Pillar Axiom Data Protection Manager

User's Guide

Part Number: E35775-01
Pillar Axiom Data Protection Manager release 3.0
2012 September

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

Chapter 3 Manage Checkpoints

Chapter 4 Manage Checkpoint Schedules

Chapter 5 Manage DPM Events

Appendix A GUI Field Definitions

Appendix B Axiom DPM CLI Command Reference

Appendix C Known Issues

List of Figures

List of Tables

Preface

Related Documentation

Being familiar with certain other Oracle Pillar Axiom technical documentation helps you succeed in the use of this guide.

Familiarize yourself with the following related documentation:

- *Pillar Axiom Customer Release Notes*: Includes late-breaking, important information about the installation and operation of the Pillar Axiom system.
- *Pillar Axiom Administrator's Guide*: Provides detailed information on creating and managing storage resources.
- *Pillar Axiom CLI Reference Guide* or *CLI Reference Guide*: Provides detailed information about functions available in the Pillar Axiom command line interface (CLI).
- Microsoft Volume Shadow Copy Service Technical Reference (http://technet.microsoft.com/en-us/library/cc738819(WS.10).aspx).

Typographical Conventions

Table 1 Typography to mark certain content

Convention	Meaning
italics	Within normal text, words in italics indicate one of the following: • A reference to a book title • New terms and emphasized words • Command variables
`monospace`	Indicates one of the following, depending on the context: • The name of a file or the path to the file

Table 1 Typography to mark certain content (continued)

Convention	Meaning
	- *Output* displayed by the system on the command line
`monospace` (bold)	*Input* provided by an administrator on the command line.
>	Indicates a menu item or a navigation path in a graphical user interface (GUI). For example, “Click Storage > Clone LUNs” means to click the Clone LUNs link on the Storage page in the graphical user interface (GUI).
...	Used within an expression of a navigation path or within a cascading menu structure. The ellipsis indicates that one or more steps have been omitted from the path or menu structure. For example, in the Groups > Volume Groups > Actions > ... > Data Protection > Create menu structure, the ... implies that one or more menu items have been omitted.

Oracle Contacts

Table 2 Oracle resources

For help with...	Contact...
Support	http://www.oracle.com/support/index.html
Training	https://education.oracle.com
Documentation	- Oracle Technical Network: http://www.oracle.com/pls/topic/lookup?ctx=pillardocs - From the Pillar Axiom Storage Services Manager (GUI): Support > Documentation - From Pillar Axiom HTTP access:

Table 2 Oracle resources (continued)

For help with...	Contact...
	http://*system-name-ip*/documentation.php where *system-name-ip* is the name or the public IP address of your system.
Documentation feedback	http://www.oracle.com/goto/docfeedback
Contact Oracle	http://www.oracle.com/us/corporate/contact/index.html

CHAPTER 1

Data Protection Manager Overview

About Data Protection Manager

The Pillar Axiom Data Protection Manager (DPM) runs in a physical or virtual environment and gives you the capability to schedule backups of your data on a regular basis.

DPM is an application that manages application-aware backup and recovery for the Pillar Axiom 600 system. The Data Protection Manager 3.0 runs on Windows, Linux, and Solaris OSs. DPM is available with both GUI and CLI interfaces.

DPM can be run from a physical or virtual environment. To work in a virtual environment, DPM requires Pillar Axiom system release 5.0, or later.

Backups within the DPM environment are called *checkpoints*. A checkpoint represents a consistent point-in-time image of all the LUNs that comprise the application data that was backed up. DPM creates a checkpoint by instructing the Pillar Axiom system to create Clone LUNs that represent the application data.

DPM allows you to control the number of checkpoints that the system retains by using the DPM retention policy. The retention policy allows you to maintain the maximum number of checkpoints or set a maximum amount of time to keep older checkpoints on your system. You can override this policy on selected checkpoints.

Data Protection Manager Requirements

Pillar Axiom Data Protection Manager has a number of requirements that must be met for the program to work properly.

Table 3 Data Protection Manager requirements

Requirement	Required version
Windows operating systems	Microsoft Windows Server 2003 (32 and 64 bit) Microsoft Windows Server 2008 (32 and 64 bit) Microsoft Windows Server 2008, R2 (64 bit)
Linux operating systems	RHEL 5.5, or later RHEL 6.0, or later Oracle Enterprise Linux 5.5, or later Oracle Enterprise Linux 6.0, or later
Solaris operating systems	Solaris Sparc 10 update 10 Solaris Sparc 11 Solaris x86 10 update 10 (32 and 64 bit), and later Solaris x86 11 Express
VSS-enabled applications	Microsoft Exchange Server 2003 Microsoft Exchange Server 2007 Microsoft Exchange Server 2010 Microsoft SQL Server 2005 Microsoft SQL Server 2008 Microsoft Sharepoint Server 2011
Oracle databases **Note:** Oracle databases are supported on Windows, Solaris, and Linux OSs.	Oracle Database 10g R2 Oracle Database 11gR1 Oracle Database 11gR2
Pillar Axiom software release with Fibre Channel SAN	Release 5.3.1, or later

Table 3 Data Protection Manager requirements (continued)

Requirement	Required version
fabric or iSCSI Ethernet connectivity capability.	
Pillar Axiom SMIProvider feature is enabled	N/A
Java Runtime (Linux and Solaris only). **Note:** DPM for Windows contains a version of JRE.	Version 1.7 Set the environment variable `%JAVA_HOME%` to the JRE parent directory.

Related concepts

- *About Data Protection Manager Software*

About VSS Integration in DPM

Pillar Axiom Data Protection Manager (DPM) uses the Microsoft Volume Shadow Copy Service (VSS) to make shadow copies of application data, which is stored on a Pillar Axiom system.

VSS enables data protection and management services through a standard set of configuration and monitoring capabilities. These capabilities include creating, and manipulating backups without shutting down applications or essential services. During a restore operation, VSS is shutdown.

A component of the VSS feature is the Hardware Provider Plug-In. The plug-in provides backups of the application data without disturbing normal operations on the Pillar Axiom system. VSS is a feature of the Microsoft Windows Server and the plug-in installs with the DPM product.

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) provided by Microsoft.
- The Microsoft Developers Network (MSDN) article The VSS Model (Windows) (http://msdn.microsoft.com/en-us/library/aa384625.aspx).

About Application-Aware Backups

Pillar Axiom Data Protection Manager (DPM) is an application-aware program that creates backups of the data that is associated with a managed application. The backups are called *checkpoints*. Checkpoints consist of one or more Clone LUNs.

An *application instance* is the state of an application and its associated data. To provide enough information to recreate an application instance, backups of application data include all relevant raw data as well as a log file. Some applications use log files that contain the application metadata to make the raw data meaningful.

The Pillar Axiom system stores data in a collection of LUNs that DPM recognizes as an *application consistency group*. Each consistency group contains all the data necessary to represent a restorable application instance.

During a checkpoint operation, the Pillar Axiom system momentarily stops all write operations and writes any cached application data to disk. The Axiom system then creates the Clone LUNs that represent the entire consistency group. After DPM creates the checkpoint, the application resumes normal read and write operations.

Data Protection Manager creates checkpoints of Oracle databases, Microsoft Exchange Server, or Microsoft SQL Server consistency groups that are stored on Pillar Axiom systems. What constitutes a consistency group differs among these applications. DPM keeps track of the LUNs that are associated with each application consistency group. This tracking process maintains data integrity during a restore operation of the checkpoint.

Related concepts

- *About Application Consistency Groups*

Related references

- *LUN Configuration for Data Consistency*
- *LUN Configuration for Applications*
- *Best Practice Resources*
- *Applications Overview Page*
- *LUN Configuration for Applications*

LUN Configuration for Applications

Configuring the LUNs of your applications affects data performance and integrity. Consider the following practices when configuring the LUNs for your applications.

- Apply Quality of Service (QoS) properties to the LUNs to optimize data throughput. The Pillar Axiom Storage Services Manager provides QoS Storage Profiles for database applications. Choose the profile for your database environment.

  Refer to the *Pillar Axiom Administrator's Guide*.

- In a virtual environment, configure the LUNs using raw device mapping (RDM). RDM stores the data information directly to the LUN instead of a virtual disk file.

- For iSCSI systems Data Protection Manager has direct access to the Pillar Axiom LUNs for mapping and informational purposes. RDM is not necessary in iSCSI environments.

About Exchange Server Backups

Microsoft Exchange Server stores data in storage groups, which are Exchange Server application instances.

Storage groups are groups of LUNs that you define when you set up your Exchange Server implementation. Microsoft Exchange storage groups can contain data LUNs and transaction log LUNs. For best performance with Pillar Axiom Data Protection Manager (DPM), we recommend setting up storage groups that consist of dedicated LUNs that are not used by other applications.

Data Protection Manager recognizes each Exchange storage group that is set up on a Pillar Axiom system as a consistency group. A consistency group contains all the data necessary to represent the Exchange application instance. DPM manages the process of making backups of these consistency groups on the Pillar Axiom system.

Related references

- *Best Practice Resources*
- *Applications Overview Page*

Related tasks

- *Refresh Applications*

About SQL Server Backups

Microsoft SQL Server stores data in database instances, which are SQL Server application instances.

Database instances consist of one or more LUNs that you define when you set up your SQL Server implementation. For best performance with Pillar Axiom

Data Protection Manager (DPM), we recommend that each database instance you set up consist of dedicated LUNs that are not used by other applications.

Data Protection Manager recognizes each database instance set up on a Pillar Axiom system as a consistency group. A consistency group contains all the data necessary to represent the SQL server application instance. DPM manages the process of creating backups of these consistency groups on the Pillar Axiom system.

Related references

- *Best Practice Resources*
- *Applications Overview Page*

Related tasks

- *Refresh Applications*

Microsoft Sharepoint Database Requirements

Pillar Axiom Data Protection Manager (DPM) supports instances of Microsoft Sharepoint that use Microsoft SQL or Oracle databases on the back end. DPM recognizes the databases provided that the specified requirements are met.

The Sharepoint database requirements include:

- Mount the database on Pillar Axiom LUNs.
- Install DPM on the database server where the LUNs are mounted.
- Install the database application on the server that runs DPM.

DPM performs a backup of the database that represents the Sharepoint data source. When you configure the database on a Pillar Axiom system, DPM recognizes the database consistency groups that support the Sharepoint application. As a result, DPM displays the supported Sharepoint database on the Applications overview page as either `Oracle` or `Microsoft SQL`, not the Sharepoint application.

Related concepts

- *About Application Consistency Groups*

Related references

- *Best Practice Resources*
- *Applications Overview Page*

Related tasks

- *Refresh Applications*

Oracle Automatic Storage Management Requirements

Automatic Storage Management (ASM) is an integrated file system and volume manager built for managing Oracle database files.

Pillar Axiom Data Protection Manager (DPM) supports Oracle databases that use ASM. ASM provides the performance of raw I/O with the easy management of a file system. ASM simplifies database administration by eliminating the need to directly manage numerous Oracle database files. ASM allows you to divide all of the available storage into Oracle ASM disk groups. You manage a small set of disk groups and ASM automates the placement of the database files within those disk groups.

You have two methods for configuring the ASM instance. You can use an initialization parameter file (PFILE) or a server parameter file (SPFILE). Both of these parameter files contain all of the ASM instance configuration details. Whichever method you use, store the parameter file on a disk group that is not being used by the managed databases.

For more information about installing and configuring Oracle ASM, see the following resources:

- Backing Up, Copying, and Moving an Oracle ASM Initialization Parameter File (http://oracle.su/docs/11g/server.112/e10500/asminst.htm#CHDEGEGB)
- Using Automatic Storage Management (http://docs.oracle.com/cd/B19306_01/server.102/b14231/storeman.htm)

When you configure the disk groups for Data Protection Manager, the following restrictions apply.

- Create one drive partition for each Pillar Axiom LUN.
- DPM treats each disk group as a consistency group, which allows DPM to back up and restore the consistency group as a single data block.
- Each disk group must consist of LUNs from a single Pillar Axiom system.
- Store all of the database files such as the control files, redo log files, and data files, on a single ASM disk group.
- Keep the ASM disk group separated from the Oracle database flash recovery area (FRA). The FRA is where you store the database archived redo log files.

- Oracle ASM can manage more than one database and several databases can reside in the same disk group, but a database must not reside on more than one disk group.
- Multiple databases that use the same disk group are backed up and restored together.
- DPM restores databases with an automatic point-in-time recovery. Roll-forward recovery is not supported.
- For Linux and Solaris OSs, DPM requires that you provide a username for the ASM instance and a username for each database you wish to manage. The username provides DPM with authenticated access to the databases. Passwords are not necessary.
- If an ASM application contains a consistency group, it represents a disk group, and you cannot set or change the credentials for that consistency group.

DPM performs tests to ensure that the above requirements are met and provides feedback if a problem occurs.

Related concepts

- *About Application Consistency Groups*

Related references

- *Oracle Database Requirements*
- *Applications Overview Page*
- *View Consistency Group, Oracle Databases Tab*

Related tasks

- *Set the Oracle Username*
- *Set the ASM Username*

Oracle Database Requirements

Pillar Axiom Data Protection Manager (DPM) can back up and restore Oracle database data. You can run multiple instances of the Oracle database, as necessary. Each database instance can have a different version number.

DPM recognizes Oracle databases when the following requirements are met:

- Each database instance must use LUNs from a Pillar Axiom system.
- The LUNs of each database must reside on a single Pillar Axiom system.
- The database LUNs must not be shared with other applications or databases, which assures backup and restore data integrity.

- Configure your Oracle database to run in *archivelog* mode. This mode provides DPM with the capability to perform online backup and restore operations.
- Place the flash recovery area (FRA) on a separate LUN that is not managed by a file management system such as the Oracle Automatic Storage Management (ASM) disk group. The FRA is where the Oracle database stores the archived redo log files. Separating the files from the ASM storage area assures backup and restore data integrity.
- For Linux and Solaris OSs, DPM requires that you provide an Oracle database username to authenticate access to the database. A password is not necessary.

Related concepts

- *About Application Consistency Groups*

Related references

- *Oracle Automatic Storage Management Requirements*
- *Applications Overview Page*
- *View Consistency Group, Oracle Databases Tab*

Related tasks

- *Set the Oracle Username*
- *Set the ASM Username*

Best Practice Resources

To work optimally with the Pillar Axiom Data Protection Manager, you might find the following documents useful for configuring your server.

For more information about Microsoft SQL server and Microsoft Exchange server best practices, refer to the following resources:

- Storage Top 10 Best Practices (http://technet.microsoft.com/en-us/library/cc966534.aspx)
- Mailbox Server Storage Design (http://technet.microsoft.com/en-us/library/bb738147(EXCHG.80).aspx)

About the DPM Virtual Environment

The Pillar Axiom Data Protection Manager (DPM) can operate in a virtual environment.

DPM supports the following virtual environments:

- VMWare ESX
- Hyper-V

The virtual environment infrastructure consists of the following primary components:

VMware ESX host The ESX host contains one or more virtual machine (VM) guests that are installed and configured by the server administrator. A VM configured for DPM requires that you install VMWare tools.

Important! The ESX host relies on a stable communication link with the Pillar Axiom management interface. If the ESX host loses communication with an Axiom system, the ESX server administrator might need to restart the ESX server to establish the connection and refresh the list of discovered systems.

DPM VMI Service The DPM virtual machine interface (VMI) provides a bridge between the VM and physical host. The VMI is available for Hyper-V and VMware ESX hypervisors.

VMware vCenter The vCenter server provides administrative support for the ESX host. The vCenter server communicates with the ESX host and all of the VMs installed on the ESX host.

Hyper-V Server Hyper-V provides the software infrastructure and basic management tools that enables you to create and manage a virtualized server.

When DPM starts from a virtual environment, DPM VMI verifies the following information to establish a connection to the virtual environment:

- The host IP address where the DPM VMI is installed
- The login name and password for the DPM VMI server host
- The HTTPS communications port that is used by the DPM VMI service

DPM initializes after successfully connecting to the DPM VMI service.

DPM might display errors if the credentials to the DPM VMI server host are changed or otherwise unavailable. If DPM fails to connect to the VMI server on startup, DPM posts failure messages in the event log.

If the server credentials have changed while DPM is running, some DPM actions might fail. Use the **Modify Virtual Machine Credentials** menu option to enter the correct credentials, then try the action again.

In a physical host environment, DPM initializes normally without the steps to confirm the virtual machine credentials.

Related concepts

- *About Hyper-V Support For DPM*

Related references

- *Virtual Machine Requirements*
- *Modify Virtual Machine Server Credentials Dialog (Step 1)*
- *Modify Virtual Machine Server Credentials Dialog (Step 2)*

Related tasks

- *Modify Virtual Machine Credentials*
- *Run Data Protection Manager for the First Time*
- *Install the DPM VMI Service*
- *Download the Data Protection Manager Software*
- *Download Pillar Axiom Utility Software*

Virtual Machine Requirements

The virtual machine environment has a number of requirements that must be met.

Table 4 Virtual machine requirements

Requirement	Required version or value
Windows operating systems	Microsoft Windows Server 2003 Microsoft Windows Server 2008
Pillar Axiom release version	Release 5.4, or later
VMware ESX virtual host	4.0 or 4.1
VMware Tools	Same version as VMware ESX software

Table 4 Virtual machine requirements (continued)

Requirement	Required version or value
	Note: Hypervisor support is limited to the supported OS.
VM login credentials	• Host IP address where the DPM VMI is installed • vCenter server Hyper-V Server host login username and password • HTTPS communications port to the DPM VMI

Related concepts

- *About the DPM Virtual Environment*

Related tasks

- *Modify Virtual Machine Credentials*

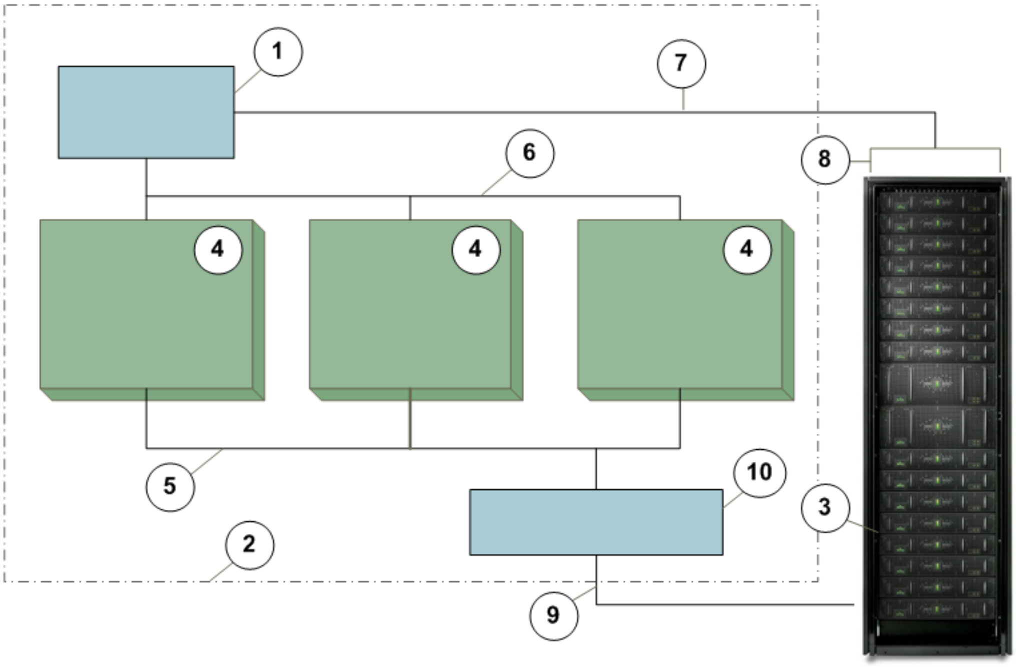
About Hyper-V Support For DPM

Pillar Axiom Data Protection Manager (DPM) can be run from a virtual server computing environment, such as Microsoft Hyper-V.

