
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 États-Unis, ou à toute entité qui délivre la licence de ce logiciel ou l’utilise pour le compte du Gouvernement des États-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.
List of Tables

Table 1: Oracle resources ................................................................. 9
Table 2: Typography to mark certain content .................................. 10
Table 3: Typography to mark command syntax .............................. 10
Table 4: Data Protection Manager requirements ............................. 13
Table 5: Virtual machine requirements .......................................... 22
Table 6: Schedule recurrence intervals ........................................... 68
Table 7: DPM CLI supported platforms .......................................... 84
List of Figures

Figure 1: DPM in a Microsoft Hyper-V environment

23
# Preface

## Oracle Resources

### Table 1: Oracle resources

<table>
<thead>
<tr>
<th>For help with...</th>
<th>Contact...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td><a href="http://www.oracle.com/support">http://www.oracle.com/support</a></td>
</tr>
<tr>
<td>Training</td>
<td><a href="https://education.oracle.com">https://education.oracle.com</a></td>
</tr>
<tr>
<td>Documentation</td>
<td>- Oracle Technology Network Documentation: <a href="http://docs.oracle.com">http://docs.oracle.com</a></td>
</tr>
<tr>
<td></td>
<td>- From Oracle FS System Manager (GUI): Help &gt; Documentation</td>
</tr>
<tr>
<td></td>
<td>- From Oracle FS System HTTP access: <a href="http://system-name-ip/documentation.php">http://system-name-ip/documentation.php</a> where system-name-ip is the name or the public IP address of your system</td>
</tr>
<tr>
<td>Documentation feedback</td>
<td><a href="http://www.oracle.com/goto/docfeedback">http://www.oracle.com/goto/docfeedback</a></td>
</tr>
</tbody>
</table>
Typographical Conventions

Table 2: Typography to mark certain content

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
</table>
| *italics*  | Within normal text, words in italics indicate one of the following items:  
- Hypertext, as in a URL  
- A reference to a book title  
- New terms and emphasized words  
- Command variables |

| monospace  | Indicates one of the following, depending on the context:  
- The name of a file or the path to the file  
- *Output* displayed by the system on the command line |

| monospace (bold) | *Input* provided by an administrator on the command line. |

| >          | Indicates a menu item or a navigation path in Oracle FS System Manager (GUI). For example, “Click SAN > Storage > LUNS > Action > Clone” means to click the Clone link on the SAN page in the GUI. |

| ...       | Indicates that one or more steps have been omitted from the path or menu structure. The ellipsis is used within an expression of a navigation path or within a cascading menu structure. For example, in the SAN > Storage > LUNS > ... > Clone menu structure, the ... implies that one or more menu items have been omitted. |

Command Syntax Conventions

Table 3: Typography to mark command syntax

<table>
<thead>
<tr>
<th>Typographic symbol</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ ]</td>
<td>Square brackets. Delimits an optional command parameter or a set of optional command parameters.</td>
</tr>
<tr>
<td>{ }</td>
<td>Braces. Delimits a set of command parameters, one of which must be selected.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>Ellipsis. Indicates that the immediately preceding parameter or group of parameters can be repeated.</td>
</tr>
<tr>
<td>monospace</td>
<td>Indicates the name of a command or the name of a command option (sometimes called a <em>flag</em> or <em>switch</em>).</td>
</tr>
<tr>
<td>italic</td>
<td>Indicates a variable for which you need to supply a value.</td>
</tr>
</tbody>
</table>
Command parameters that are not enclosed within square brackets ([ ] ) are required.

**Important:** The above symbols (and font styling) are based on the POSIX.1-2008 specification. These symbols are used in the command syntax only to clarify how to use the command parameters. *Do not enter these symbols on the command line.*

**Related Documentation**

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

Familiarize yourself with the following related documentation:


- *Oracle FS System Oracle Flash Storage System Administrator’s Guide:* Provides detailed information on creating and managing storage resources.

