- Scheduled Updates page 573, 575
- schedules
 - data protection
 - jobs 206
 - how to
 - view 206
 - reporting 456, 488
- screen updates
 - how to
 - disable 35
 - enable 35
 - manually refresh 35
- SCSI Task Management Operations controls
 - FC Slammer details 516
 - iSCSI Slammer details 520
- Security controls 367
- Security Settings overview
 - field definitions 403
- security settings, account
 - about modifying 51
 - how to
 - configure 52
- session time-out period 276
- Set Event Log Filter
 - field definitions 494
- SetAutoModeOff PITMAN command 567
- SetAutoModeOn PITMAN command 567
- severities of system events 505
- severities, event 194
- shadow copy, volume
 - about the VSS Provider plug-in 163
 - how to
 - download and install the VSS Provider 164
- shut down the system 232
- Slammer Statistics Trending dialog
 - field definitions 500
- Slammer storage controllers
 - connectivity testing 223
 - diagnostics 220
 - how to
 - configure trending charts 260
 - run diagnostics 221
 - view diagnostic results 222
 - view statistics 258
- limits
 - name length 277
- performance statistics 257
- PITMAN commands
 - ClearStats 570
 - CtrlSImDev 570
 - GetMarksDb RecordCount 568
 - GetMarksDb Summary 568
 - GetPitmanStatus 567
 - GetStatsSession Info 570
 - PushMarksDbToPilot 568
 - ResetSImSwitch 571
 - SetAutoModeOff 567
 - SetAutoModeOn 567
 - StartRecordingStats 570
 - StopRecordingStats 570
 - TrafficGenOff 569
 - TrafficGenOn 568
- port connection status 112
- port mask status 113
- SAN connectivity commands
 - perf 223
- startup 234, 236
- testing connectivity 220
- Slammers overview
 - field definitions 496
- Slammers overview (Pillar Axiom MaxMan)
 - field definitions 607
- SMI-S provider
 - system component monitoring 44
- SNMP agent
 - about trap host management 53
 - how to
 - create hosts 55
 - delete hosts 56
 - download the Pillar Axiom MIB table 58

- modify hosts *56*
- view hosts *57*
- limits
 - community strings *279*
- Pillar Axiom resources *53*
- system component monitoring *44*
- SNMP Hosts overview
 - field definitions *404*
- Software modules
 - update options *574*
- Software update
 - options *574*
- Software Update Scheduled controls *559*
- software updates
 - description *167*
 - how to
 - cancel scheduled updates *172*
 - display Pillar Axiom software versions *166*
 - download software package *167*
 - stage the update package *169*
 - update the system *170*
 - view upgrade paths *169*
- software, client
 - available packages *24*
- software, Pillar Axiom
 - versions as MIB objects *54*
- SSNs, drive *181*
- staged software
 - how to
 - view upgrade paths *169*
- Staged Software controls *560*
- StartRecordingStats PITMAN command *570*
- startup, Slammer
 - halt points, use of *236*
 - PROM actions *234*
 - stages *234, 236*
- Statistics Overview page
 - field definitions *498*
- Statistics Overview page (Pillar Axiom MaxMan)
 - field definitions *608*
- statistics, performance
 - for Slammers *257*
 - how to
 - collect *216*
 - configure trending charts for LUNs *254*
 - configure trending charts for Slammers *260*
 - export trending chart *264*
 - print trending charts *265*
 - view for LUNs *251*
 - view for SAN Slammers *258*
 - LUN trending charts *251*
 - LUNs *250*
 - Slammer port trending charts *258*
- status bar
 - component descriptions *33*
 - components *33*
 - status, system
 - summary *211*
 - StopRecordingStats PITMAN command *570*
 - Storage Classes
 - description *92*
 - Storage Domains
 - Brick limits *277*
 - description *73*
 - effect created by
 - adding a Brick *185*
 - adding a logical volume *83, 114*
 - copying a logical volume *132*
 - creating a domain when volumes exist *78*
 - moving a volume to another domain *130*
 - reassigning a Brick to another domain *188*
 - how to
 - accept a Brick *186*
 - create *78*
 - delete *80*
 - modify *80*
 - move a logical volume *130*
 - reassign a Brick *188*
 - transfer primary status to another domain *82*
 - impact scenarios for Bricks and logical volumes *77*
 - managing *77*
 - maximum number *277*
 - name limits
 - names *277*
 - primary (definition) *76*
 - relationship to volume groups *75*
 - unassigned Bricks *75*
 - usage scenarios *73*
 - Storage Domains Overview Page
 - field definitions *405*
 - Storage Overview
 - field definitions (Pillar Axiom MaxMan) *583*
 - Storage Profiles
 - Backup *101*
 - description *99, 107*
 - General Purpose *105*
 - Generic Logs *105*
 - how to
 - create *108*
 - delete *110*
 - view *108*
 - MaxRep *104*
 - MSSQL *102*
 - MSXchg *102*
 - Oracle ASM *105*
 - OracleDB *103*
 - OracleUCM *103*