Hyper-V provides the software infrastructure and basic management tools that enables you to create and manage a virtualized server. Within the virtual environment you can create a virtual machine (VM) guest host. The guest host provides a virtual machine interface (VMI) that allows administrators to install and run DPM in a virtual environment. The DPM interface and functionality is the same whether run from within a virtual or physical environment.

Hyper-V is available on Windows 2008 R2 servers. This version provides the ability to dynamically add storage to an existing virtual machine. This feature allows you to add storage to your virtual environment without service disruption.

Figure 1 DPM in a Microsoft Hyper-V environment



Legend

1 DPM VMI Service	6 DPM VMI API calls
2 Windows 2008 R2 server with Hyper-V enabled	7 Pillar Axiom access
3 Pillar Axiom system	8 WebCLI
4 Virtual Machine guest running DPM with any of the following applications: ○ SQL database ○ Microsoft Exchange ○ Oracle database	9 Mapped LUN information
5 Pass-through LUNs access	10 HBA

In the above illustration, a Windows 2008 R2 server is configured with a Hyper-V environment and three VM guests. Each VM guest is configured with different applications. DPM manages the supported applications independently using a single VMI service.

Such a configuration assures data integrity by keeping the LUNs of each database separated from other database instances.

Related concepts

- *About the DPM Virtual Environment*

Related tasks

- *Run Data Protection Manager for the First Time*
- *Install the DPM VMI Service*
- *Download the Data Protection Manager Software*
- *Download Pillar Axiom Utility Software*

Chapter 2

Install Data Protection Manager

About Data Protection Manager Software

The installation package for the Pillar Axiom Data Protection Manager (DPM) contains the files necessary to install the main program and the hardware provider plug-in.

The DPM installation package performs the following actions:

- For Windows system, installs the Volume Shadow Copy Service (VSS) hardware provider plug-in, as necessary.
- For all OSs, installs the Data Protection Manager graphical user interface (GUI), CLI, and host agent service applications.

Additional utility software might be required if, for example, you are running DPM in a virtual environment.

Related references

- *Data Protection Manager Requirements*

Related tasks

- *Download the Data Protection Manager Software*
- *Download Pillar Axiom Utility Software*
- *Install Data Protection Manager for Windows*
- *Install Data Protection Manager for Linux*
- *Install Data Protection Manager for Solaris*

Download the Data Protection Manager Software

Download Pillar Axiom Data Protection Manager (DPM) and any necessary utilities from My Oracle Support (MOS) so that you can install the software on a host.

Prerequisite	A Customer Support portal account.

1 Point your web browser to My Oracle Support (http://support.oracle.com) and log in.

2. On the top menu bar, click **Patches & Updates**.
3. From the Patch Search pane Search tab, click **Product or Family (Advanced)**.
4. From the **Product** field enter the product family as the first search criterion.

   ```
   Oracle Axiom Product Family
   ```

5. From the **Release** drop-down list, select the appropriate DPM product release.
6. (Optional) From the **Platform** drop-down list, select the desired platform operating system.
7. Click **Search**.

   Result:
   The system displays the Patch Search page with your search results.

8. (Optional) Click **Edit Search** to refine your search criteria.
9. To display detailed information about the DPM version, click the link under the **Patch Name** field.

   Result:
   The Patch Search page displays details about the released software version and provides a download link.

10. To download the software package, click **Download**.
11. Save the software to your workstation.
12. (Optional) To read information about the download or the Release Notes (if available), click **Read Me**.

Related concepts

- *About Data Protection Manager Software*

Related tasks

- *Download Pillar Axiom Utility Software*
- *Install Data Protection Manager for Windows*
- *Install Data Protection Manager for Linux*
- *Install Data Protection Manager for Solaris*

Download Pillar Axiom Utility Software

The utility software for the Pillar Axiom system is available on the Pilot management controller, which is accessed from a web browser.

You will need the system name or IP address to the Pillar Axiom system that contains the utility software. Contact the system administrator for the login credentials.

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 Utility Software.

4 Select a link for the software that you want to download.

5 Save the file to your client workstation.

In the next steps you can perform one of the following actions:

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

Install Data Protection Manager for Windows

Install Pillar Axiom Data Protection Manager by running the installer that you downloaded from the Customer Support Portal to your host system.

Prerequisites:

○ You are logged in as administrator.

○ No previous versions of Data Protection Manager and Volume Shadow Copy Service (VSS) hardware provider exists on the system.

When you install DPM, the procedure also installs VSS.

1 Locate the downloaded DPM installation package on your system and double click the package name.

  Note: The filename for the DPM installation package is dpm_n.n.n.exe, where *n* is the revision number.

2 From the welcome installation screen, follow the instructions provided in the installation wizard.

Note: We recommend accepting the default installation folder location.

3 From the Welcome to the Pillar Axiom Data Protection Manager Setup Wizard dialog, click **Next**.

4 Accept the defaults for the next screen by clicking **Next**.

5 From the Completing the Pillar Axiom Data Protection Manager Setup Wizard screen, click **Finish** to close the wizard.

Related concepts

- *About Data Protection Manager Software*

Related tasks

- *Download the Data Protection Manager Software*
- *Download Pillar Axiom Utility Software*
- *Install Data Protection Manager for Linux*
- *Install Data Protection Manager for Solaris*

Install Data Protection Manager for Linux

You can install the Pillar Axiom Data Protection Manager package on Red Hat Enterprise Linux and Oracle Enterprise Linux operating systems.

Prerequisites:

○ You are logged in as root.

○ No previous versions of Data Protection Manager exists on the system.

Use the same installer package for any of the supported Linux operating systems and architecture (32-bit or 64-bit).

1 Copy the installation archive file to the Linux server.

2 Use the `rpm` utility to extract and install the archive file.

```
$ rpm -i InstallPackageName
```

Where *InstallPackageName* is the filename of the installation package.

Result:
Data Protection Manager installs to the default directory, which is`$/Applications/System Tools/Pillar Axiom Data Protection Manager`.

3 Set the security permissions to the DPM executable file to restrict access to Data Protection Manager to only authorized personnel.

Example:
For example:

```
$ chmod -744 "/Applications/System Tools/Pillar Axiom
Data Protection Manager/bin/runHostAgentManager.sh"
```

Note: Security restrictions vary by location. Consult your system administrator for the proper security setting.

Related concepts

- *About Data Protection Manager Software*

Related tasks

- *Download the Data Protection Manager Software*
- *Download Pillar Axiom Utility Software*
- *Install Data Protection Manager for Windows*
- *Install Data Protection Manager for Solaris*

Install Data Protection Manager for Solaris

You can install the Pillar Axiom Data Protection Manager package on Solaris Sparc or Solaris Intel architectures.

Make sure that you are using the correct Data Protection Manager installer package for your Solaris system architecture:

- For Solaris on Intel: `DPM-i386-`*`xxx`*`.pkg`
- For Solaris Sparc: `DPM-sparc-`*`xxx`*`.pkg`

where *xxx* is the appropriate version number for the software package.

1 Copy the installation archive file to the Solaris server.

2 Use the `pkgadd` command to extract and install the archive file.

```
$ pkgadd -d InstallPackageName
```

Result:
Data Protection Manager installs to the default directory which is `$/Applications/Utilities/Pillar Axiom Data Protection Manager`.

3 Set the security permissions to the DPM executable file to restrict access to Data Protection Manager to only authorized personnel.

Example:
For example:

```
$ chmod -744 "/Applications/Utilities/Pillar Axiom Data
Protection Manager/bin/runHostAgentManager.sh"
```

Note: Security restrictions vary by location. Consult your system administrator for the proper security setting.

Related concepts

- *About Data Protection Manager Software*

Related tasks

- *Download the Data Protection Manager Software*
- *Download Pillar Axiom Utility Software*
- *Install Data Protection Manager for Windows*
- *Install Data Protection Manager for Linux*

Install the DPM VMI Service

When installing Pillar Axiom Data Protection Manager (DPM) in a virtual environment such as a vSphere or Hyper-V, you must install the virtual machine interface (VMI) service. The DPM virtual machine interface (VMI) provides a bridge between the VM and physical host. The VMI is available for Hyper-V and VMware ESX hypervisors.

Prerequisites: A functioning virtual machine exists on the host where DPM will be installed. DPM supports the following utilities:

- For VMWare ESX, which is managed by a vCenter server:

  install-win-pds-dpmvmiserver-vcenter.exe

- For Hyper-V:

  install-win-pds-dpmvmiserver-hyperv.exe

You install the DPM VMI onto the following locations:

- For VMWare ESX: Install the software onto the Windows server that is running the vCenter server.
- For Hyper-V: Install the software onto the virtual machine host.

1 Locate the downloaded DPM VMI installation package and double-click the package name.

2 From the Welcome screen, click **Next**.

3 From the Installation Folder dialog, accept the default folder location, or provide a folder name of your choice, and click **Next**.

Note: We recommend accepting the default installation folder location.

4 From the Port Information dialog, record the VMI communications port number for later use.

The port number is used when installing DPM on a virtual machine.

Note: Also ensure that the port is available through the firewall on the system.

5 To continue, click **Next**.

6 From the Ready to Install dialog, click **Next**.

Result:
The program completes the installation steps.

When the installation is complete, the DPM VMI service starts.

Note: Be sure that the VMI port number on your system firewall is open.

Related concepts

- *About Hyper-V Support For DPM*
- *About the DPM Virtual Environment*

Related tasks

- *Run Data Protection Manager for the First Time*
- *Download the Data Protection Manager Software*
- *Download Pillar Axiom Utility Software*

About Data Protection Manager Security

Pillar Axiom Data Protection Manager (DPM) encrypts all data transmissions to attached clients to ensure data integrity and security.

- DPM never exposes passwords in clear text within the GUI or command line.
- DPM stores passwords in an internal database and secures the data with a customer-supplied encryption key.
- The DPM administrator sets the encryption key during the initial startup, or as necessary.
- DPM transmits data over a secure socket layer (SSL).

Related tasks

- *Run Data Protection Manager for the First Time*
- *Set the Data Protection Manager Encryption Key*

Run Data Protection Manager for the First Time

When you run Pillar Axiom Data Protection Manager (DPM) for the first time, the system prompts you for an encryption key and the type of environment from which to run the application.

You might be prompted for the encryption key or environment type if this information has been changed on system.

1. Log in to the computer where DPM is installed.
2. Launch the DPM application.
   - For Windows, choose **Start** > **All Programs** > **Oracle Corporation** > **Pillar Axiom Data Protection Manager** > **Pillar Axiom Data Protection Manager**.
   - For Linux, choose **Applications** > **System Tools** > **Pillar Axiom Data Protection Manager**.
   - For Solaris, choose **Applications** > **Utilities** > **Pillar Axiom Data Protection Manager**.

   Result:
   The system displays the Update Encryption Key dialog.
3. From the Update Encryption Key dialog, enter the key, then click **Submit**.

Result:
If you are running DPM in a virtual environment, the Virtual Machine Environment dialog displays.

4 (Optional) From the Virtual Machine Environment dialog, select the **Virtual Machine** checkbox and then click **Submit**.

The Data Protection Manager GUI opens the Axioms overview page.

Related concepts

- *About Hyper-V Support For DPM*
- *About the DPM Virtual Environment*
- *About Data Protection Manager Security*

Related tasks

- *Install the DPM VMI Service*
- *Download the Data Protection Manager Software*
- *Download Pillar Axiom Utility Software*
- *Set the Data Protection Manager Encryption Key*

Set the Data Protection Manager Encryption Key

You can set the Pillar Axiom Data Protection Manager (DPM) encryption key at any time during normal operations.

1 From the **Manager** menu, click **Update Encryption Key**.

2 From the Update Encryption Key dialog box, enter an encryption value of your choice, then click **Submit**.

Result:
DPM stores the key and uses it to encrypt sensitive data.

If you have replaced an existing encryption key, any secured data is re-encrypted using the updated key.

Related concepts

- *About Data Protection Manager Security*

Related tasks

- *Run Data Protection Manager for the First Time*

Modify Virtual Machine Credentials

Update the virtual machine login credentials for the Pillar Axiom Data Protection Manager (DPM) whenever changes are made to the virtual server login information or to the communications port.

When DPM starts from a virtual machine (VM) environment, the system verifies the login credentials to the VM server. If DPM cannot communicate with the VM server, the Modify Virtual Machine Server Credentials dialog appears.

1. From the **Manager** menu, click **Modify Virtual Machine Server Credentials**.
2. From the Modify Virtual Machine Server Credentials, Step 1 of 2 dialog box, read the information provided, then click **Next**.
3. From the Modify Virtual Machine Server Credentials, Step 2 of 2 dialog box, enter the login credentials.

   Required credentials:

   - IP address
   - Port number
   - User name
   - Password
4. To save the information, click **Submit**.

   Result:
   DPM verifies the login credentials and, if accepted, closes the dialog. If a problem exists, the dialog box appears again prompting you for the correct information.

   Note: Contact your system administrator if you are having difficulties modifying the virtual machine server credentials.

Related concepts

- *About the DPM Virtual Environment*

Related references

- *Virtual Machine Requirements*
- *Modify Virtual Machine Server Credentials Dialog (Step 1)*
- *Modify Virtual Machine Server Credentials Dialog (Step 2)*

About Accessing the Data Protection Manager

You can run Pillar Axiom Data Protection Manager (DPM) from a graphical user interface (GUI) or command line interface (CLI).

The DPM GUI and CLI are independent programs. Using one interface does not depend on the other to accomplish a task. All of the DPM features are available in both programs.

The CLI allows you to automate commands using programs such as Python, Perl, and standard shell scripting commands.

You might experience a delayed response when performing actions on the CLI and the results appearing in the GUI. For example, if you create a schedule using the CLI, that schedule may not immediately appear in the GUI. We recommend that you restart the GUI DPM application to display any objects created by the CLI.

Related concepts

- *About Data Protection Manager Software*
- *About the Axiom DPM CLI*

Related tasks

- *Run Data Protection Manager GUI*

About the Axiom DPM CLI

The Pillar Axiom Data Protection Manager (DPM) provides a command-line interface called the *axiomdpmcli*. The axiomdpmcli allows you to configure and manage DPM functions on the command line or through custom scripts.

Below are listed some of the characteristics of the DPM CLI:

- Installs with the DPM product and provides the same capabilities as the DPM graphical user interface (GUI)
- Runs as a command-line interface from a console window
- Communicates from the host system to the Pillar Axiom DPM
- Uses familiar conventions for parameters and options, and provides reasonable default values where possible
- Checks for required sets of parameters and displays error messages if the required values are missing

- Returns error messages that are detected by the DPM host agent and passed through to the CLI
- Supports automation through custom scripts that use Perl, Python, and standard shell commands
- Provides help for each of its commands
- Displays data output in an XML format

The DPM CLI provides limited data input validation. The CLI sends commands in packages to the DPM server where the commands are processed. CLI input has the following limitations:

- Object identifiers are not validated. Ensure that you enter the correct values for commands that require an object ID or name, such as a consistency group or checkpoint identifier, or schedule description. The CLI does not validate whether the object exists or that the object information is correct.
- Command parameters are not validated. For example, if a command requires input for a host IP address, the CLI does not validate that the input follows a specific form or pattern.

Use the `event -list` CLI command to view the status of your processed commands.

Related concepts

- *About Data Protection Manager Software*

Related tasks

- *Issue an axiomdpmcli Command for Windows*
- *Issue an axiomdpmcli Command for Solaris and Linux*

Run Data Protection Manager GUI

After you have set the encryption key and default environment, you can run the Pillar Axiom Data Protection Manager GUI without interruption.

1. Log in to the computer where DPM is installed.
2. Launch the DPM application.
   - For Windows, choose **Start** > **All Programs** > **Oracle Corporation** > **Pillar Axiom Data Protection Manager** > **Pillar Axiom Data Protection Manager**.
   - For Linux, choose **Applications** > **System Tools** > **Pillar Axiom Data Protection Manager**.

- For Solaris, choose **Applications** > **Utilities** > **Pillar Axiom Data Protection Manager**.

The Data Protection Manager GUI opens the Axioms overview page, or the page you visited when you last logged off.

Related concepts

- *About Data Protection Manager Software*

Related tasks

- *Download the Data Protection Manager Software*
- *Download Pillar Axiom Utility Software*
- *Install Data Protection Manager for Windows*
- *Install Data Protection Manager for Linux*
- *Install Data Protection Manager for Solaris*

About Configuring Pillar Axiom Access

To create and manage checkpoints, you must grant permission to the Pillar Axiom Data Protection Manager (DPM) so it can access the Pillar Axiom system.

Data Protection Manager lists each Pillar Axiom system that is accessible from the host. Initially, DPM displays the Pillar Axiom status as Connected, but the system is not accessible to manage checkpoints.

To view the applications and consistency groups, and to manage and create checkpoints on the system, you must provide the login credentials to the Pillar Axiom system and enable DPM access to that system. The login name and password you supply are the administrative credentials that Data Protection Manager uses to access the Pillar Axiom system. You can set the Enable Axiom Access option and enter the Axiom credentials from the Configure Axiom Access option. Setting the Axiom access option allows you to view applications and consistency group LUNs on the Pillar Axiom system.

The Clear Axiom Access option removes the login credentials to the Pillar Axiom system. Clearing the login credentials causes DPM to lose visibility to the applications and consistency group LUNs that reside on the Pillar Axiom system. Reinstate the credentials by using the Configure Axiom Access option.

Related references

- *Configure Axiom Access Page*
- *Axioms Overview Page*

Related tasks

- *Configure Pillar Axiom Access*
- *Clear Pillar Axiom Access*
- *Refresh the List of Pillar Axiom Systems*

Configure Pillar Axiom Access

Configure Pillar Axiom access by specifying a login name and password that Data Protection Manager (DPM) can use to log in to the Pillar Axiom system.