- *Oracle Flash Storage System CLI Reference* provides detailed information about functions available in the Oracle FS System command line interface (CLI).

CHAPTER 1

DPM Overview

Data Protection Manager Overview

The Oracle FS 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 creates and manages application-aware backup and recovery of application data using storage for the Oracle FS System and Oracle Axiom Systems. DPM runs on Windows, Linux, and Solaris operating systems. DPM is available with both GUI and CLI interfaces.

DPM can be run from a physical or virtual environment. To work in either environment, DPM requires Oracle FS System release 6.1 or higher and Oracle Axiom Systems release 5.4 or higher.

Note: DPM supports both Oracle Axiom Systems release 5.4 or higher and Oracle FS System release 6.1 or higher. Throughout this documentation, references made to the Oracle FS System also apply to the Oracle Axiom System unless noted. Also, any reference to Oracle Storage Systems includes both the Oracle Axiom System and Oracle FS System.

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 Oracle FS System to create Clone LUNs that represent the application data. The Clone LUNs are stored on the Oracle FS System.

Note: For information on LUN and Clone LUN requirements including storage capacity, review the Oracle Flash Storage System Administrator’s Guide.

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.

Note: DPM works with applications that are online and available and is intended to restore point in time checkpoints for the purpose of recovering data. DPM is not designed to provide disaster recovery. For example, to restore a checkpoint for an Oracle database, the Oracle database must be in the Open state. If the
Oracle database is in the Offline state and not the Open state, the checkpoint cannot be restored.

**Data Protection Manager Requirements**

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

**Table 4: Data Protection Manager requirements**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Required version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows operating systems</td>
<td>Microsoft Windows Server 2008 (32 and 64 bit)</td>
</tr>
<tr>
<td></td>
<td>Microsoft Windows Server 2008 R2 (64 bit)</td>
</tr>
<tr>
<td></td>
<td>Microsoft Windows Server 2012</td>
</tr>
<tr>
<td></td>
<td>Microsoft Windows Server 2012 R2</td>
</tr>
<tr>
<td>Linux operating systems</td>
<td>RHEL 5.8, or later</td>
</tr>
<tr>
<td></td>
<td>RHEL 6.2, or later</td>
</tr>
<tr>
<td></td>
<td>RHEL 7.0 or later</td>
</tr>
<tr>
<td></td>
<td>Oracle Enterprise Linux 5.8, or later</td>
</tr>
<tr>
<td></td>
<td>Oracle Enterprise Linux 6.2, or later</td>
</tr>
<tr>
<td></td>
<td>Oracle Enterprise Linux 7.0, or later</td>
</tr>
<tr>
<td>Solaris operating systems</td>
<td>Solaris Sparc 10 and later</td>
</tr>
<tr>
<td></td>
<td>Solaris Sparc 11 and later</td>
</tr>
<tr>
<td></td>
<td>Solaris x86 10 update 10 (32 and 64 bit), and later</td>
</tr>
<tr>
<td></td>
<td>Solaris x86 110 (64 bit), and later</td>
</tr>
<tr>
<td>VSS-enabled applications</td>
<td>Microsoft Exchange Server 2003</td>
</tr>
<tr>
<td></td>
<td>Microsoft Exchange Server 2007</td>
</tr>
<tr>
<td></td>
<td>Microsoft Exchange Server 2010</td>
</tr>
<tr>
<td></td>
<td>Microsoft Exchange Server 2013</td>
</tr>
<tr>
<td></td>
<td>Microsoft SQL Server 2005</td>
</tr>
<tr>
<td></td>
<td>Microsoft SQL Server 2008</td>
</tr>
<tr>
<td></td>
<td>Microsoft SQL Server 2012</td>
</tr>
<tr>
<td></td>
<td>Microsoft SharePoint Server 2011</td>
</tr>
<tr>
<td></td>
<td>Microsoft SharePoint Server 2013</td>
</tr>
</tbody>
</table>
### Table 4: Data Protection Manager requirements (continued)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Required version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle databases</td>
<td>Oracle Database 10g Release 2</td>
</tr>
<tr>
<td><strong>Note:</strong> Oracle databases are supported on Windows, Solaris, and Linux OSs.</td>
<td>Oracle Database 11g Release 1</td>
</tr>
<tr>
<td></td>
<td>Oracle Database 11g Release 2</td>
</tr>
<tr>
<td></td>
<td>Oracle Database 12c Release 1</td>
</tr>
<tr>
<td>Oracle FS System software release with Fibre Channel SAN fabric or iSCSI Ethernet connectivity capability.</td>
<td>Release 6.1 or later</td>
</tr>
<tr>
<td>Oracle Axiom systems software release with Fibre Channel SAN fabric or iSCSI Ethernet connectivity capability.</td>
<td>Release 5.4 or higher</td>
</tr>
<tr>
<td>Java Runtime (Linux and Solaris only).</td>
<td>Version 1.7</td>
</tr>
<tr>
<td><strong>Note:</strong> DPM for Windows contains a version of JRE.</td>
<td>Set the environment variable <code>JAVA_HOME</code> to the JRE parent directory.</td>
</tr>
<tr>
<td>Java for DPM VMI vCenterServer plugin.</td>
<td>Version 1.6</td>
</tr>
<tr>
<td></td>
<td>Set the environment variable <code>JAVA_HOME</code> or <code>JRE_HOME</code> to the JDK parent directory.</td>
</tr>
<tr>
<td>Supported virtual environments.</td>
<td>Windows Hyper V (2008 and 2012 servers), vCenter Server 4.1 or higher (DPM VMI must be installed on a Windows 2008 or 2012 server)</td>
</tr>
<tr>
<td>Port 8083 on the Oracle FS System needs to be able to communicate with DPM.</td>
<td>Used by DPM to communicate with Oracle FS System when issuing CLI commands.</td>
</tr>
</tbody>
</table>