-
- Performance Benchmark *105*
 - predefined settings *101*
 - Streaming Media *105*
 - Web Files *105*
 - Xen *104*
 - Storage System Fabric (SSF) errors
 - how to
 - troubleshoot *226*
 - storage usage (MIB object) *54*
 - Streaming Media Storage Profile settings *105*
 - stripes overview, RAID array *106*
 - Summary Overview
 - field definitions *410*
 - Support portal *20*
 - support tools
 - description *209*
 - synchronization, data
 - difference among replica types *150*
 - system alerts
 - how to
 - copy to clipboard *203*
 - display *203*
 - manage *203*
 - provided by MIB objects *53*
 - responding to *203*
 - System Alerts overview
 - field definitions *504*
 - System Alerts overview (Pillar Axiom MaxMan)
 - field definitions *609*
 - system halt points
 - description *236*
 - how to
 - clear *237*
 - continue startup *238*
 - manage *237*
 - Manage Halt Points dialog *557*
 - overview page *562*
 - use of *236*
 - system limits *275*
 - System Load controls *512*
 - system logs
 - bundles *214*
 - description *194*
 - System Logs overview
 - field definitions *563*
 - system operating limits *275*
 - system serial numbers
 - how to
 - reset *239*
 - system startup *234*
 - System Status overview
 - field definitions *501*
 - System Summary
 - field definitions *411*
 - System Summary controls (Pillar Axiom MaxMan)
 - 594*
 - System Trouble overview
 - field definitions *564*
 - system, Pillar Axiom
 - capacity usage by replica type *149*
 - configuration (as an MIB object) *54*
 - description of status bar *33*
 - event severities *505*
 - how to
 - configure time *39*
 - display event logs *195*
 - display event properties *196*
 - identify hardware *179*
 - modify asset descriptions *40*
 - modify hardware names *178*
 - reset the serial number *239*
 - reset the system configuration *239*
 - restart *233*
 - shut down *232*
 - update the software *170*
 - upload the software *169*
 - monitoring system components *44*
 - notifications *43*
 - T
 - tar
 - file type explained *26*
 - tasks, scheduled
 - how to
 - view details *206*
 - tasks, system
 - as an MIB object *54*
 - background tasks (MIB object) *54*
 - TCP connections
 - maximum for each iSCSI port *276*
 - technical support *20*
 - telephone numbers
 - limits
 - data type and length *278*
 - test
 - Call-Home *46*
 - Test Connectivity
 - field definitions *565*
 - tgz
 - file type explained *26*
 - thin provisioning
 - definition *85*
 - on Linux *89*
 - on Windows NTFS *88*
 - thinly provisioned volumes
 - definition *86*
 - on Windows NTFS *88*
-