Prerequisite: A unique Pillar Axiom system username, with an Administrator 1 role, that is used for DPM purposes.

1 From the DPM left navigation pane, click Axioms.

2 From the Pillar Axiom Systems overview page, select the name of a Pillar Axiom system to access.

3 Choose **Actions** > **Configure Axiom Access**.

4 To enable DPM access to the Pillar Axiom system, select the **Axiom Access Enabled** option.

Note: Enabling Axiom Access allows you to view applications and consistency group LUNs on the Pillar Axiom system.

5 Enter the **Login name** for accessing the Pillar Axiom system.

6 Enter the **Password** for accessing the Pillar Axiom system.

7 To save the settings, click **OK**.

Related concepts

- *About Configuring Pillar Axiom Access*

Related references

- *Configure Axiom Access Page*
- *Axioms Overview Page*

Related tasks

- *Clear Pillar Axiom Access*
- *Refresh the List of Pillar Axiom Systems*

Clear Pillar Axiom Access

You can remove the Pillar Axiom system login credentials that the Pillar Axiom Data Protection Manager (DPM) uses.

1 From the DPM left navigation pane, click **Axioms**.

2 From the Pillar Axiom Systems overview page, select the name of a Pillar Axiom system.

3 Choose **Actions** > **Clear Axiom Access**.

4 Click **OK**.

Related concepts

- *About Configuring Pillar Axiom Access*

Related references

- *Configure Axiom Access Page*
- *Axioms Overview Page*

Related tasks

- *Configure Pillar Axiom Access*
- *Refresh the List of Pillar Axiom Systems*

Refresh the List of Pillar Axiom Systems

You can update the list of Pillar Axiom systems that are connected to the Pillar Axiom Data Protection Manager (DPM).

When DPM starts, the program automatically updates the list of available Pillar Axiom systems and adds newly discovered systems to the list. Use this option to manually update the list of systems.

1. From the DPM GUI, choose Manager > Refresh Axioms.
2. Click OK.

   Result:
   A list of connected Pillar Axiom systems appears on the page.

Related concepts

- *About Configuring Pillar Axiom Access*

Related references

- *Configure Axiom Access Page*
- *Axioms Overview Page*

Related tasks

- *Configure Pillar Axiom Access*
- *Clear Pillar Axiom Access*

Chapter 3

Manage Checkpoints

About Application Consistency Groups

When you log into Pillar Axiom Data Protection Manager (DPM) that has access to the connected Pillar Axiom systems, DPM discovers all supported application instances. These applications and associated consistency groups appear on the Applications overview page.

Consistency groups are the smallest unit of application data that can represent an application instance. Consistency groups contain all the relevant raw data that is necessary to define the application instance. The raw data would include any additional metadata that the application uses. Backups are made at the consistency group level to ensure that all relevant data is included in each backup.

Data Protection Manager recognizes the following application data as consistency groups:

- Microsoft Exchange Server storage groups
- Microsoft SQL Server database instances
- Oracle database instances
- Oracle Automatic Storage management (ASM) disk groups

For DPM to back up and restore application data, the data of the consistency groups must be consistent. Consistency means that the LUNs where the data is stored must be configured correctly.

Related references

- *Axioms Overview Page*
- *Oracle Database Requirements*
- *Oracle Automatic Storage Management Requirements*
- *Applications Overview Page*
- *View Consistency Group, Oracle Databases Tab*
- *Restore Checkpoint Dialog*

Related tasks

- *View Consistency Group Details*
- *Refresh the List of Pillar Axiom Systems*
- *Set the Oracle Username*
- *Set the ASM Username*
- *Restore a Checkpoint*

LUN Configuration for Data Consistency

Configuring the LUNs of your application consistency groups according to established best practices ensures data consistency.

Correctly configuring the LUNs for the application consistency groups allows the Pillar Axiom Data Protection Manager (DPM) to create checkpoints without error. The applications you configure might include:

- Microsoft Exchange
- Microsoft SQL
- Oracle databases

A consistency group represents the set of data LUNs for back up. DPM can track, manage, and restore the LUNs provided that the data is consistent. Data consistency means that consistency groups contain LUNs that are configured according to the following specifications:

- Place all of the application data LUNs on a Pillar Axiom system. DPM does not back up or restore applications that use LUNs from different manufacturers of data storage systems.
- Configure all of the application consistency group LUNs on a single Pillar Axiom system.
- Ensure that each LUN of the consistency group is not used by other consistency groups.

DPM checks for consistency and displays the status on the Applications overview page. Any error indicates that the LUNs were not configured properly.

Related tasks

- *Verify a Consistency Group*

View Consistency Group Details

You can review the details of a selected consistency group. For example, if the consistency group status is `Unsupported LUNs`, you can view the LUNs that the consistency group is using.

1 From the left navigation pane, click **Applications**.

2 From the Applications overview page, select a consistency group from the list.

3 Choose **Actions** > **View Consistency Group**.

4 From the View Consistency Group dialog, click the available tabs to review the consistency group details.

5 When finished, click **OK**.

Related references

- *View Consistency Group, Consistency Group Tab*
- *View Consistency Group, LUNs Tab*
- *View Consistency Group, Retention Policy Tab*
- *View Consistency Group, Schedules Tab*
- *View Consistency Group, Oracle Databases Tab*
- *Best Practice Resources*

Verify a Consistency Group

You can confirm that the LUNs of a selected consistency group are consistent and ready for back up.

Perform this task on consistency groups that have a `Not Verified` state.

1 From the left navigation pane, click **Applications**.

2 From the Applications page, select a consistency group that has the status `Not Verified`.

3 Choose **Actions** > **Modify Consistency Group** > **Verify Consistency Group**.

   Result:
   A list of source LUNs appears.

4 Review the information on the dialog and then click **OK**.

The verification is successful when the consistency group status changes to `Optimal`.

Related concepts

- *About Application Consistency Groups*

Related references

- *Applications Overview Page*
- *Verify Consistency Group Dialog*
- *LUN Configuration for Data Consistency*

Related tasks

- *Refresh Applications*
- *Hide a Consistency Group*
- *Set the Oracle Username*

Hide a Consistency Group

You can hide a consistency group to prevent it from being managed by Pillar Axiom Data Protection Manager (DPM). Hiding the consistency group removes it from the Applications overview page.

1 From the left navigation pane, click **Applications**.

2 From the Applications page, select a consistency group from the list.

3 Choose **Actions** > **Modify Consistency Group** > **Hide Consistency Group**.

4 To remove the consistency group from the list and to prevent it from being managed by DPM, click **OK**.

The consistency group remains hidden even after you restart DPM. To show the consistency group again, refresh the applications list.

Related concepts

- *About Application Consistency Groups*

Related references

- *Applications Overview Page*

Related tasks

- *Refresh Applications*

Set the Oracle Username

Set the Oracle username to allow Pillar Axiom Data Protection Manager (DPM) to access the database source LUNs.

Prerequisite: The consistency group status is one of the following:

- ○ `Username required`
- ○ `Set Oracle Username`
- ○ `Invalid Username`

The database login is only applicable for Solaris and Linux OSs.

1. From the left navigation pane, click **Applications**.
2. From the Applications page, select the consistency group that requires a username.
3. Choose **Actions** > **Manage Consistency Group** > **Set Oracle Username**.

   Result:
   A dialog appears that prompts you for the username.
4. Enter the username, and then click **OK**.

The system verifies the database username and refreshes the application overview page.

Related concepts

- *About Application Consistency Groups*

Related references

- *Oracle Database Requirements*
- *Oracle Automatic Storage Management Requirements*
- *Applications Overview Page*
- *View Consistency Group, Oracle Databases Tab*

Set the ASM Username

When you set the Automatic Storage Management (ASM) username, you are setting the username to be used for querying information about the ASM instance.

Prerequisite:	The consistency group or application status is the following: `ASM Credentials Required`

The database login is only applicable for Solaris and Linux OSs.

If ASM is managing more than one Oracle database, Pillar Axiom Data Protection Manager (DPM) prompts you for a username for each managed database.

1. From the left navigation pane, click **Applications**.
2. From the Applications page, select an application group that requires a username.
3. Choose **Actions** > **Set ASM Username**.

   Result:
   A dialog appears that prompts you for the username.
4. Enter the username, and then click **OK**.

The system verifies the username and refreshes the application overview page.

Related concepts

- *About Application Consistency Groups*

Related references

- *Oracle Database Requirements*
- *Oracle Automatic Storage Management Requirements*
- *Applications Overview Page*
- *View Consistency Group, Oracle Databases Tab*

Refresh Applications

Refresh the applications to manually update the list of application consistency groups that are displayed on the Applications overview page. For example, refresh the applications after you have corrected an `Unsupported LUNs` status.

When you launch Pillar Axiom Data Protection Manager (DPM), the Applications content page displays supported applications and associated application consistency groups. While DPM is running, it will not discover any newly added applications until you refresh the applications.

1. From the DPM left navigation pane, click **Applications**.
2. Choose **Actions** > **Refresh Applications**.
3. Click **OK**.

Related concepts

- *About Application Consistency Groups*

Related references

- *Best Practice Resources*
- *Applications Overview Page*
- *Best Practice Resources*
- *Applications Overview Page*
- *Microsoft Sharepoint Database Requirements*

Related tasks

- *Verify a Consistency Group*
- *Hide a Consistency Group*

About Checkpoints

Checkpoints represent a consistent point-in-time image of all the LUNs that comprise the consistency group that was backed up.

Creating a checkpoint instructs Pillar Axiom Data Protection Manager to create Clone LUNs of the specified consistency groups, ensuring that normal operation of the application is affected as little as possible.

Before creating a checkpoint, you must first select either an application or a consistency group.

- If you select an application, DPM creates a series of checkpoints, one for each consistency group in the application. Creating a series of checkpoints on multiple consistency groups is asynchronous, which means that the DPM creates a checkpoint before creating the next one.
- If you select a single consistency group, you create a checkpoint for only the selected consistency group.

Checkpoints can be created on the Applications overview page, and they can be modified or deleted on the Checkpoints overview page. Checkpoints created on the Applications overview page are displayed on the Checkpoints overview page.

The status of the latest checkpoint that was created for any consistency group is displayed on the Applications page. The description and time of creation of each completed checkpoint are listed on the Checkpoints overview page.

You can also have DPM create checkpoints on a regular basis as defined by a scheduled job. You can schedule checkpoints to be created hourly, daily, or weekly.

When you are creating a large number of checkpoints, we recommend that you set a retention policy that deletes older checkpoints. You can set a retention policy based on the checkpoint age (which is measured in a specific number of days with a 30 day maximum) or on a specified quantity with a maximum of 30 checkpoints to keep. You can also apply a combination of both criteria.

Related concepts

- *About Checkpoint Schedules*
- *About Checkpoint Retention Policy*

Related references

- *Restore Checkpoint Dialog*

Related tasks

- *Restore a Checkpoint*

Create an Immediate Checkpoint

You can create a checkpoint for a consistency group or an application. You can create an immediate checkpoint to back up an application or consistency group.

1. From the left navigation pane, click **Applications**.
2. From the Applications page, select the checkpoint source.

   Valid sources:

   - An application
   - An application consistency group
3. Choose **Actions** > **Plan Checkpoint**.
4. (Optional) If you want the checkpoint to override the default consistency group retention policy, select **Permanent**.
5. (Optional: *Applies to MS Exchange applications only*) If you want to verify the checkpoint data when creating the checkpoint, select **Run Exchange Backup Verification**.

   Note: You cannot schedule this option.
6. To create the checkpoint immediately, click **OK**.

After you click **OK**, the system creates checkpoints for the selected application or application consistency group. You can monitor the checkpoint progress from the Checkpoints overview page.

Related concepts

- *About Checkpoints*
- *About Transportable Checkpoints*

Related references

- *Checkpoints Overview Page*
- *Applications Overview Page*

View Checkpoint Details

You can review information about a checkpoint, such as the Clone LUNs that are used for the checkpoint.

1. From the left navigation pane, click **Checkpoints**.

2 From the Checkpoints page, select a checkpoint from the list.

3 Choose **Actions** > **View Checkpoint**.

4 Click the Clone LUNs tab.

Result:
A list of Clone LUNs created for the checkpoint appears.

Related concepts

- *About Checkpoints*

Related references

- *View Checkpoint, Checkpoint Tab*
- *View Checkpoint, Clone LUNs Tab*

Modify a Checkpoint Description

You can modify the Checkpoint description as necessary. For example, you might want to describe a permanent checkpoint to include the application source.

1 From the left navigation pane, click **Checkpoints**.

2 Select a checkpoint from the list.

3 Choose **Actions** > **Modify Checkpoint**.

4 Enter a new description in the **Description** field.

5 To save the change, click **OK**.

Related concepts

- *About Checkpoints*
- *About Checkpoint Retention Policy*

Related references

- *Modify Checkpoint Dialog*

Delete Checkpoints

Deleting a checkpoint removes the checkpoint Clone LUNs from the Pillar Axiom system.

Note: If you want to delete checkpoints on a regular basis, use the **Set Retention Policy** option that is available from the Applications page.

1. From the left navigation pane, click **Checkpoints**.

2. In the Checkpoints list, select the checkpoint that you want to delete.

3. Choose **Actions** > **Delete Checkpoint**.

   Result:
   The Delete dialog appears prompting you to confirm the deletion of the checkpoint.

4. When prompted to delete the checkpoint, click **Yes**.

   Result:
   The Pillar Axiom system removes the Clone LUNs that are associated with the checkpoint.

Related concepts

- *About Checkpoint Retention Policy*

Related references

- *Set Retention Policy Dialog*

About Transportable Checkpoints

When creating an immediate or scheduled checkpoint, you can set an option that makes the checkpoint *transportable*. A transportable checkpoint is defined in a Microsoft Volume Shadow Copy Service (VSS) XML document that contains Clone LUN information about the checkpoint. The VSS terminology for Clone LUN is *snapshot*. You can create transportable checkpoints for Microsoft Exchange and Microsoft SQL databases.

You store the document file on your local workstation. Therefore, the file is not known to the Pillar Axiom Data Protection Manager (DPM). Because DPM is not aware of this document, DPM cannot maintain or display the document.

Transportable checkpoints can be imported into the original host or to a different host that is connected to the Pillar Axiom system. You can import the Clone LUNs of a transportable checkpoint to a host if that host is connected to the Pillar Axiom system from which you created the checkpoint. After a Clone LUN is imported, it becomes a LUN that is not managed by DPM.

The transportable checkpoint XML document is dependant on the OS and system architecture of the host on which the document is placed. When importing transportable checkpoints, ensure that the originating OS and architecture is compatible to the target host to which you are importing.

- Transportable checkpoints that are created on a Windows 2003 server with 32-bit or 64-bit architecture can be imported on a target host of the same OS and architecture.
- Transportable checkpoints that are created on a Windows 2008 server with 32-bit or 64-bit architecture can be imported on a target host of the same OS of any architecture.

Note: Refer to the Microsoft Developer Network article about VSS Application Compatibility (http://msdn.microsoft.com/en-us/library/aa384627(VS.85).aspx).

When importing a transportable checkpoint, you have the option to mount the Clone LUNs (called *snapshots within the DPM interface*) during the import process or later after the checkpoint XML file has been imported. When you mount the Clone LUNs at the time of import, you can mount the volumes to their original location or map them to a new location. In both cases, imported checkpoints are not seen or managed by DPM. If you choose not to map the Clone LUNs during the import process, you can map them later using Windows disk management tools.

Note: When mounting checkpoints on Windows systems, mount to a mapped drive, not a mount folder.

You can use a transportable checkpoint for diagnostic purposes. For example, to test the integrity of your Microsoft SQL database, create a checkpoint of the Microsoft SQL application and import the checkpoint XML file to another host that manages the same Pillar Axiom system. Then, map the restored volume to a drive location on the host and examine the contents or test its integrity.

During the transportable checkpoint creation process, you have the option of specifying the prefix portion of the filename for the transportable checkpoint. For example, you might want to easily identify the database application checkpoints from your San Francisco financial office. To make these checkpoints easier to identify and retrieve, you can add the prefix *sf_finance* to your transportable checkpoints.

Related references

- *Import Transportable Checkpoint, Import Checkpoint Dialog*
- *Import Transportable Checkpoint, Mount Snapshot Dialog*

Related tasks

- *Create a Transportable Checkpoint*
- *Import a Transportable Checkpoint*

Create a Transportable Checkpoint

You can create a transportable checkpoint for a consistency group or an application. Transportable checkpoints are XML documents that contain checkpoint information. You store the file on your location workstation and therefore are not seen or managed by Pillar Axiom Data Protection Manager.

1 From the left navigation pane, click **Applications**.

2 From the Applications page, select the checkpoint source.

Valid sources:

- An application
- An application consistency group

3 Choose **Actions** > **Plan Checkpoint**.

4 To create a transportable checkpoint, select **Transportable Checkpoint**.

5 If you selected the Transportable Checkpoint option, provide the local **Directory** where you want the checkpoints to be created.

Note: Use local drive paths only. Mapped network drives are not supported.

6 (Optional) In the **Prefix** field, enter the text prefix for the transportable checkpoint.

7. To create the checkpoint immediately, click **OK**.

After you click **OK**, the system creates checkpoints from the selected application or application consistency group. The transportable checkpoint files are available in the directory you specified.

Related concepts

- *About Transportable Checkpoints*
- *About Checkpoints*

Related references

- *Import Transportable Checkpoint, Import Checkpoint Dialog*
- *Import Transportable Checkpoint, Mount Snapshot Dialog*

Import a Transportable Checkpoint

Import a transportable checkpoint when you need to analyze the data from your application.

You can import transportable checkpoints that were created on the current host or from another Data Protection Manager host.

1. From the **Manager** menu, click **Import Transportable Checkpoint.**
2. To select the checkpoint file from the workstation, click the browse button [...].
3. Navigate to and select the transportable checkpoint file.
4. To select the file, click **Open.**
5. From the Import Transportable Checkpoint dialog, click **Next.**
6. (Optional) Select **Mount Snapshots.**

   Note: You can mount the snapshot at a later time using a Windows disk management tool.

   Result:
   The dialog adds fields to map each LUN to a drive letter.
7. Enter the drive letters in the spaces provided.
8. To map the LUNs to their respective drive letters, click **Finish.**

Related concepts

- *About Transportable Checkpoints*
- *About Checkpoints*

Related references

- *Import Transportable Checkpoint, Import Checkpoint Dialog*
- *Import Transportable Checkpoint, Mount Snapshot Dialog*

About Restoring Checkpoints

Restoring from a checkpoint reverts a consistency group to a particular point-in-time. The restore process uses the Clone LUNs on the Pillar Axiom system to restore the LUNs. For more information about restoring a LUN from a Clone LUN, refer to the *Pillar Axiom Administrator's Guide*.