### Related Links

*Software Installation Overview*

### Microsoft VSS Integration with DPM Overview

Oracle FS Data Protection Manager (DPM) uses the Microsoft Volume Shadow Copy Service (VSS) to make shadow copies of application data, which is stored on a Oracle FS 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 shuts down or pauses applications as needed to enable the restore operation.

Microsoft VSS is a plug-in based service and allows third-party add ons, such as the Oracle FS Volume Shadow Copy Service Provider, to be installed to provide vendor specific backups of the application data without interrupting the normal operations of the applications.

Hardware Providers are a component of the VSS feature that manages snapshots on storage hardware. Oracle provides the Oracle FS Volume Shadow Copy Service Hardware Provider plug-in that enables backups of the application data without interrupting normal operations on the Oracle FS System. VSS is a feature of the Microsoft Windows Server. The plug-in, which is required to support VSS, is installed during the DPM installation.

**Note:** During the DPM installation, the plug-in is installed unless there is a version of the plug-in already installed that matches the version that DPM installs. If DPM detects a matching plug-in, DPM does not install the plug-in supplied with DPM. Once DPM is installed, Oracle recommends that you do not install a newer version of the plug-in; instead use the plug-in supplied by DPM.

For more information about VSS, refer to the following documentation:


**Application-Aware Backups Overview**

Oracle FS 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*. A 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. Backups of application data contain all the relevant data and/or logs required to restore the data for that application to a particular point in time.

The Oracle FS 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, DPM pauses the application, the filesystem flushes volume data and the Oracle FS System momentarily stops all write operations and writes any cached application data to disk. The Oracle FS 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. The Clone LUNs are stored on the Oracle FS System.
DPM creates checkpoints of Oracle databases, Microsoft Exchange Server, or Microsoft SQL Server consistency groups that are stored on Oracle FS System. 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 Links
- Application Consistency Groups Overview
- LUN Configuration for Data Consistency
- LUN Configuration for Applications
- Applications Overview Page

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 Oracle FS System Manager provides QoS Storage Profiles for database applications. Choose the profile for your database environment.