- provisioning of 88
- Tools overview
 - field definitions 566
- tools, support
 - description 209
 - PITMAN description 225
- TrafficGenOff PITMAN command 569
- TrafficGenOn PITMAN command 568
- training programs 20
- traps (MIB object) 54
- trending charts
 - configure for SAN Slammers
 - how to 260
 - how to 260
 - configure for LUNs 254
 - export 264
 - print 265
 - LUNs 251
 - Slammer ports 258
- troubleshooting
 - Call-Home logs 45
 - how to
 - clear system halt points 237
 - continue system startup after a halt 238
 - run PITMAN 226
 - set halt points 237
- txt
 - file type explained 26
- typographical conventions 20

U

- unassociated hosts
 - definition 135
- Uninterruptible Power Supplies overview
 - field definitions 531
- Uninterruptible Power Supplies overview (Pillar Axiom MaxMan)
 - field definitions 609
- upload
 - Call-Home matrix 48
- UPS
 - how to
 - create 191
 - delete 193
 - modify 192
 - view 192
- usage graphs
 - field definitions 409
- Utilities overview
 - field definitions 578
- utilities software
 - how to
 - download 26

V

- VDS
 - See Pillar Axiom Virtual Disk Service (VDS) Provider.
- verify
 - data consistency 213
- view
 - account summaries 61
 - alerts 204
 - capacity usage 65
 - clone LUN details 155
 - data protection details 161
 - data protection schedules 152
 - event logs 195
 - event notification details 200
 - event properties 196
 - hardware component status
 - overview 176
 - hardware FRU details 177
 - LUN details 124
 - reporting schedules 247
 - SAN host settings 136
 - SAN Slammer statistics 258
 - Slammer diagnostic results 222
 - Storage Profiles 108
 - system alerts 203
 - UI client logs 215
- View
 - Data Protection Schedule 544
- View Administrator Account
 - field definitions 414
- View Brick
 - Components
 - field definitions 506
 - I/O Ports
 - field definitions 508
- View Details Dialog (FC Slammers)
 - field definitions 515
- View Details Dialog (iSCSI Slammers)
 - field definitions 519
- View Details Dialog (LUNs)
 - field definitions 512
- View Event Notification
 - field definitions 524
- View Reporting Schedule dialog
 - field definitions 525
- View SAN LUN 427
 - Data Protection
 - field definitions 430
- View Scheduled Job
 - field definitions 510
- View Slammer
 - Components
 - field definitions 526

- I/O Ports
 - field definitions *528*
- View Uninterruptible Power Supplies overview
 - field definitions *536*
- virtual capacity, Brick *91*
- Virtual Disk Service (VDS) *580*
- Virtual Disk Service (VDS) Provider, Pillar Axiom
 - how to
 - download *147*
- Virtual Tape Library (VTL) Storage Profiles *101*
- VLAN IDs
 - data type and length *278*
 - maximum for each iSCSI port *276*
- volume capacities, about *85*
- Volume Copies
 - capacity usage *150*
 - re-homing of logical volumes *149*
- volume groups
 - about volume groups *67*
 - how to
 - create *69*
 - delete *70*
 - modify attributes *69*
 - limits
 - name length *277*
 - number of *275*
 - relationship to Storage Domains *75*
- Volume Groups overview page
 - field definitions *434*
- Volume Shadow Copy Service (VSS) page *581*
- VSS Provider
 - See Pillar Axiom VSS Provider.*
- VSS Provider, Pillar Axiom
 - description *163*
 - how to
 - download and install *164*

W

- warning event severity (system event) *505*
- Web Files Storage Profile settings *105*
- Wide Stripe feature *106*
- Windows installer
 - how to
 - install GUI application *27*
- write cache, LUN *205*

X

- Xen Storage Profile settings *104*
- XenServer Storage Profiles *104*

Z

- zip
 - file type explained *26*