During the restore process, the consistency group is taken offline while the source LUNs are synchronized to the checkpoint LUNs on the Pillar Axiom system. For Windows-based systems, Microsoft Volume Shadow Copy Service (VSS) manages the consistency group during checkpoint restore process. When the background copy begins, the consistency group is brought back online and, if necessary, the restored data is verified.

Related references

- *Restore Checkpoint Dialog*

Related tasks

- *Restore a Checkpoint*

Restore a Checkpoint

You can restore the Clone LUNs of a checkpoint to the state of its point-in-time backup.

Prerequisite The checkpoint status should read `Ready to Restore`.

1 From the left navigation pane, click **Checkpoints**.

2 Select a checkpoint from the list.

3 Choose **Actions** > **Restore**.

4 To restore the checkpoint, click **OK**.

Result:

The system reverts the Clone LUNs to their state when the checkpoint was created.

Related concepts

- *About Restoring Checkpoints*

Related references

- *Restore Checkpoint Dialog*

About Checkpoint Retention Policy

A retention policy specifies which checkpoints to keep on the system. You can specify the maximum number of checkpoints to keep, the age of checkpoints, or a combination of the two. You apply the policy to an application consistency group. By applying a retention policy you ensure that all checkpoints that are created for the consistency group are governed by the same retention policy.

You have three options for setting a retention policy:

- By the number days to keep the checkpoints. The system saves checkpoints for up to 30 days.
- By the number of checkpoints to keep. You can save up to 30 checkpoints.
- A combination of the above two options. When both options are enabled, the threshold that is crossed first results in that limit being applied. For example, if you set the number of days to keep to 7 and the number of checkpoints to keep to 10, the system will not keep more than 10 checkpoints in a seven day period.

You can override the retention policy by marking a checkpoint *permanent*. Use the permanent option when planning an immediate or scheduled checkpoint. While the permanent option can be used when you plan a scheduled checkpoint, choosing that option results in the system setting all of the checkpoints that are created by that schedule to permanent. Only individual checkpoints should be set to permanent to avoid stressing available resources.

Note: Checkpoints consume Clone LUN storage on the Pillar Axiom system. Refer to the *Pillar Axiom Administrator's Guide* for managing the Clone LUNs.

You can monitor the checkpoint removal activity from the Events overview page. Permanent checkpoints cannot be deleted by the system by means of a retention policy. You must delete permanent checkpoints manually.

Related concepts

- *About Checkpoint Schedules*
- *About Checkpoints*

Related references

- *Checkpoints Overview Page*
- *Applications Overview Page*
- *Set Retention Policy Dialog*

Related tasks

- *Create an Immediate Checkpoint*
- *Plan a Checkpoint Schedule*
- *Set a Checkpoint Retention Policy*
- *Make a Checkpoint Permanent*
- *Delete Checkpoints*

Set a Checkpoint Retention Policy

You can set the retention policy for any consistency group. The policy specifies to Pillar Axiom Data Protection Manager when to purge the checkpoints that are created by the consistency group. Set the policy in terms of the maximum number of checkpoints, the maximum number of days to keep older checkpoints, or both.

1. From the left navigation pane, click Applications.
2. Select a consistency group from the list.
3. Choose Actions > Modify Consistency Group > Set Retention Policy.
4. (Optional) To set the retention policy for the maximum number of checkpoints to keep, select the Enabled option for Maximum Checkpoints Retention Policy, and then select a number in the drop-down list.
5. (Optional) To set the retention policy for the maximum number of days to keep the checkpoints, select the Enabled option for Maximum Duration Retention Policy. and then select a number in the drop-down list.
6. To save the retention policy settings, click OK.

The checkpoint retention policy applies to all checkpoints that are associated with the consistency group.

Related concepts

- *About Checkpoint Retention Policy*

Related references

- *Set Retention Policy Dialog*

Make a Checkpoint Permanent

You can make a checkpoint permanent, which overrides an active retention policy.

1 From the left navigation pane, click **Checkpoints**.

2 Select a checkpoint from the list.

3 Choose **Actions** > **Modify Checkpoint**.

4 Select the **Permanent** option.

5 To save the change, click **OK**.

Related concepts

- *About Checkpoint Retention Policy*

Related references

- *Set Retention Policy Dialog*

CHAPTER 4

Manage Checkpoint Schedules

About Checkpoint Schedules

A checkpoint schedule creates checkpoints on a regular basis. You can control the automatic checkpoint activity by using the following scheduling parameters:

- The date and time that the automatic checkpoints starts
- The recurrence for when the automatic checkpoints operates
- The frequency at which the automatic checkpoints operates

When planning your checkpoint schedules, consider the following:

- Allow sufficient time intervals between scheduled checkpoints. Creating checkpoints requires system resources on the Pillar Axiom system and the host on which the database application is running. A scheduled checkpoint cannot start until a previously scheduled checkpoint is completed.
- The request for checkpoint creation is placed in a queue. No options are available for scheduling priority. The lack of checkpoint priority means that an immediate checkpoint might delay your scheduled checkpoints.
- You cannot set the verification option on a scheduled Microsoft Exchange checkpoint. The verification applies to immediate checkpoint creation.
- Use a retention policy to purge older checkpoints from the system.
- Select the permanent option when you want to keep a checkpoint beyond the retention policy setting. The permanent option overrides the retention policy placed on the application consistency group.

Related concepts

- *About Checkpoints*
- *About Checkpoint Retention Policy*

Related references

- *Schedules Overview Page*
- *Plan Checkpoint, Checkpoint Tab*
- *Plan Checkpoint, Schedule Tab*
- *View Checkpoint Schedule Dialog*
- *Modify Checkpoint Schedule Dialog*

Related tasks

- *Plan a Checkpoint Schedule*
- *Display All Checkpoint Schedules*
- *Delete a Checkpoint Schedule*
- *View a Checkpoint Schedule*
- *Modify a Checkpoint Schedule*
- *Refresh All Checkpoint Schedules*

Plan a Checkpoint Schedule

You can create a schedule that creates checkpoints at regular intervals.

You can create checkpoints for each consistency group within an application or for a selected application.

1. From the left navigation pane, click **Applications**.
2. From the Applications page, select the checkpoint source.

   Valid sources:

   - An application
   - An application consistency group
3. Choose **Actions** > **Plan Checkpoint**.
4. (Optional) To create a transportable checkpoint, select **Transportable Checkpoint**.
5. From the Schedule tab, click **Create Schedule**.
6. In the **Schedule Name** field, enter the checkpoint schedule name.
7. To activate the schedule, select **Enabled**.

   If you do not enable your schedule now, you can enable it later by modifying the schedule.
8. Click the **Browse** button to the right of **Start Time** to select the day and time for your schedule to start.

   To select the date and time, use the controls in the **Modify Date/Time** dialog.

   Note: Schedule your checkpoint start time to no more than three weeks in the future.
9. To close the calendar dialog, click **OK**.
10. Select a frequency for your schedule.

    Valid frequencies include:

    - Hourly
    - Daily
    - Weekly
11. Choose a recurrence value for your schedule.

If you chose a frequency of Weekly, choose the day or days of the week on which you would like your checkpoint to be generated.

12 To save the schedule, click OK.

Result:
Your schedule is listed on the Schedules overview page.

Related concepts

- *About Checkpoints*
- *About Transportable Checkpoints*
- *About Checkpoint Schedules*

Related references

- *Checkpoints Overview Page*
- *Applications Overview Page*
- *Schedules Overview Page*
- *Plan Checkpoint, Checkpoint Tab*
- *Plan Checkpoint, Schedule Tab*

Related tasks

- *Display All Checkpoint Schedules*
- *Delete a Checkpoint Schedule*

Modify a Checkpoint Schedule

You can revise a checkpoint schedule when your requirements change.

1. From the left navigation pane, click **Schedules**.
2. Select a checkpoint schedule from the list.
3. Choose **Actions** > **Modify Schedule**.
4. (Optional) From the Modify Checkpoint Schedule dialog, enter a new name in the **Schedule Name** field.
5. (Optional) To enable or disable the checkpoint schedule, select the **Enabled** option.

   You can disable the schedule to stop checkpoint operations temporarily.
6. (Optional) To select a revised day and time for your schedule to start, click the **Browse** button to the right of **Start Time**.

   To close the Start Time dialog, click **OK**.
7. (Optional) Choose a new frequency for your schedule.
8. (Optional) Choose a **Recurrence** value for your schedule.
9. (Optional) If you want the checkpoint to override the default consistency group retention policy, select **Permanent**.
10. To save the schedule, click **OK**.

Related concepts

- *About Checkpoint Schedules*

Related references

- *Modify Checkpoint Schedule Dialog*

View a Checkpoint Schedule

You can review a checkpoint schedule. For example, you might want to know if the schedule will interrupt other scheduled checkpoint creation or affect an immediate checkpoint you are creating.

1. From the left navigation pane, click **Schedules**.
2. Select a checkpoint schedule from the list.
3. Choose **Actions** > **View Schedule**.
4. Review the displayed information to ensure that the schedule details are what you expect.
5. When you are finished reviewing the schedule, click **Close**.

Related concepts

- *About Checkpoint Schedules*

Related references

- *View Checkpoint Schedule Dialog*

Refresh All Checkpoint Schedules

You can manually refresh the list of available checkpoint schedules that are running on the Pillar Axiom Data Protection Manager.

1. From the left navigation pane, click **Schedules**.
2. Choose **Action** > **Refresh Schedules**.

   Result:
   The system updates the list of available schedules and provides the latest status.

Related concepts

- *About Checkpoint Schedules*

Related references

- *Modify Checkpoint Schedule Dialog*

Delete a Checkpoint Schedule

You can delete a checkpoint schedule when your requirements change. After you delete the schedule, no future automatic checkpoints that are based on the schedule will occur.

1. From the left navigation pane, click **Schedules**.
2. Select a checkpoint schedule from the list.
3. Choose **Actions** > **Delete Schedule**.
4. When prompted to confirm the deletion, click **OK**.

Related concepts

- *About Checkpoint Schedules*

Related references

- *Schedules Overview Page*
- *Plan Checkpoint, Checkpoint Tab*
- *Plan Checkpoint, Schedule Tab*

Related tasks

- *Plan a Checkpoint Schedule*
- *Display All Checkpoint Schedules*

Display All Checkpoint Schedules

You can view a list of checkpoint schedules for the Pillar Axiom Data Protection Manager. You can determine, for example, whether the schedule is enabled or the frequency of the schedule.

1. From the left navigation pane, click **Schedules**.
2. Review the schedule details to ensure that the information is what you expect.

Related concepts

- *About Checkpoint Schedules*

Related references

- *Schedules Overview Page*
- *Plan Checkpoint, Checkpoint Tab*
- *Plan Checkpoint, Schedule Tab*

Related tasks

- *Plan a Checkpoint Schedule*
- *Delete a Checkpoint Schedule*

CHAPTER 5

Manage DPM Events

About Data Protection Manager Events

Pillar Axiom Data Protection Manager (DPM) records in the event log significant events that are related to both the program and the OS. DPM does not log events for the Call-Home log bundles.

For Windows systems, DPM also records significant events, such as checkpoint failures, in the Windows events log.

Some of the logged DPM events include the following types of information:

- Checkpoint created or failed
- Checkpoint restored or deleted
- Checkpoint imported or failed
- Schedule created, modified, or deleted
- Configuring or clearing access to the Pillar Axiom system
- Setting retention policies
- Warnings and errors

You can view details about a selected event and, if desired, export the information to the workstation clipboard.

Related references

- *Events Overview Page*
- *View Event Properties Dialog*

Related tasks

- *Display All Events*
- *View Event Details*
- *Refresh the List of Events*

Display All Events

You can view a list of existing events. Events contain information about tasks that have been performed by the Pillar Axiom Data Protection Manager.

1. From the left navigation pane, click **Events**.
2. Review the event details to ensure that the information is what you expect.

Related concepts

- *About Data Protection Manager Events*

Related references

- *Events Overview Page*
- *View Event Properties Dialog*

Refresh the List of Events

Under normal conditions, the Pillar Axiom Data Protection Manager (DPM) keeps the event list up to date. You can update the list of events as required.

Note: Depending on the number of events that DPM must retrieve, refreshing the list of events might take several minutes to complete. DPM could retrieve up to 4032 events.

1 From the left navigation pane, click **Events**.

2 Choose **Actions** > **Refresh Events**.

3 Review the list of events to ensure that the information is what you expect.

Related concepts

- *About Data Protection Manager Events*

Related references

- *Events Overview Page*
- *View Event Properties Dialog*

View Event Details

You can view the details of an event and copy the information to your workstation clipboard.

1. From the left navigation pane, click **Events**.
2. Select the name of the event from the list.
3. Choose **Actions** > **View Event**.
4. Review the information about the event.
5. (Optional) To save the event information in the clipboard memory, click **Copy to Clipboard**.
6. When you are finished, click **OK**.

Related concepts

- *About Data Protection Manager Events*

Related references

- *Events Overview Page*
- *View Event Properties Dialog*

APPENDIX A

GUI Field Definitions

Applications Overview Page

Allows you to review the applications that are managed by the Pillar Axiom Data Protection Manager (DPM). The Applications overview page also provides status information about existing checkpoints. Options from this page allow you to create checkpoints and to modify and view consistency groups.

Name

Identifies the name of the application that is managed by the Data Protection Manager. Any application consistency groups that are associated with the application are also displayed.

Valid applications include:

- ○ Microsoft Exchange Server
- ○ Microsoft SQL Server
- ○ Oracle Database
- ○ Automatic Storage Management (ASM)

Consistency Status

Identifies the status of the consistency group or application. On Linux and Solaris systems, DPM requires an Oracle database login before database-specific information is displayed.

DPM cannot create immediate or scheduled checkpoints when an application or consistency group has a state other than `Optimal`.

Possible status:

ASM Credentials Required

Indicates that DPM requires an Oracle ASM login credential to display additional database information.

ASM Parameter File

Indicates that DPM has detected an ASM startup parameter file on the Oracle ASM disk group that is represented by the consistency group.

Axiom Access Required

Indicates that DPM requires the Pillar Axiom login credentials.

Consistency Status Unknown

Indicates that insufficient information is available to determine the consistency status. This status might be caused by the application being in an inoperable or otherwise unstable state.

Database Shutdown

Indicates that the connected database has been shut down.

Files Not in Consistency Group

Indicates that some files that are associated with the Oracle database, such as log or control files, are not stored on the same Oracle ASM disk group.

Invalid Username

Indicates that the supplied database username is invalid.

Multiple Applications

Indicates that the consistency group shares one or more LUNs with other consistency groups on the Pillar Axiom system. Sharing LUNs across consistency groups is not a DPM best practice for configuring applications on the system.

Multiple Axioms

Indicates that the consistency group uses LUNs from more than one Pillar Axiom system.

Non-Pillar LUNs

Indicates that the consistency group contains LUNs that do not reside on a Pillar Axiom system.

Not In Archivelog Mode

Indicates that an Oracle database is not set to `Archivelog` mode.

Not Verified

Indicates that the administrator has not verified that the discovered consistency group is correct.

Optimal

Indicates that no known issues exist with the consistency group.

Username Required

Indicates that the database requires authentication.

Checkpoint Status

Identifies the status of the checkpoint.

Possible status:

Creating

Indicates that DPM is currently creating a checkpoint.

Refreshing

Indicates that DPM is accessing current information about the checkpoint.

Deleting

Indicates that DPM is deleting the Clone LUNs of the checkpoint.

Restoring

Indicates that DPM is restoring the Clone LUNs that represent the checkpoint.

No checkpoints

Indicates that no checkpoint has been created for this consistency group.

Last Checkpoint

Indicates the date and time of the checkpoint completion. When the system does not contain any checkpoints, the status reads, `No checkpoints`.

Schedule Status

Identifies whether a checkpoint schedule applies to the application consistency group.

Possible status:

Scheduled

Indicates that the application consistency group is the source of at least one checkpoint schedule.

Unscheduled

Indicates that the application consistency group is not the source of any checkpoint schedule.

Retention Status

Indicates that a retention policy is set for the application consistency group.

Possible status:

Enabled

Indicates that all checkpoints created for the application consistency group are affected by a retention policy.

Disabled

Indicates that all checkpoints will be retained.

Related concepts

- *About Application Consistency Groups*
- *About Checkpoints*
- *About Transportable Checkpoints*

Related references

- *LUN Configuration for Data Consistency*
- *LUN Configuration for Applications*
- *Best Practice Resources*

Related tasks

- *Set the Oracle Username*
- *Create an Immediate Checkpoint*
- *Plan a Checkpoint Schedule*

Axioms Overview Page

Allows you to view the connection and access status for the Pillar Axiom systems that are visible and managed by the Pillar Axiom Data Protection Manager. Options on this page allow you to enable access and to provide the login credentials to the Pillar Axiom system.

Serial Number

Identifies the Pillar Axiom system serial number.

Connected

Indicates whether the Pillar Axiom system is physically connected to the host.

Axiom Access Enabled

Indicates whether the Pillar Axiom system is managed by the Data Protection Manager. To enable or disable access to the Pillar Axiom system, use the **Actions** menu. Access to the Pillar Axiom requires login credentials.

Login Name

Identifies the username that can be used to access and manage the Pillar Axiom system. This account must have Administrator 1 or Administrator 2 privileges to create and manage Clone LUNs. Refer to the *Pillar Axiom Administrator's Guide*.

Related concepts

- *About Configuring Pillar Axiom Access*
- *About Application Consistency Groups*

Related tasks

- *Configure Pillar Axiom Access*
- *Clear Pillar Axiom Access*
- *Refresh the List of Pillar Axiom Systems*
- *View Consistency Group Details*
- *Refresh the List of Pillar Axiom Systems*

Checkpoints Overview Page

Allows you to review checkpoints for a managed application. Options on this page allow you to manage and restore the checkpoints.

Timestamp

Identifies the time at which the checkpoint was completed.

Source

Identifies the name of the application consistency group from which the checkpoint was created.

Description

Identifies the description of the checkpoint.

Status

Identifies the status of the checkpoint.

Possible status:

Ready to Restore	The checkpoint is consistent and ready for restoration.
Deleting	DPM is currently deleting the checkpoint.
Restoring	DPM is currently restoring the checkpoint.
Not Restorable	DPM cannot restore the checkpoint. Verify the Consistency Group LUNs for consistency.

Permanent

Identifies whether the checkpoint overrides the retention policy.

Permanency values:

- ○ Yes
- ○ No

Related concepts

- *About Checkpoints*
- *About Transportable Checkpoints*

Related tasks

- *Create an Immediate Checkpoint*
- *Plan a Checkpoint Schedule*

Configure Axiom Access Page

Allows you to enter the Pillar Axiom login name and password and to enable the Pillar Axiom Data Protection Manager (DPM) to have access to the LUNs used by the managed applications.

Login Name

Identifies the username that can be used to access and manage the Pillar Axiom system. This account must have Administrator 1 or Administrator 2 privileges to create and manage Clone LUNs. Refer to the *Pillar Axiom Administrator's Guide*.

Password

Identifies the Pillar Axiom login password that is associated with the user account that was entered for Login Name. Passwords are case sensitive. Blank passwords are not permitted.

Axiom Access Enabled

Specifies whether to allow DPM to have access to the Pillar Axiom LUNs that are used by the managed applications.

Valid access options:

Enabled

Indicates that DPM has permission to access the Pillar Axiom system for any LUNs used by the applications and consistency groups.

The applications and consistency groups are displayed on the Applications overview page. When the applications and the consistency groups are visible, checkpoints can be created.

Disabled

Indicates that DPM does not have permission to access the Pillar Axiom system to correlate LUNs that may be used by applications and consistency groups. This may cause certain valid applications and consistency groups to not display in the Applications screen.

When the applications and application consistency groups are not visible, checkpoints cannot be created.

Related concepts

- *About Configuring Pillar Axiom Access*

Related tasks

- *Configure Pillar Axiom Access*
- *Clear Pillar Axiom Access*
- *Refresh the List of Pillar Axiom Systems*

Events Overview Page

Allows you to review entries in the Pillar Axiom Data Protection Manager event log. From this page you can view the details of a selected event or refresh the events list.

Note: DPM retains the last 4032 events.

Type

Displays the severity level of the entries in the Pillar Axiom event log.

Possible error types:

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.

Error

Reports that an operation has failed. Might require action to prevent subsequent failures of the same type.

Time

Specifies the date and time that the event occurred.

Generating Operation

Indicates the name of the operation, such as checkpoint creation, that generated the event notice.

Operation Status

Indicates the status of the operation that initiated the event.

Related concepts

- *About Data Protection Manager Events*

Related tasks

- *Display All Events*
- *View Event Details*
- *Refresh the List of Events*

Import Transportable Checkpoint, Import Checkpoint Dialog

Allows you to import a transportable checkpoint file. During the import process, you can optionally mount the checkpoint to a drive letter. After the checkpoint is mounted to a dedicated drive, you can use the checkpoint data for diagnostic purposes.

Backup Document

Specifies the name of the transportable XML document.

[...]

Opens a browse dialog box so that you can navigate to the XML document and select it for importing.

Related concepts

- *About Transportable Checkpoints*
- *About Checkpoints*

Related tasks

- *Create a Transportable Checkpoint*
- *Import a Transportable Checkpoint*

Import Transportable Checkpoint, Mount Snapshot Dialog

The second phase of importing a transportable checkpoint involves mounting the Clone LUNs of the checkpoint to the original drive or to a new drive.

Mount Snapshots

Specifies whether the imported Clone LUNs are mounted as a drive letter.

Valid options:

Enabled

Specifies that the imported Clone LUNs are to be mounted to a specific drive letter.

Note: After a Clone LUN is imported, it becomes a LUN that is not managed by DPM.

Selecting this option enables the mount point fields. The default information is the original drive and mapped drive letters that were used to create the Clone LUN. If you are restoring a checkpoint for diagnostic purposes on the source system, use a different drive letter.

Disabled

Specifies that the imported Clone LUNs are not to be mounted to a specific drive letter. After the checkpoint is imported, you can use a Windows disk management tool to mount the Clone LUN.

Related concepts

- *About Transportable Checkpoints*
- *About Checkpoints*

Related tasks

- *Create a Transportable Checkpoint*
- *Import a Transportable Checkpoint*

Modify Checkpoint Dialog

Allows you to change the description of the checkpoint and to set the checkpoint to permanent, which overrides the active retention policy.

Description

Identifies the user-supplied description for the checkpoint.

Permanent

Identifies whether the checkpoint overrides the retention policy.

Valid permanency values:

Enabled	Indicates that the checkpoint is not subject to the active retention policy.
Disabled	Indicates that the checkpoint is subject to the active retention policy.

Note: Permanent checkpoints cannot be deleted by the system by means of a retention policy. You must delete permanent checkpoints manually.

Related concepts

- *About Checkpoints*
- *About Checkpoint Retention Policy*

Related tasks

- *Modify a Checkpoint Description*
- *Make a Checkpoint Permanent*

Modify Checkpoint Schedule Dialog

Allows you to update the details of a selected checkpoint schedule.

Schedule Name

Identifies the name of the schedule.

Enabled

Specifies whether the schedule is enabled. Valid options:

Enabled

Indicates that the scheduled operation occurs at the specified time.

Disabled

Indicates that the operation will not occur as scheduled. You can disable the schedule, for example, to stop the schedule temporarily.

Start Time

Identifies the date and time at which the system starts a scheduled operation.

Identifies the frequency at which the system performs the scheduled operation.

Valid frequencies:

- Hourly
- Daily
- Weekly

Recurrence

Specifies how many hours, days, or weeks to wait before generating this scheduled operation again.

Valid values are listed in the following table.

Table 5 Schedule recurrence intervals

Recurrence interval	Valid values
Hourly	1 through 24
Daily	1 through 7

Table 5 Schedule recurrence intervals (continued)

Recurrence interval	Valid values
Weekly	1 though 52

Permanent

Identifies whether the checkpoint overrides the retention policy.

Related concepts

- *About Checkpoint Schedules*

Related tasks

- *Modify a Checkpoint Schedule*
- *Refresh All Checkpoint Schedules*

Modify Virtual Machine Server Credentials Dialog (Step 1)

Allows you to modify information about the virtual machine server credentials.

Modifying the virtual machine credentials requires two steps:

- Step one requests the information about the connection.
- Step two allows you to modify the existing information.

Related concepts

- *About the DPM Virtual Environment*

Related tasks

- *Modify Virtual Machine Credentials*

Modify Virtual Machine Server Credentials Dialog (Step 2)

Allows you to update the credentials for logging into the virtual machine (VM) server. Update this information when the IP address or port number of the virtual machine interface (VMI) have changed.

Note: Update the values on this dialog immediately after changing the VM server credentials. This dialog continues to display until the correct credentials are entered or the dialog is cancelled.

IP Address

Specifies the IP address of the host where the DPM VMI is installed.

Port

Specifies the communications port used by the DPM VMI.

Username

Specifies the user name that is authorized to access the vCenter server or Hyper-V server host.

Password

Specifies the user password for accessing the vCenter server or Hyper-V server host.

Related concepts

- *About the DPM Virtual Environment*

Related tasks

- *Modify Virtual Machine Credentials*

Plan Checkpoint, Checkpoint Tab

Allows you to create checkpoints on managed applications or consistency groups. You can create an immediate checkpoint or create a schedule that creates checkpoints on a regular basis.

Source

Identifies the checkpoint source, which is the application or application consistency group.

Description

Identifies the user-supplied description for the checkpoint.

Permanent

Identifies whether the checkpoint overrides the retention policy.

Valid permanency values:

Enabled

Indicates that the checkpoint is not subject to the active retention policy.

Disabled

Indicates that the checkpoint is subject to the active retention policy.

Transportable Checkpoint *(VSS-managed sources only)*

If the checkpoint is to be transportable, select the options, as necessary.

Note: The transportable checkpoint option only applies to Microsoft Volume Shadow Copy Service (VSS) sources.

Transportable Checkpoint

Indicates whether the checkpoint is transportable.

Valid options:

Enable

Enable transportable checkpoints when you want to save the checkpoint as an XML document to a location on the client. Transportable checkpoints are not visible to Data Protection Manager and therefore cannot be managed.

Disable

Disable transportable checkpoints when you want the checkpoint to be managed by the Data Protection Manager.

Prefix

Specifies the text that is appended to the beginning of the transportable checkpoint filename.

Directory

Allows you to select the folder in which to save the transportable checkpoint file.

Note: Use a local drive and directory only. Mapped network drives are not supported.

Browse [...]

Opens a browse dialog so that you can navigate to and select the file location.

Note: Select a local drive and directory only. Mapped network drives are not supported.

Run Exchange backup verification *(Microsoft Exchange Server source only)*

Indicates whether to verify the Exchange server data before completing the checkpoint. Selecting this option increases the time to create the checkpoint.

Note: You cannot perform the following actions on this option:

- ○ You cannot schedule this action. Selecting this option disables the Create Schedule option on the Schedule tab.
- ○ You cannot set this verify option with Transportable Checkpoint option.

Related concepts

- *About Checkpoint Schedules*

Related tasks

- *Plan a Checkpoint Schedule*
- *Display All Checkpoint Schedules*
- *Delete a Checkpoint Schedule*

Plan Checkpoint, Schedule Tab

Allows you to create a checkpoint schedule. You can create the schedule and not enable it, if desired. Pillar Axiom Data Protection Manager creates checkpoints when the schedule is enabled.

Create Schedule

Indicates that checkpoint creation is controlled by a schedule.

Note: Selecting **Create Schedule** enables the remaining options on the page.

Schedule

Specifies the criteria for the scheduled checkpoint.

Note: If you select the **Run Exchange Backup Verification** option from the Checkpoint tab, the **Create Schedule** option is not available.

Schedule Name

Identifies the unique name of a schedule.

Enabled

Specifies whether the schedule is enabled. Valid options:

Enabled	Indicates that the scheduled operation occurs at the specified time.
Disabled	Indicates that the operation will not occur as scheduled. You can disable the schedule, for example, to stop the schedule temporarily.

Start Time

Identifies the date and time at which the system starts a scheduled operation.

Schedule Frequency

Identifies the frequency at which the system performs the scheduled operation.

Valid frequencies:

- Hourly
- Daily
- Weekly

Recurrence

Identifies how often the system should perform the scheduled operation. Valid values vary based on the recurrence interval and frequency of the schedule.

Related concepts

- *About Checkpoint Schedules*

Related tasks

- *Plan a Checkpoint Schedule*
- *Display All Checkpoint Schedules*
- *Delete a Checkpoint Schedule*

Restore Checkpoint Dialog

Allows you to revert the consistency group source LUNs to the time when the checkpoint was taken. When you restore a checkpoint, the Checkpoint status on both the Application page and the Checkpoint page is displayed as `restoring`. When the system completes the checkpoint restoration, DPM updates the Events page.

Consistency Group

Indicates the name of the consistency group from which the checkpoint was created.

Checkpoint

Indicates the date and time that the checkpoint was created.

Related concepts

- *About Restoring Checkpoints*

Related tasks

- *Restore a Checkpoint*

Schedules Overview Page

Allows you to review a summary of the Pillar Axiom Data Protection Manager checkpoint schedules. You can review the schedule names, the date and time for the schedule to start, and the name of the source application. This page provides options to review and manage the checkpoint schedules.

Name

Identifies the name of the scheduled operation.

Enabled

Identifies whether the schedule is enabled.

Valid states:

Yes	Indicates that the schedule is active.
No	Indicates that the schedule is inactive.

Start Time

Identifies the time and date that Pillar Axiom Data Protection Manager is scheduled to start a scheduled job.

Next Run Time

Identifies the time and date of the next scheduled job.

Frequency

Specifies the frequency by which the scheduled operation runs.

Examples include:

- ○ Every 12 hours
- ○ Every 2 days
- ○ Every 4 weeks

Applies To

Identifies the name of the application or consistency group to which the schedule applies.

Related concepts

- *About Checkpoint Schedules*

Related tasks

- *Plan a Checkpoint Schedule*
- *Display All Checkpoint Schedules*
- *Delete a Checkpoint Schedule*

Set Retention Policy Dialog

Allows you to configure the retention policy for all checkpoints that are associated with the selected application consistency group.

Setting the retention policy affects all existing and new checkpoints of the selected consistency group. Your changes take effect the next time that the retention policy engine runs.

Maximum Checkpoints Retention Policy

Sets the retention policy to apply to a specific number of checkpoints.

Enabled

Specifies whether the maximum checkpoints retention policy is enabled. Possible states:

Enabled

Indicates that DPM retains the specified number of checkpoints.

Disabled

Indicates that all checkpoints are retained.

1 through 30

Indicates the number of checkpoints to keep.

Maximum Duration Retention Policy

Sets the retention policy to apply to a specific number of days.

Enabled

Specifies whether the maximum duration retention policy is enabled. Possible states:

Enabled

Indicates that DPM retains the checkpoints for a specified number of days.

Disabled

Indicates that all checkpoints are retained.

1 through 30

Indicates the number of days to keep the checkpoints.

Related concepts

- *About Checkpoint Retention Policy*

Related tasks

- *Set a Checkpoint Retention Policy*
- *Make a Checkpoint Permanent*
- *Delete Checkpoints*

Verify Consistency Group Dialog

Allows you to make the consistency group available to Pillar Axiom Data Protection Manager (DPM) for creating checkpoints and schedules. The dialog also allows you to view the LUN sources that are used for checkpoints and schedules.

LUN ID (LUID)

Displays the internal identifier of the LUN. This value is the same as the LUN identifier that is used on the Pillar Axiom system.

LUN Device Name

Identifies the LUN name that was assigned by the operating system.

View Checkpoint, Checkpoint Tab

Allows you to review the checkpoint properties, such as the associated consistency group and the checkpoint timestamp.

Consistency Group

Identifies the name of the application consistency group from which the checkpoint was created.

Timestamp

Identifies the time at which the checkpoint was completed.

Description

Identifies the description of the checkpoint.

Status

Identifies the status of the checkpoint.

Possible status:

Ready to Restore	The checkpoint is consistent and ready for restoration.
Deleting	DPM is currently deleting the checkpoint.
Restoring	DPM is currently restoring the checkpoint.
Not Restorable	DPM cannot restore the checkpoint. Verify the Consistency Group LUNs for consistency.

Permanent

Identifies whether the checkpoint overrides the retention policy.

Related concepts

- *About Checkpoints*

Related tasks

- *View Checkpoint Details*

View Checkpoint, Clone LUNs Tab

Use the View Checkpoint, Clone LUNs tab to review the Clone LUN details of the selected checkpoint. This page provides information about the source LUNs and Clone LUNs that are used to create the checkpoints.

Clone LUN ID (LUID)

Displays the internal identifier of the Clone LUN. This value is the same as the Clone LUN identifier that is used on the Pillar Axiom system.

Source LUN ID (LUID)

Displays the internal identifier of the source LUN that was used to create the Clone LUN. This value is the same as the LUN identifier that is used on the Pillar Axiom system.

Snapshot ID

Displays the identification number that was assigned to the LUN when the checkpoint was created.

Related concepts

- *About Checkpoints*

Related tasks

- *View Checkpoint Details*

View Checkpoint Schedule Dialog

Allows you to review the details of a selected checkpoint schedule.

Schedule Name

Identifies the name of the scheduled job.

Enabled

Indicates whether the consistency group schedule is enabled.

Start Time

Identifies the date and time at which the system starts a scheduled operation.

Specifies the frequency by which the scheduled operation runs.

Recurrence

Identifies the interval by which the scheduled job occurs.

Permanent

Identifies whether the checkpoint overrides the retention policy.

Transportable Checkpoint
(for transportable checkpoint schedules only)

Provides information about the creation of the transportable checkpoint, if selected.

Transportable Checkpoint

Indicates whether the transportable checkpoint is enabled.

Possible states:

Enabled	Indicates that the schedule creates transportable checkpoints.
Disabled	Indicates that the schedule creates standard checkpoints.

Prefix

Specifies the text that is appended to the beginning of the transportable checkpoint filename.

Directory

Identifies the local directory where the transportable checkpoints are stored.

Related concepts

- *About Checkpoint Schedules*

Related tasks

- *View a Checkpoint Schedule*

View Consistency Group, Consistency Group Tab

Allows you to review the details of the Pillar Axiom Data Protection Manager (DPM) application consistency group.

Data Protection Manager recognizes the following application data as consistency groups:

- Microsoft Exchange Server storage groups
- Microsoft SQL Server database instances
- Oracle database instances
- Oracle Automatic Storage management (ASM) disk groups

Name

Identifies the name of the consistency group.

Consistency Group ID

Displays the consistency group unique identifier.

Consistency Status

Identifies the status of the consistency group or application. On Linux and Solaris systems, DPM requires an Oracle database login before database-specific information is displayed.

Possible status:

ASM Credentials Required

Indicates that DPM requires an Oracle ASM login credential to display additional database information.

ASM Parameter File

Indicates that DPM has detected an ASM startup parameter file on the Oracle ASM disk group that is represented by the consistency group.

Axiom Access Required

Indicates that DPM requires the Pillar Axiom login credentials.

Consistency Status Unknown

Indicates that insufficient information is available to determine the consistency status. This status might be caused by the application being in an inoperable or otherwise unstable state.

Database Shutdown

Indicates that the connected database has been shut down.

Files Not in Consistency Group

Indicates that some files that are associated with the Oracle database, such as log or control files, are not stored on the same Oracle ASM disk group.

Invalid Username

Indicates that the supplied database username is invalid.

Multiple Applications

Indicates that the consistency group shares one or more LUNs with other consistency groups on the Pillar Axiom system. Sharing LUNs across consistency groups is not a DPM best practice for configuring applications on the system.

Multiple Axioms

Indicates that the consistency group uses LUNs from more than one Pillar Axiom system.

Non-Pillar LUNs

Indicates that the consistency group contains LUNs that do not reside on a Pillar Axiom system.

Not In Archivelog Mode

Indicates that an Oracle database is not set to `Archivelog` mode.

Not Verified

Indicates that the administrator has not verified that the discovered consistency group is correct.

Optimal

Indicates that no known issues exist with the consistency group.

Username Required

Indicates that the database requires authentication.

Checkpoint Status

Identifies the status of the checkpoint.

Possible states:

Creating

Indicates that DPM is creating checkpoints from the consistency group.

Deleting

Indicates that DPM is removing checkpoints from the consistency group.

Ready to Restore

Indicates that DPM can create checkpoints from the consistency group.

Not Restorable

Indicates that the checkpoint contains consistency errors that prevents DPM from restoring the checkpoint.

Restoring

Indicates that DPM is restoring the consistency group from a checkpoint.

Unknown

Indicates that DPM cannot determine the checkpoint status.

Schedule Status

Identifies whether the consistency group has any associated schedules. Possible states:

- Scheduled
- Unscheduled

Retention Policy

Identifies whether a retention policy applies to checkpoints that are created from the source.

Possible retention states:

- Enabled
- Disabled

Related tasks

- *View Consistency Group Details*
- *Refresh Applications*

View Consistency Group, LUNs Tab

Allows you to review the LUNs that are associated with the application consistency group. The Data Protection Manager discovers only those LUNs that are resident on a managed Pillar Axiom system.

LUN ID (LUID)

Displays the internal identifier of the LUN. This value is the same as the LUN identifier that is used on the Pillar Axiom system.

LUN Device Name

Identifies the LUN name that was assigned by the operating system.

Related tasks

- *View Consistency Group Details*
- *Refresh Applications*

View Consistency Group, Schedules Tab

Allows you to review the checkpoint schedule that is assigned to the selected consistency group.

Name

Identifies the name of the schedule.

Enabled

Identifies whether the schedule is enabled.

Valid states:

Yes	Indicates that the schedule is active.
No	Indicates that the schedule is inactive.

Start Time

Identifies the date and time at which the scheduled operation is set to start.

Frequency

Specifies the frequency by which the scheduled operation runs.

Examples include:

- Every 12 hours
- Every 2 days
- Every 4 weeks

Related tasks

- *View Consistency Group Details*
- *Refresh Applications*

View Consistency Group, Retention Policy Tab

Allows you to review the retention policy that is assigned to the selected consistency group.

Maximum Checkpoints Retention Policy

Indicates that the retention policy applies to a specific number of checkpoints.

Enabled

Specifies whether the maximum checkpoints retention policy is enabled. Possible states:

Enabled	Indicates that DPM retains the specified number of checkpoints.
Disabled	Indicates that all checkpoints are retained.

1 through 30

Indicates the number of checkpoints to keep.

Maximum Duration Retention Policy

Indicates that the retention policy applies for a specific number of days.

Enabled

Specifies whether the maximum duration retention policy is enabled. Possible states:

Enabled	Indicates that DPM retains the checkpoints for a specified number of days.
Disabled	Indicates that all checkpoints are retained.

1 through 30

Indicates the number of days to keep the checkpoints.

Related tasks

- *View Consistency Group Details*
- *Refresh Applications*

View Consistency Group, Oracle Databases Tab

Allows you to review the Oracle database states that are associated with the selected Automatic Storage Management (ASM) disk group.

Note: The Oracle Databases tab appears only when the Oracle database is a member of the ASM diskgroup.

SID

Identifies the Oracle system identifier that distinguishes the database from all other databases in the disk group.

Note: The SID column appears only when the selected ASM consistency group contains Oracle databases.

Archive Log Mode

Identifies the status of the Oracle database.

Possible states:

Requires Credentials	Indicates that DPM cannot access the Oracle database because of invalid or missing username.
Valid Credentials	Indicates that the Oracle database credentials are correct.

Related concepts

- *About Application Consistency Groups*

Related references

- *Oracle Database Requirements*
- *Oracle Automatic Storage Management Requirements*
- *Applications Overview Page*

Related tasks

- *View Consistency Group Details*
- *Refresh Applications*
- *Set the Oracle Username*
- *Set the ASM Username*

View Event Properties Dialog

Allows you to review the properties of the selected event. Oracle Customer Support requests this information for troubleshooting purposes.

Type

Displays the severity level of the entries in the Pillar Axiom event log.

Possible error types:

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.
Error	Reports that an operation has failed. Might require action to prevent subsequent failures of the same type.

Time

Specifies the date and time that the event occurred.

Generating Operation

Indicates the name of the operation, such as checkpoint creation, that generated the event notice.

Operation Status

Indicates the status of the operation that initiated the event.

Number

Identifies the number assigned to the event.

Affected Object

Provides details about the object that caused the event. For Oracle databases, Data Protection Manager provides additional event information.

Identifies the specific object type affected by the event.

Name

Identifies the name of the affected object.

UID

Identifies the unique identification number of the affected object, if available.

Additional Event Details

Provides error information directly from the Oracle database. For more information about these errors, refer to the Oracle Database Error Codes web page (http://docs.oracle.com/cd/B28359_01/server.111/b28278/toc.htm).

Related concepts

- *About Data Protection Manager Events*

Related tasks

- *Display All Events*
- *View Event Details*
- *Refresh the List of Events*

APPENDIX B

Axiom DPM CLI Command Reference

About Axiom DPM CLI Commands

Pillar Axiom Data Protection Manager installs with a command line interface (CLI) utility called the Axiom DPM CLI. When you request a list of DPM objects, the utility uses fully qualified names (FQNs) in the results.

Note: If the filename, command, or description that you are specifying contains spaces, use double quotes when entering the command. The double quotes ensure that the spaces are not removed when the utility processes the command.

When specifying dates and time, use the following format:

```
MM/DD/YYYY HH:mm:SS CM
```

where:

- MM/DD/YYYY designates the date as the two-digit month, two-digit day, and four-digit year.
- HH:mm:SS designates the time as two-digit hour, two-digit minutes, and two-digit seconds.
- CM designates the morning or afternoon value as AM or PM, respectively.

For example, 10/11/2012 01:02:03 PM specifies a date of 3 seconds after 1:02 PM, October 11, 2012.

Related concepts

- *About Data Protection Manager Software*

Related references

- *Axiom DPM CLI Supported Platforms*
- *help*

Related tasks

- *Issue an axiomdpmcli Command for Windows*
- *Issue an axiomdpmcli Command for Solaris and Linux*

Axiom DPM CLI Supported Platforms

The Axiom Data Protection Manager (DPM) CLI runs on Windows, Solaris, and Linux operating systems.

Table 6 DPM CLI supported platforms

Operating system	Required version
Windows	Microsoft Windows Server 2003 Microsoft Windows Server 2008 Microsoft Windows Server 2008, R2
Solaris	Solaris 10, update 10 Solaris 11
Linux	Oracle Linux 5.6 Oracle Linux 6.1

Related concepts

- *About Axiom DPM CLI Commands*

Set the DPM Encryption Key for CLI

Set or update the encryption key for the Pillar Axiom Data Protection Manager (DPM) to ensure secure transactions with the Pillar Axiom system.

1 Open a command console.

2 Change directories to the DPM installation folder.

3 Set the encryption key.

Example:

```
$ axiomdpmcli settings -setEncryptionKey encryptionKey
```

The *encryptionKey* variable identifies the user-supplied encryption key.

Issue an axiomdpmcli Command for Windows

The Axiom DPM CLI utility is installed with the Pillar Axiom Data Protection Manager product. You issue axiomdpmcli commands for the CLI from a console window.

1 Open a command console window by selecting Start > Run, and then enter **`cmd`** in the Open field.

2 From the command prompt, change directories to the installation folder.

```
C:\> chdir “C:\Program Files\Oracle\Pillar Axiom Data
Protection Manager”
```

3 Issue an Axiom DPM CLI command.

Example:

To see a list of the available subcommands, issue the following command:

```
C:\> axiomdpmcli
```

Result:
The CLI displays a list of all of the available subcommands and their options.

Related concepts

- *About Axiom DPM CLI Commands*

Related tasks

- *Issue an axiomdpmcli Command for Solaris and Linux*

Issue an axiomdpmcli Command for Solaris and Linux

The Axiom DPM CLI utility is installed with the Pillar Axiom Data Protection Manager product. You issue axiomdpmcli commands for the CLI from a console window.

1 Open a command console window.

2 From the command prompt, change directories to the installation folder.

Example:

```
chdir DPMInstallFolder/bin
```

The *DPMInstallFolder* variable is the directory path to the Data Protection Manager files.

3 Launch the axiomdpmcli program.

```
$ ./runHostAgentManager.sh
```

4 Issue an Axiom DPM CLI command.

Example:

To see a list of the available subcommands, issue the following command:

```
$ axiomdpmcli
```

Result:
The CLI displays a list of all of the available subcommands and their options.

Related concepts

- *About Axiom DPM CLI Commands*

Related tasks

- *Issue an axiomdpmcli Command for Windows*

application

DESCRIPTION

Lists all of the available applications that are managed by Pillar Axiom Data Protection Manager.

You can use the `-details` option to display a detailed list of information about a specific application.

You can use `-options` to display the options that can be used for specific actions, such as creating a new checkpoint.

SYNTAX

```
axiomdpmcli application -help
```

```
axiomdpmcli application -list [-details]
[-application applicationIdentifier [-options]]
```

PARAMETERS

-help

Displays the `application` subcommand help documentation.

-list

Displays a list of applications that are visible to and supported by DPM.

Valid options:
-details

Provides additional details about the application, if available.

-application

Specifies the application identification number for which to list information. You must supply the *applicationIdentifier* value when using this parameter. Obtain the *applicationIdentifier* value by issuing the following command:

`$ axiomdpmcli application -list`.

Use the *guid* value that is returned by the CLI.

Note: The identifier value includes the curly brackets (`{}`), if returned by the CLI.

The `-application` parameter implies the `-details` parameter.

-options

Displays the parameters that can be used to import, restore, or create the application checkpoint.

Returned options:

- Restore checkpoint options
- Import checkpoint options
- Create checkpoint options

Note: Not all of the values returned by `-options` can be used with the `checkpoint` command.

You can use the returned parameters when importing, restoring, or creating new checkpoints.

For example, some of the returned parameters include the Create Checkpoint Options:

- Checkpoint type: transportable
- Transportable checkpoint indicator: true or false
- Transportable checkpoint directory
- Transportable checkpoint prefix

EXAMPLE

Run the `application` command to display the details and checkpoint creation options of a managed application.

```
$ axiomdpmcli application -list -application
{DA849819-EF2E-4C95-8E7E-10C7A1ADFB76} -options
```

Results:

```
Pillar Axiom Data Protection Manager - CLI v3.0.1
Restore Checkpoint Options:
<data />

Import Checkpoint Options:
<data />

Create Checkpoint Options:
<data>
   <value>
      <struct>
         <member>
            <name>optionName</name>
            <value>Transportable</value>
         </member>
         <member>
            <name>optionType</name>
            <value>{true|false}</value>
         </member>
         <member>
```

```
            <name>optionMessage</name>
            <value>This option causes the creation of
a transportable snapshot. If this option is given, you
must also give the TransportableDirectory option.</
value>
         </member>
      </struct>
   </value>
   <value>
      <struct>
         <member>
            <name>optionName</name>
            <value>TransportableDirectory</value>
         </member>
         <member>
            <name>optionType</name>
            <value>string</value>
         </member>
         <member>
            <name>optionMessage</name>
            <value>This option specifies the directory
in which to store the transportable document. This
option is required if the Transportable option is
given. It cannot be specified without the
Transportable option.</value>
         </member>
      </struct>
   </value>
   <value>
      <struct>
         <member>
            <name>optionName</name>
            <value>TransportablePrefix</value>
         </member>
         <member>
            <name>optionType</name>
            <value>string</value>
         </member>
         <member>
            <name>optionMessage</name>
            <value>This option tells the host what
prefix, if any, to give the transportable document. It
cannot be specified without the Transportable option.</
value>
         </member>
      </struct>
   </value>
</data>
```

Related references

- *checkpoint*
- *event*

axiom

DESCRIPTION

Manages the Pillar Axiom system that is connected to the Pillar Axiom Data Protection Manager (DPM).

Use the `axiom` subcommand to perform any of the following actions:

- List the details of the specified Pillar Axiom system that is managed by DMP.
- Change the login credentials for the specified Pillar Axiom system.
- Remove the login credentials for the specified Pillar Axiom system.

To display the applications and consistency groups, and to manage and create checkpoints on the system, you must provide the login credentials to the Pillar Axiom system and enable DPM access to that system. The login name and password you supply are the administrative credentials that DPM uses to access the Pillar Axiom system. You can set the `-isManaged` parameter and provide the Axiom credentials. Setting the `-isManaged` option allows DPM to display applications and consistency group LUNs that belong to the Pillar Axiom system.

SYNTAX

```
axiomdpmcli axiom -help
```

```
axiomdpmcli axiom -list [-details] [-axiom serialNumber]
```

```
axiomdpmcli axiom -modify -axiom serialNumber
-username usersname [-isManaged {true | false}]
```

```
axiomdpmcli axiom -delete -axiom serialNumber
```

PARAMETERS

-help

Displays the `axiom` subcommand help documentation.

-list

Displays a list of Pillar Axiom systems that are managed by DPM.

Valid options:
-details

Provides additional details about the Pillar Axiom system.

-axiom

Specifies the Pillar Axiom system for which you want to list information. The `-axiom` parameter implies the `-details` parameter.

-**`modify`**

Modifies and stores the Pillar Axiom system administrative login credentials that are managed by DPM.

Valid options:
-**`axiom`**

Specifies the serial number of the Pillar Axiom system that you want to modify.

The `-axiom` parameter implies the `-details` parameter.

-**`username`**

Specifies the new user name to use with the Pillar Axiom system. The `axiomdpmcli` prompts you for the password to manage the Pillar Axiom system.

-**`isManaged`**

Specifies whether DPM displays applications and consistency group LUNs of the Pillar Axiom system.

Valid options:
true

Indicates that the applications, checkpoints, and consistency groups that belong to the Pillar Axiom system are managed by DPM.

false

Indicates that the applications, checkpoints, and consistency groups that belong to the Pillar Axiom system are not managed by DPM.

-**`delete`**

Clears the Pillar Axiom system administrative credentials that are stored by DPM. Clearing the login credentials causes DPM to lose visibility to the applications and consistency group LUNs that reside on the Pillar Axiom system. Reinstate the credentials by using the `axiom -modify` command.

Valid options:
-**`axiom`**

Specifies the Pillar Axiom system administrative credentials that you want to remove from DPM.

EXAMPLE

Run the `axiom` command to display the details of a managed Pillar Axiom system.

```
$ axiomdpmcli axiom -list -axiom A001650XYZ
```

Results:

```
Pillar Axiom Data Protection Manager - CLI v3.0.1
<data>
   <value>
      <struct>
         <member>
            <name>isConnected</name>
            <value>false</value>
         </member>
         <member>
            <name>isManaged</name>
            <value>true</value>
         </member>
         <member>
            <name>serialNumber</name>
            <value>A001650XYZ</value>
         </member>
         <member>
            <name>username</name>
            <value>administrator</value>
         </member>
      </struct>
   </value>
</data>
```

Related references

- *application*

checkpoint

DESCRIPTION

Manages checkpoints on Pillar Axiom Data Protection Manager (DPM).

Use the `checkpoint` subcommand to perform any of the following actions:

- Create checkpoints, which represent a consistent point-in-time image of all the LUNs that comprise the consistency group to back up.
- List checkpoints that are visible to DPM.
- Display information about discovered checkpoints that are not managed by DPM.
- Display detailed information about a specified checkpoint.
- Modify the checkpoint description.
- Restore the checkpoint source LUNs to the point-in-time represented by the checkpoint.
- Import a transportable checkpoint file.
- Mount an imported transportable checkpoint file to its original or a new drive location.

SYNTAX

```
axiomdpmcli checkpoint -help
```

```
axiomdpmcli checkpoint -create
-id consistencyGroupOrAppIdentifier [-application]
[-description description] [-permanent {true | false}]
[-options optionName1:value, optionName2:value, …]
```

```
axiomdpmcli checkpoint -list
[-checkpoint checkpointIdentifier] [-details]
```

```
axiomdpmcli checkpoint -modify
-checkpoint checkpointIdentifier [-description description]
[-permanent {true | false}]
```

```
axiomdpmcli checkpoint -delete
-checkpoint checkpointIdentifier
```

```
axiomdpmcli checkpoint -restore
[-checkpoint checkpointIdentifier]
[-options optionName1:value,  optionName2:value, …]
```

```
axiomdpmcli checkpoint -import -file absolutePathToFile
[-options optionName1:value,  optionName2:value, …]
```

```
axiomdpmcli checkpoint -mount -file absolutePathToFile
[-snapshots snapshotId1:mountPoint1,  snapshotId2:mountPoint2, …]
```

PARAMETERS **-help**

Displays the `checkpoint` subcommand help documentation.

-create

Creates a checkpoint from a designated application or consistency group.

Valid options:
-id

Specifies the application or consistency group identifier from which to create the checkpoint. The `-id` option can have different meanings depending on the presence of other options.

- When `-id` is used without the `-application` option, DPM uses a consistency group as the source of the checkpoint.
- When `-id` is used with the `-application` option, DPM uses an application as the source of the checkpoint.

The `-id` option requires the *consistencyGroupOrAppIdentifier* parameter, which specifies the identifier of the consistency group or application. Obtain the value by issuing one of the following commands:

- `$ axiomdpmcli consistencygroup -list`.

  Use the *associatedApplicationId* value that is returned by the CLI.
- `$ axiomdpmcli application -list`.

  Use the *guid* value that is returned by the CLI.

Note: The identifier value includes the curly brackets (`{}`), if returned by the CLI.

-application

Indicates that the *consistencyGroupOrAppIdentifier* value represents an application as the checkpoint source. When you use the `-application` and `-id` options together, DPM creates a series of checkpoints, one for each consistency group in the application. Creating a series of checkpoints on multiple consistency groups is asynchronous, which means that the DPM creates a checkpoint before creating the next one. To use the consistency group as the checkpoint source, use `-id` without the `-application` option.

-**`description`**

Identifies the description of the checkpoint.

-**`permanent`**

Indicates whether to override the active retention policy. A retention policy specifies that DPM does not keep all of the created checkpoints.

Valid permanency options:
true

Indicates that the checkpoint is not subject to the active retention policy.

false

Indicates that the checkpoint is subject to the active retention policy.

Use the `consistencygroup -modify` command to set the retention policy for all checkpoints. You can specify the maximum number of checkpoints to keep, the maximum number of days to keep the checkpoints, or a combination of both parameters.

-**`options`**

Specifies the options that were used to create the checkpoint from an application or consistency group. Use the form, *optionname:value* for each pair. Separate multiple *optionname:value* pairs with commas.

Obtain the option name and value pairs by issuing the following commands:

- `$ axiomdpmcli application -list -application` *associatedApplicationId* `-options`
- `$ axiomdpmcli consistencgroup -list -consistencygroup` *associatedApplicationId* `-options`

-**`list`**

Displays a list of checkpoints that are visible to DPM.

Valid options:
-**`checkpoint`**

Specifies the checkpoint for which you want to list information. The `-checkpoint` option implies the `-details` option.

Checkpoint requires the *checkpointIdentifier* parameter, which is the identifier of the checkpoint. Obtain the value by issuing the following command:

`$ axiomdpmcli checkpoint -list`.

Use the *guid* value that is returned by the CLI.

-**`details`**

Provides additional information about the checkpoint, if available.

-**`modify`**

Modifies the name, description, and retention policy settings for a given checkpoint.

Valid options:
-**`checkpoint`**

Specifies the checkpoint to modify.

Checkpoint requires the *checkpointIdentifier* parameter, which is the identifier of the checkpoint. Obtain the value by issuing the following command:

`$ axiomdpmcli checkpoint -list`.

Use the *guid* value that is returned by the CLI.

-**`description`**

Specifies the new description for the checkpoint.

-**`permanent`**

Indicates whether to override the active retention policy. A retention policy specifies that DPM does not keep all of the created checkpoints.

Valid permanency options:
true

Indicates that the checkpoint is not subject to the active retention policy.

false

Indicates that the checkpoint is subject to the active retention policy.

Use the `consistencygroup -modify` command to set the retention policy for all checkpoints. You can specify the maximum number of checkpoints to keep, the maximum number of days to keep the checkpoints, or a combination of both parameters.

Permanent checkpoints cannot be deleted by the system by means of a retention policy. You must delete permanent checkpoints manually.

-**`delete`**

Deletes a designated checkpoint.

Valid options:
-**`checkpoint`**

Specifies the checkpoint to delete.

Checkpoint requires the *checkpointIdentifier* parameter, which is the identifier of the checkpoint. Obtain the value by issuing the following command:

`$ axiomdpmcli checkpoint -list`.

Use the *guid* value that is returned by the CLI.

-**`restore`**

Restores the checkpoint source LUNs to the point-in-time represented by the checkpoint.

Restoring from a checkpoint reverts a consistency group to a particular point-in-time. The restore process uses the Clone LUNs on the Pillar Axiom system to restore the LUNs. For more information about restoring a LUN from a Clone LUN, refer to the *Pillar Axiom Administrator's Guide*.

During the restore process, the consistency group is taken offline while the source LUNs are synchronized to the checkpoint LUNs on the Pillar Axiom system. For Windows-based systems, Microsoft Volume Shadow Copy Service (VSS) manages the consistency group during checkpoint restore process. When the background copy begins, the consistency group is brought back online and, if necessary, the restored data is verified.

Valid options:
-**`checkpoint`**

Specifies the checkpoint to restore.

Checkpoint requires the *checkpointIdentifier* parameter, which is the identifier of the checkpoint. Obtain the value by issuing the following command:

`$ axiomdpmcli checkpoint -list`.

Use the *guid* value that is returned by the CLI.

-**`options`**

Specifies the options for restoring the checkpoint. Use the form, *optionname:value* for each pair. Separate multiple *optionname:value* pairs with commas.

Obtain the option name and value pairs by issuing the following commands:

- `$ axiomdpmcli application -list -application` *associatedApplicationId* `-options`
- `$ axiomdpmcli consistencgroup -list -consistencygroup` *associatedApplicationId* `-options`

-**`import`**

Imports a transportable checkpoint file. When creating an immediate or scheduled checkpoint, you can set an option that makes the checkpoint *transportable*. A transportable checkpoint is defined in a Microsoft Volume Shadow Copy Service (VSS) XML document that contains Clone LUN information about the checkpoint. The VSS terminology for Clone LUN is *snapshot*. You can create transportable checkpoints for Microsoft Exchange and Microsoft SQL databases.

Transportable checkpoints can be imported into the original host or to a different host that is connected to the Pillar Axiom system. You can import the Clone LUNs of a transportable checkpoint to a host if that host is connected to the Pillar Axiom system from which you created the checkpoint. After a Clone LUN is imported, it becomes a LUN that is not managed by DPM.

The transportable checkpoint XML document is dependant on the OS and system architecture of the host on which the document is placed. When importing transportable checkpoints, ensure that the originating OS and architecture is compatible to the target host to which you are importing.

- ○ Transportable checkpoints that are created on a Windows 2003 server with 32-bit or 64-bit architecture can be imported on a target host of the same OS and architecture.
- ○ Transportable checkpoints that are created on a Windows 2008 server with 32-bit or 64-bit architecture can be imported on a target host of the same OS of any architecture.

Note: Refer to the Microsoft Developer Network article about VSS Application Compatibility (http://msdn.microsoft.com/en-us/library/aa384627(VS.85).aspx).

When importing a transportable checkpoint, you have the option to mount the Clone LUNs (called *snapshots within the DPM interface*) during the import process or later after the checkpoint XML file has been imported. When you mount the Clone LUNs at the time of import, you can mount the volumes to their original location or map them to a new location. In both cases, imported checkpoints are not seen or managed by DPM. If you choose not to map the Clone LUNs during the import process, you can map them later using Windows disk management tools.

Note: When mounting checkpoints on Windows systems, mount to a mapped drive, not a mount folder.

Valid options:
-**`file`**

Specifies the full path and filename that is used as the source file of the import operation.

-**`options`**

Specifies the options for importing the checkpoint. Use the form, *optionname:value* for each pair. Separate multiple *optionname:value* pairs with commas.

Obtain the option name and value pairs by issuing the following commands:

- `$ axiomdpmcli application -list -application` *associatedApplicationId* `-options`
- `$ axiomdpmcli consistencgroup -list -consistencygroup` *associatedApplicationId* `-options`

-**`mount`**

Mount an imported transportable checkpoint from its transportable snapshot document.

Valid options:
-**file**

Specifies the full path and filename that is used as the source data of the mount operation. The `-file` option is the same information provided to `-import` the file.

Note: When mounting checkpoints on Windows systems, mount to a mapped drive, not a mount folder.

For example to specify the drive path, use the following syntax:

```
C:\fulldrivepath\filename
```

-**snapshots**

Specifies the imported transportable Clone LUN (snapshot) to mount on the system. Use the form, *snapshotID:desiredMountPoint* for each mount. Separate multiple pairs with commas.

Obtain the mount information by using the `checkpoint -import` command.

EXAMPLE

Run the `checkpoint` command to create a permanent checkpoint on a specified consistency group.

```
$ axiomdpmcli checkpoint -create -id
{DA849819-EF2E-4C95-8E7E-10C7A1ADFB76} -description "CLI
Checkpoint" -permanent true
```

Results: DPM creates the checkpoint.

Run `checkpoint -list` to display the checkpoint.

```
$ axiomdpmcli checkpoint -list
```

```
Pillar Axiom Data Protection Manager - CLI v3.0.1
<data>
   <value>
      <struct>
         <member>
            <name>checkpointStatus</name>
            <value>Ready for Restore</value>
         </member>
         <member>
            <name>description</name>
            <value>CLI Checkpoint 2</value>
         </member>
         <member>
            <name>guid</name>
            <value>41303031363A1049D4E14B986DE</value>
         </member>
         <member>
            <name>name</name>
            <value />
         </member>
         <member>
            <name>timestamp</name>
            <value>03/29/2012 01:13:46 PM</value>
         </member>
      </struct>
   </value>
   <value>
      <struct>
         <member>
            <name>checkpointStatus</name>
            <value>Ready for Restore</value>
         </member>
         <member>
            <name>description</name>
            <value>CLI Checkpoint 3</value>
         </member>
         <member>
            <name>guid</name>
            <value>{7FBC98C3-B4FA-AE6277BE065E}</value>
         </member>
         <member>
            <name>name</name>
            <value />
         </member>
         <member>
            <name>timestamp</name>
            <value>3/30/2012 3:04:39 PM</value>
         </member>
      </struct>
   </value>
   <value>
      <struct>
         <member>
            <name>checkpointStatus</name>
            <value>Ready for Restore</value>
         </member>
         <member>
            <name>description</name>
            <value>checkpoints for SQL server</value>
         </member>
         <member>
            <name>guid</name>
            <value>{FF4710CF-B019-C6E08412F84C}</value>
         </member>
         <member>
```

```
            <name>name</name>
            <value />
         </member>
         <member>
            <name>timestamp</name>
            <value>3/29/2012 12:43:08 PM</value>
         </member>
      </struct>
   </value>
</data>
```

Related references

- *application*
- *consistencygroup*
- *event*
- *schedule*

consistencygroup

DESCRIPTION

Manages the consistency groups on Pillar Axiom Data Protection Manager (DPM).

Use the `consistencygroup` subcommand to perform any of the following actions:

- List consistency groups visible to DPM.
- Display information about discovered consistency groups that are not managed by DPM.
- Display detailed information about a specified consistency group.
- Provide login credentials to access consistency group data.
- Modify the consistency group retention policy.
- Hide or expose a consistency group from DPM.

SYNTAX

```
axiomdpmcli consistencygroup -help
```

```
axiomdpmcli consistencygroup -list [-details]
[-showDiscovered]
[-consistencygroup consistencyGroupIdentifier [-options]]
```

```
axiomdpmcli consistencygroup -credentials
-consistencygroup consistencyGroupIdentifier
-username usersname
[-databaseCredentials sid1:username1, sid2:username2, …]
```

```
axiomdpmcli consistencygroup -hide -consistencygroup
consistencyGroupIdentifier
```

```
axiomdpmcli consistencygroup -unhide -consistencygroup
consistencyGroupIdentifier
```

```
axiomdpmcli consistencygroup -verify
-consistencygroup consistencyGroupIdentifier
```

```
axiomdpmcli consistencygroup -modify
-consistencygroup consistencyGroupIdentifier
[-maxDaysEnabled {true | false}] [-maxDaysValue value]
[-maxCountEnabled {true | false}]     [-maxCountValue value]
```

PARAMETERS

`-help`

Displays the `consistencygroup` subcommand help documentation.

`-list`

Displays a list of consistency groups that are visible to DPM.

Valid options:
-**`details`**

Provides additional details about the checkpoint, if available.

-**`showDiscovered`**

Displays information about discovered consistency groups that are not managed by DPM.

-**`consistencygroup`**

Specifies the consistency group you want to manage. The `-consistencygroup` option requires the *consistencyGroupIdentifier*. To obtain the *consistencyGroupIdentifier* value issue the following command:

`$ axiomdpmcli consistencygroup -list`.

Use the *associatedApplicationId* value that is returned by the CLI.

The `-consistencygroup` option implies the `-details` option.

-**`options`**

Displays the options that were used to create the consistency group. Use the returned values with the `checkpoint -create -id` command.

Note: Not all of the values returned by the `-options` option may be used with the `checkpoint` command.

-**`hide`**

Prevents a specified consistency group from being listed by DPM.

Valid options:
-**`consistencygroup`**

Specifies the consistency group you want to manage. The `-consistencygroup` option requires the *consistencyGroupIdentifier*. To obtain the *consistencyGroupIdentifier* value issue the following command:

`$ axiomdpmcli consistencygroup -list`.

Use the *associatedApplicationId* value that is returned by the CLI.

-**`unhide`**

Allows a specified consistency group to be listed by DPM. Use `-unhide` to reverse the `-hide` action.

Valid options:
-**`consistencygroup`**

Specifies the consistency group you want to manage. The `-consistencygroup` option requires the *consistencyGroupIdentifier*. To obtain the *consistencyGroupIdentifier* value issue the following command:

`$ axiomdpmcli consistencygroup -list`.

Use the *associatedApplicationId* value that is returned by the CLI.

-**`verify`**

Verifies that a specified consistency group is ready to create checkpoints.

Valid options:
-**`consistencygroup`**

Specifies the consistency group you want to manage. The `-consistencygroup` option requires the *consistencyGroupIdentifier*. To obtain the *consistencyGroupIdentifier* value issue the following command:

`$ axiomdpmcli consistencygroup -list`.

Use the *associatedApplicationId* value that is returned by the CLI.

-**`credentials`**

Sets up the credentials that allow DPM authorized access to the consistency group for management purposes.

Valid options:
-**`consistencygroup`**

Specifies the consistency group you want to manage. The `-consistencygroup` option requires the *consistencyGroupIdentifier*. To obtain the *consistencyGroupIdentifier* value issue the following command:

`$ axiomdpmcli consistencygroup -list`.

Use the *associatedApplicationId* value that is returned by the CLI.

-**`username`**

Specifies the user name of the managed consistency group. The `axiomdpmcli` prompts you for the `password`.

-**`databaseCredentials`**

Note: The `databaseCredentials` option only applies to Solaris and Linux OSs.

Specifies the unique identifier for the Oracle database (*sid*) and the username to access the database.

Use the form *sid1:username1* for each pair. Separate multiple sid:username pairs with commas.

-**`modify`**

Modifies the retention policy settings of a specified consistency group. A retention policy specifies which checkpoints to keep on the system. You can specify the maximum number of checkpoints to keep, the age of checkpoints, or a combination of the two. You apply the policy to an application consistency group. By applying a retention policy you ensure that all checkpoints that are created for the consistency group are governed by the same retention policy.

You have three options for setting a retention policy:

- By the number days to keep the checkpoints. The system saves checkpoints for up to 30 days.
- By the number of checkpoints to keep. You can save up to 30 checkpoints.
- A combination of the above two options. When both options are enabled, the threshold that is crossed first results in that limit being applied. For example, if you set the number of days to keep to 7 and the number of checkpoints to keep to 10, the system will not keep more than 10 checkpoints in a seven day period.

You can override the retention policy by marking a checkpoint *permanent*. Use the permanent option when planning an immediate or scheduled checkpoint. While the permanent option can be used when you plan a scheduled checkpoint, choosing that option results in the system setting all of the checkpoints that are created by that schedule to permanent. Only individual checkpoints should be set to permanent to avoid stressing available resources.

Note: Checkpoints consume Clone LUN storage on the Pillar Axiom system. Refer to the *Pillar Axiom Administrator's Guide* for managing the Clone LUNs.

Setting the retention policy affects all existing and new checkpoints of the selected consistency group. Your changes take effect the next time that the retention policy engine runs.

Valid options:
-**`consistencygroup`**

Specifies the consistency group you want to manage. The `-consistencygroup` option requires the *consistencyGroupIdentifier*. To obtain the *consistencyGroupIdentifier* value issue the following command:

`$ axiomdpmcli consistencygroup -list`.

Use the *associatedApplicationId* value that is returned by the CLI.

-**`maxDaysEnabled`**

Specifies whether the maximum duration retention policy is enabled. Possible states:
true

Indicates that DPM retains the checkpoints for a specified number of days.

false

Indicates that all checkpoints are retained.

-**`maxDaysValue`**

Indicates the number of days to keep the checkpoints.

Valid values: 1 through 30

-**`maxCountEnabled`**

Specifies whether the maximum checkpoints retention policy is enabled. Possible states:
true

Indicates that DPM retains the specified number of checkpoints.

false

Indicates that all checkpoints are retained.

-maxCountValue

Indicates the number of checkpoints to keep.

Valid values: 1 through 30

EXAMPLE

Run the `consistencygroup` command to display the details of discovered application consistency groups.

```
$ axiomdpmcli consistencygroup -list -showDiscovered
```

Results:

```
Pillar Axiom Data Protection Manager - CLI v3.0.1
<data>
   <value>
      <struct>
         <member>
            <name>associatedApplicationId</name>
            <value>Oracle database</value>
         </member>
         <member>
            <name>consistencyStatus</name>
            <value>Unsupported Lun</value>
         </member>
         <member>
            <name>credentialsAreValid</name>
            <value>true</value>
         </member>
         <member>
            <name>guid</name>
            <value>ORA11G1</value>
         </member>
         <member>
            <name>name</name>
            <value>ORA11G1</value>
         </member>
         <member>
            <name>requiresCredentials</name>
            <value>true</value>
         </member>
         <member>
            <name>username</name>
            <value />
         </member>
      </struct>
   </value>
   <value>
```

```
      <struct>
         <member>
            <name>associatedApplicationId</name>
            <value>Oracle database</value>
         </member>
         <member>
            <name>consistencyStatus</name>
            <value>Unknown Status</value>
         </member>
         <member>
            <name>credentialsAreValid</name>
            <value>true</value>
         </member>
         <member>
            <name>guid</name>
            <value>ORA11G2</value>
         </member>
         <member>
            <name>name</name>
            <value>ORA11G2</value>
         </member>
         <member>
            <name>requiresCredentials</name>
            <value>true</value>
         </member>
         <member>
            <name>username</name>
            <value />
         </member>
      </struct>
   </value>
   <value>
      <struct>
         <member>
            <name>associatedApplicationId</name>
            <value>{DA849819-8E7E-10C7A1ADFB76}</value>
         </member>
         <member>
            <name>consistencyStatus</name>
            <value>Optimal</value>
         </member>
         <member>
            <name>credentialsAreValid</name>
            <value>false</value>
         </member>
         <member>
            <name>guid</name>
            <value>{WINVM\SQLEXP\AxiomSQL}</value>
         </member>
         <member>
            <name>name</name>
            <value>AxiomSQL</value>
         </member>
         <member>
            <name>requiresCredentials</name>
            <value>false</value>
         </member>
         <member>
            <name>username</name>
            <value />
         </member>
      </struct>
   </value>
</data>
```

Related references

- *application*
- *checkpoint*
- *event*

dpmvmi

DESCRIPTION

Manages the virtual machine interface (VMI) connection for Pillar Axiom Data Protection Manager (DPM).

Use the `dpmvmi` subcommand to perform any of the following actions:

- Register a VMI with DPM.
- Display information about an existing VMI connection.
- Update the login credentials associated with the VMI connection.
- Remove an existing VMI connection.

SYNTAX

```
axiomdpmcli dpmvmi -help
```

```
axiomdpmcli dpmvmi -add -ipAddress ipAddress -port port
-username username
```

```
axiomdpmcli dpmvmi -list [-details] [-ipAddress ipAddress]
```

```
axiomdpmcli dpmvmi -modify -ipAddress ipAddress
[-port port] [-username username]
```

```
axiomdpmcli dpmvmi -delete -ipAddress ipAddress
```

PARAMETERS

-help

Displays the `dpmvmi` subcommand help documentation.

-add

Registers a new VMI with DPM.

The virtual environment infrastructure consists of the following primary components:

VMware ESX host

The ESX host contains one or more virtual machine (VM) guests that are installed and configured by the server administrator. A VM configured for DPM requires that you install VMWare tools.

Important! The ESX host relies on a stable communication link with the Pillar Axiom management interface. If the ESX host loses communication with an Axiom system, the ESX server administrator might need to restart the ESX server to establish the connection and refresh the list of discovered systems.

DPM VMI Service

The DPM virtual machine interface (VMI) provides a bridge between the VM and physical host. The VMI is available for Hyper-V and VMware ESX hypervisors.

VMware vCenter

The vCenter server provides administrative support for the ESX host. The vCenter server communicates with the ESX host and all of the VMs installed on the ESX host.

Hyper-V Server

Hyper-V provides the software infrastructure and basic management tools that enables you to create and manage a virtualized server.

When DPM starts from a virtual environment, DPM VMI verifies the following information to establish a connection to the virtual environment:

- The host IP address where the DPM VMI is installed
- The login name and password for the DPM VMI server host
- The HTTPS communications port that is used by the DPM VMI service

DPM might display errors if the credentials to the DPM VMI server host are changed or otherwise unavailable. If DPM fails to connect to the VMI server on startup, DPM posts failure messages in the event log.

If the vCenter server credentials are changed while DPM is running, some DPM actions may fail. Use the `dpmvmi -modify` option to enter the correct credentials, then try the action again.

Valid options:
-**`ipAddress`**

Specifies the IP address of the VMI service.

-**`port`**

Specifies the communications port number of theVMI service.

-**`username`**

Specifies the username to use when connecting to the VMI service. The `axiomdpmcli` prompts you for the password to set for the VMI service.

-**`list`**

Lists the existing VMI with DPM.

Valid options:
-**`ipAddress`**

Specifies the IP address of the virtual machine interface object. The `-ipAddress` option implies the `-details` option.

-**`details`**

Provides additional information about the VMI service, if available.

-**`modify`**

Modifies an existing VMI.

Valid options:
-**`ipAddress`**

Specifies the IP address of the VMI service.

-**`port`**

Specifies the new communications port number of the VMI service.

-**`username`**

Specifies the new username to use when connecting to the VMI service. The `axiomdpmcli` prompts you for the password to set for the VMI service.

-delete

Removes the virtual machine interface from DPM.

Valid options:
-ipAddress

Specifies the IP address of the VMI service to remove.

EXAMPLE

Run the `dpmvmi` command to list the details of the DPM VMI credentials.

```
$ axiomdpmcli dmpvmi -list
```

Results:

```
Pillar Axiom Data Protection Manager - CLI v3.0.1
<data>
   <value>
      <struct>
         <member>
            <name>ipAddress</name>
            <value>18.2.5.555 </value>
         </member>
         <member>
            <name>isValid</name>
            <value>true</value>
         </member>
         <member>
            <name>port</name>
            <value>8008</value>
         </member>
         <member>
            <name>username</name>
            <value>Administrator</value>
         </member>
      </struct>
   </value>
</data>
```

Related references

- *event*
- *settings*

event

DESCRIPTION

Displays system events that occur with Pillar Axiom Data Protection Manager (DPM).

Event details include the following:

- The timestamp that the event occurred
- Error type
- Affected object identification type and number
- Event sequence number
- Event status

SYNTAX

```
axiomdpmcli event -help
```

```
axiomdpmcli event -list [-timestamp timestamp] [-details]
[-event eventNumber]
```

PARAMETERS

-help

Displays the `event` subcommand help documentation.

-list

Displays event information generated by DPM operations.

Valid options:
-timestamp

Specifies the date and time that the event occurred.

-details

Displays additional event details.

-event

Identifies the event for which you want to list information. The `-event` option implies the `-details` option.

The `-list` option displays error types under the *eventType* label.

Possible error types:

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.

Error

Reports that an operation has failed. Might require action to prevent subsequent failures of the same type.

EXAMPLE

Run the `event` command to display the details of a specific event.

```
$ axiomdpmcli event -list -event 41
```

Results:

```
Pillar Axiom Data Protection Manager - CLI v3.0.1
<data>
   <value>
      <struct>
         <member>
            <name>affectedObjectDescriptor</name>
            <value>checkpoint_TP</value>
         </member>
         <member>
            <name>affectedObjectIdentifier</name>
            <value>{227D409F-A7B8-AA2C5FAFE646}</value>
         </member>
         <member>
            <name>affectedObjectType</name>
            <value>Checkpoint</value>
         </member>
         <member>
            <name>eventDescription</name>
            <value>Failed restore of Checkpoint:
{227D409F-A7B8-AA2C5FAFE646}. Checkpoint volumes do not
match Consistency Group volumes.</value>
         </member>
         <member>
            <name>eventExternalSoftwareInformation
            </name>
            <value>UNDEFINED</value>
         </member>
         <member>
            <name>eventNumber</name>
            <value>41</value>
         </member>
         <member>
            <name>eventSourceClass</name>
            <value>Host Agent</value>
         </member>
         <member>
            <name>eventSummary</name>
            <value>RestoreCheckpoint Failed</value>
         </member>
         <member>
            <name>eventTime</name>
            <value>03/29/2012 02:06:36.566 PM</value>
         </member>
         <member>
            <name>eventType</name>
            <value>Error</value>
         </member>
         <member>
            <name>generatingOperation</name>
            <value>Restore Checkpoint</value>
         </member>
         <member>
            <name>generatingOperationStatus</name>
            <value>Failed</value>
         </member>
      </struct>
   </value>
</data>
```

Related references

- *application*
- *checkpoint*
- *consistencygroup*
- *dpmvmi*
- *schedule*

help

DESCRIPTION

Displays a list of all supported Pillar Axiom Data Protection Manager (DPM) subcommands and their options. The `-help` subcommand also provides detailed information about a specific subcommand.

The syntax conventions used for `axiomdpmcli` command arguments are:

Curly brackets ({ })	Indicate a set of command parameters, one of which must be selected.
Square brackets ([ ])	Indicate an optional command parameter or a set of optional command parameters. Command parameters that are not enclosed in square brackets are required.
Vertical bar (|)	Indicates a set of mutually exclusive parameters.
Ellipsis (...)	Indicate that the immediately preceding parameters or group of parameters can be repeated.
Camel case	Used in `axiomdpmcli` commands for ease of reading. Entering commands is not case-sensitive. You can use either camel case or lowercase.

SYNTAX

```
axiomdpmcli -help
```

```
axiomdpmcli command-name -help
```

PARAMETERS

Help is available for the following commands:

- `axiom`
- `application`
- `consistencygroup`
- `checkpoint`
- `event`

- `schedule`
- `settings`
- `dpmvmi`

EXAMPLE

Use the `help` command to display a list of all `axiomdpmcli` commands and options.

`$ axiomdpmcli help`

Results:

```
Pillar Axiom Data Protection Manager - CLI v3.0.1
No Parameters Given.
Application Usage:
    application -help
    application -list
        [-details]
        [-application applicationIdentifier [-options]]

Axiom Usage:
    axiom -help
    axiom -list
        [-details]
        [-axiom serialNumber]
    axiom -modify
        -axiom serialNumber
        -username username
        [-isManaged {true|false}]
    axiom -delete
        -axiom serialNumber

Checkpoint Usage:
    checkpoint -help
    checkpoint -list
        [-details]
        [-checkpoint checkpointIdentifier]
    checkpoint -create
        -id consistencyGroupOrAppIdentifier
        [-application]
        [-name name]
        [-description description]
        [-permanent {true|false}]
        [-options
optionName1:value,optionName2:value,...]
    checkpoint -restore
        -checkpoint checkpointIdentifier
        [-options
optionName1:value,optionName2:value,...]
    checkpoint -modify
        -checkpoint checkpointIdentifier
        [-name name]
        [-description description]
        [-permanent {true|false}]
    checkpoint -delete
        -checkpoint checkpointIdentifier
    checkpoint -import
        -file absolutePathToFile
        [-options
optionName1:value,optionName2:value,...]
    checkpoint -mount
        -file absolutePathToFile
        [-snapshots
snapshotId1:mountPoint1,snapshotId2:mountPoint2,...]

Consistency Group Usage:
    consistencygroup -help
    consistencygroup -list
        [-details]
        [-consistencygroup consistencyGroupIdentifier
[-options]]
    consistencygroup -credentials
        -consistencygroup consistencyGroupIdentifier
        -username username
    consistencygroup -hide
        -consistencygroup
consistencyGroupIdentifier
    consistencygroup -verify
        -consistencygroup
consistencyGroupIdentifier
    consistencygroup -modify
        -consistencygroup consistencyGroupIdentifier
        [-maxDaysEnabled {true|false}]
        [-maxDaysValue value]
        [-maxCountEnabled {true|false}]
        [-maxCountValue value]

DPM VMI Usage:
    dpmvmi -help
    dpmvmi -list
        [-details]
        [-ipAddress dpmVmiIdentifier]
    dpmvmi -add
        -ipAddress ipAddress
        -port port
        -username username
    dpmvmi -delete
        -ipAddress dpmVmiIdentifier
    dpmvmi -modify
        -ipAddress ipAddress
        [-port port]
        [-username username]

Event Usage:
    event -help
    event -list
        [-details]
        [-timestamp timestamp]
        [-event eventNumber]

Schedule Usage:
    schedule -help
    schedule -list
        [-details]
        [-schedule scheduleIdentifier]
    schedule -create
        -id consistencyGroupOrAppIdentifier
        [-application]
        -name scheduleName
        -begin beginTime
        -frequency frequency
        -recurrence recurrence
        -enabled {true|false}
        -permanent {true|false}
        [-recurrenceDays recurrenceDays]
        [-options
optionName1:value,optionName2:value,...]
    schedule -delete
        -schedule scheduleIdentifier
    schedule -modify
        -schedule scheduleIdentifier
        [-enabled {true|false}]
        [-permanent {true|false}]
        [-name scheduleName]
        [-begin beginTime]
        [-frequency frequency]
        [-recurrence recurrence]

Settings Usage:
    settings -help
    settings -isEncryptionInitialized
    settings -getVirtualStatus
    settings -setVirtualStatus
        -virtualStatus {true|false}
    settings -setEncryptionKey
```

Related references

- *application*
- *axiom*
- *checkpoint*
- *consistencygroup*
- *dpmvmi*
- *event*
- *schedule*
- *settings*

schedule

DESCRIPTION

Manages Pillar Axiom Data Protection Manager (DPM) checkpoint schedules to be performed in the future during specified intervals.

A checkpoint schedule creates checkpoints on a regular basis. You can control the automatic checkpoint activity by using the following scheduling parameters:

- The date and time that the automatic checkpoints starts
- The recurrence for when the automatic checkpoints operates
- The frequency at which the automatic checkpoints operates

SYNTAX

```
axiomdpmcli schedule -help
```

```
axiomdpmcli schedule -create [-application]
-id consistencyGroupOrAppIdentifier -name scheduleName
-begin beginTime -frequency frequency -recurrence recurrence
[-permanent {true | false}] [-enabled {true | false}]
[-recurrenceDays recurrenceDays]
[-optionsName optionName1:value, optionName2:value, …]
```

```
axiomdpmcli schedule -list -schedule scheduleIdentifier
[-details]
```

```
axiomdpmcli schedule -modify -schedule scheduleIdentifier
[-name scheduleName] [-begin beginTime]
[-frequency frequency] [-recurrence recurrence]
[-permanent {true | false}] [-enabled {true | false}]
```

```
axiomdpmcli schedule -delete -schedule scheduleIdentifier
```

PARAMETERS

-help

Displays the `schedule` subcommand help documentation.

-create

Creates a DPM schedule that creates checkpoints from a designated application and consistency group.

Valid options:
-application

Indicates that the *consistencyGroupOrAppIdentifier* value represents an application as the checkpoint source. When you use the `-application` and `-id` options together, DPM creates a series of checkpoints, one for each consistency group in the application. Creating a series of checkpoints on multiple consistency groups is asynchronous, which means that the DPM creates a checkpoint before creating the next one. To use the consistency group as the checkpoint source, use `-id` without the `-application` option.

-**`id`**

Specifies the application or consistency group identifier from which to create the checkpoint. The `-id` option can have different meanings depending on the presence of other options.

- When `-id` is used without the `-application` option, DPM uses a consistency group as the source of the checkpoint.
- When `-id` is used with the `-application` option, DPM uses an application as the source of the checkpoint.

-**`enabled`**

Indicates whether the schedule is enabled. Valid options:
true

Specifies that the scheduled operation is performed at the specified time.

false

Specifies that no scheduled operation is performed.

-**`begin`**

Specifies the date and time at which DPM starts the scheduled operation.

-**`frequency`**

Specifies the date and time at which DPM starts a scheduled operation.

Valid options:

1	Schedule runs every hour.
2	Schedule runs every day.
3	Schedule runs every week.

-**`recurrence`**

Specifies how often the system should perform the scheduled operation. Valid values vary based on the schedule's recurrence interval and frequency.

Valid options:
`1 through 24`

Specifies values that are valid with the hourly frequency option based on a 24-hour clock (`-frequency` *2*).

`1 through 7`

Specifies values that are valid with the daily frequency option (`-frequency` *3*). For example, the value for Monday is *1*.

`1 through 4`

Specifies values that are valid with the weekly frequency option (`-frequency` *4*). For example, a value of *4* indicates to run the schedule every four weeks.

-**`recurrenceDays`**

Specifies the weekday on which to run the scheduled operation. Separate multiple days with commas. Valid weekday values:

- sunday
- monday
- tuesday
- wednesday
- thursday
- friday
- saturday

-**`options`**

Specifies the options that were used to create the checkpoint from an application or consistency group. Use the form, *optionname:value* for each pair. Separate multiple *optionname:value* pairs with commas.

Obtain the option name and value pairs by issuing the following commands:

- `$ axiomdpmcli application -list -application` *associatedApplicationId* `-options`

- `$ axiomdpmcli consistencgroup -list -consistencygroup` *associatedApplicationId* `-options`

-**`list`**

Displays a list of schedules that will be performed in the future.

Valid options:
-**`schedule`**

Specifies the schedule for which you want to list information. The `-schedule` option implies the `-details` option.

-**`details`**

Provide additional information about the schedule, if available.

-**`modify`**

Modifies a DPM schedule that creates checkpoints from a designated application and consistency group.

Valid options.
-**`schedule`**

Specifies the schedule that you want to modify.

-**`name`**

Specifies the new name of the scheduled operation.

-**`permanent`**

Valid permanency options:
true

Indicates that the checkpoint is not subject to the active retention policy.

false

Indicates that the checkpoint is subject to the active retention policy.

-**`enabled`**

Indicates whether the schedule is enabled. Valid options:
true

Specifies that the scheduled operation is performed at the specified time.

false

Specifies that no scheduled operation is performed.

-**begin**

Specifies the date and time at which DPM starts the scheduled operation.

-**frequency**

Specifies the date and time at which DPM starts a scheduled operation.

Valid options:

1	Schedule runs every hour.
2	Schedule runs every day.
3	Schedule runs every week.

-**recurrence**

Specifies how often the system should perform the scheduled operation. Valid values vary based on the schedule's recurrence interval and frequency.

Valid options:
1 through 24

Specifies values that are valid with the hourly frequency option based on a 24-hour clock (`-frequency` *2*).

1 through 7

Specifies values that are valid with the daily frequency option (`-frequency` *3*). For example, the value for Monday is *1*.

1 through 4

Specifies values that are valid with the weekly frequency option (`-frequency` *4*). For example, a value of *4* indicates to run the schedule every four weeks.

-**delete**

Deletes a designated schedule.

Valid options:
-**schedule**

Specifies the schedule that you want to delete.

EXAMPLE

Run the `schedule` command to generate a schedule that will create a checkpoint every two weeks from the Oracle application at 1:00 am every other Sunday.

```
$ axiomdpmcli schedule -create -id "Oracle (Need
default name defined)" -application -begin "04/05/2012
01:00:00 AM" -name "bi-weekly Oracle backup" -frequency
4 -recurrence 2 -recurrenceDays sunday -enabled true
-permanent false
```

Run the `schedule -list -details` command to display the results:

```
Pillar Axiom Data Protection Manager - CLI v3.0.1
<data>
   <value>
      <struct>
         <member>
            <name>affectedObjectIdentifier</name>
            <value>Oracle database</value>
         </member>
         <member>
            <name>affectedObjectType</name>
            <value>Application</value>
         </member>
         <member>
            <name>permanent</name>
            <value>false</value>
         </member>
         <member>
            <name>scheduleBeginTime</name>
            <value>4/8/2012 1:00:00 AM</value>
         </member>
         <member>
            <name>scheduleEnabled</name>
            <value>true</value>
         </member>
         <member>
            <name>scheduleFrequency</name>
            <value>Weekly</value>
         </member>
         <member>
            <name>scheduleIdentifier</name>
            <value>bi-weekly Oracle backup1</value>
         </member>
         <member>
            <name>scheduleName</name>
            <value>bi-weekly Oracle backup_Sunday
            </value>
         </member>
         <member>
            <name>scheduleRecurrence</name>
            <value>2</value>
         </member>
         <member>
            <name>scheduleType</name>
            <value>Clone</value>
         </member>
      </struct>
   </value>
</data>
```

Related references

- *checkpoint*
- *consistencygroup*

settings

DESCRIPTION

Manages the host agent settings for Pillar Axiom Data Protection Manager (DPM).

Use the `settings` subcommand to manage the host agent settings for DPM to perform any of the following actions:

- Determine whether DPM is protected with an encryption key.
- Set the encryption passkey that DPM uses to store credential information.
- Set the status for DPM to behave properly within a virtual environment.
- Determine the status of an existing encryption key.
- Determine the status of whether DPM is working within a virtual environment.

Encryption ensures that DPM can safely perform transactions by registering and managing the following login credentials:

- Virtual machine interface (VMI)
- Consistency group
- Pillar Axiom

SYNTAX

```
axiomdpmcli settings -help
```

```
axiomdpmcli settings -isEncryptionInitialized
```

```
axiomdpmcli settings -setEncryptionKey
```

```
axiomdpmcli settings -getEncryptionKey
```

```
axiomdpmcli settings -setVirtualStatus {true | false}
```

```
axiomdpmcli settings -getVirtualStatus
```

PARAMETERS

-help

Displays the `settings` subcommand help documentation.

-isEncryptionInitialized

Displays the state of the persistent manager in the DPM host agent.

Possible states:
true

Indicates that DPM contains an encryption key and is able to persist confidential information.

false

Indicates that DPM contains no encryption key and is unable to persist confidential information.

-setEncryptionKey

Allows the administrator to store or change an encryption pass key that DPM uses when storing confidential information.

-setVirtualStatus

Sets the virtual status of the host agent that is running DPM.

Valid options:
-virtualStatus

Specifies the `-setVirtualStatus` state to set.

Valid options:
true

Specifies that DPM is operating within a virtual environment.

false

Specifies that DPM is operating within a physical environment.

-getVirtualStatus

Displays the state of the DPM virtual environment.

Valid states:
true

Indicates that DPM is operating within a virtual environment.

false

Indicates that DPM is operating within a physical environment.

EXAMPLE

Run the `settings` command to display whether DPM is running within a virtual environment.

```
$ axiomdpmcli settings -getVirtualStatus
```

Results:

```
Pillar Axiom Data Protection Manager -CLI v3.0.1
<data>
   <value>
      <struct>
         <member>
            <name>isVirtual</name>
            <value>true</value>
         </member>
      </struct>
   </value>
</data>
```

Related references

- *axiom*
- *dpmvmi*
- *event*

APPENDIX C

Known Issues

Known Issues

The issues listed in the following table were known at the time of this release.

Table 7 Known issues

Issue	Workaround or planned fix
Residual host entries from a previous installation of Pillar Axiom Path Manager (APM) can interfere with checkpoint creation. These residual host entries interfere when Data Protection Manager attempts to create checkpoint Clone LUNs on the Pillar Axiom system, causing Data Protection Manager to report a checkpoint creation error. **Note:** This issue does not occur if APM is still installed and running on the host accessing the Pillar Axiom system.	Use the Pillar Axiom GUI to delete any residual APM-created host entries from the Pillar Axiom system.
Pillar Axiom Data Protection Manager reports an error in the Events log when restoring a Microsoft Exchange 2003 checkpoint running Windows 2003. Exchange writer reports that the storage group you are attempting to restore is online and therefore produces two errors: Processing pre-restore and Storage Group is online.	You can safely ignore this error. The internal scripts use the MS Exchange System Management tool to determine whether the storage group is online or not, and proceeds accordingly.

Index