  Refer to the Oracle FS System Oracle Flash Storage System 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 Oracle FS System LUNs for mapping and informational purposes. RDM is not necessary in iSCSI environments.

Microsoft Exchange Server Backups Description
Microsoft Exchange Server 2010 and 2013 stores data in databases (previous versions of Microsoft Exchange used storage groups), which are Exchange Server application instances.

Microsoft Exchange databases or storage groups are groups of LUNs that you define when you set up your Exchange Server implementation. Microsoft Exchange databases or storage groups can contain data LUNs and transaction log LUNs. For best performance with Oracle FS Data Protection Manager (DPM), Oracle recommends setting up databases or storage groups that consist of dedicated LUNs that are not used by other applications that contain a single Microsoft Exchange database.

Data Protection Manager recognizes each Exchange database or storage group that is set up on a Oracle FS 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 Oracle FS System.

**Related Links**

*Applications Overview Page*

*Refresh Applications*

**Microsoft SQL Server Backups Description**

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 Oracle FS Data Protection Manager (DPM), Oracle recommends 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 Oracle FS 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 Oracle FS System.

**Related Links**

*Microsoft SQL and Exchange Resources*

*Applications Overview Page*

*Refresh Applications*

**Microsoft SharePoint Database Requirements**

Oracle FS 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 the Oracle FS System 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 Oracle FS 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.
Oracle Automatic Storage Management Requirements

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

Oracle FS 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:


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

- Create one drive partition for each Oracle FS System 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 Oracle FS System.
- Store all of the datafiles, control files, SPFILE, and redo logs on a single ASM disk group. For example place all of the datafiles on DATA diskgroup and the backups and archive log files on flash recovery area (FRA) diskgroup. Control files and redo logs multiplexed across multiple diskgroups are not supported.
- Keep the ASM disk group separated from the Oracle database FRA. The FRA is where you store the database archived redo log files. The FRA with the archive logs and database backups can be in a separate diskgroup from the datafiles. But the FRA must not be on a diskgroup that includes data,
control, and log files of another database that a user may want to backup and restore.

- 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 operating systems, 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 operating system 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 Links**

* Application Consistency Groups Overview
* Applications Overview Page
* Oracle Database Requirements
* View Consistency Group, Oracle Databases Tab
* Set the Oracle Database Username
* Set the ASM Username

**Oracle Database Requirements**

Oracle FS 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 an Oracle FS System.
- The LUNs of each database must reside on a single Oracle FS 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. FRA is where the Oracle database stores the archive log files. Separating the files from the ASM storage area assures backup and restore data integrity.

- For Linux and Solaris operating systems, DPM requires that you provide an Oracle database username to authenticate operating system access to the database. A password is not necessary.

**Note:** When creating an Oracle database, make sure the length of the Oracle System ID (SID) does not exceed eight characters to ensure compatibility with DPM.

**Related Links**
- Application Consistency Groups Overview
- Applications Overview Page
- View Consistency Group, Oracle Databases Tab
- Oracle Automatic Storage Management Requirements
- Set the ASM Username
- Set the Oracle Database Username

**Microsoft SQL and Exchange Resources**
To work optimally with the Oracle FS Data Protection Manager, the following resources can be helpful for configuring your server.

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


**DPM Virtual Environment Overview**
The Oracle FS 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 Oracle FS System management interface. If the ESX host loses communication with an Oracle FS 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.

Note: Within a virtualized environment, DPM communicates with DPMVMI, and then DPMVMI communicates with either the VMware vCenter Server or Hyper-V Server to obtain the responses required by DPM. Neither DPM nor the DPMVMI service communicates directly with the ESX Hosts.

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.
Virtual Machine Requirements

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

Table 5: Virtual machine requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Required version or value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows operating systems</td>
<td>Microsoft Windows Server 2008</td>
</tr>
<tr>
<td></td>
<td>Microsoft Windows Server 2012</td>
</tr>
<tr>
<td>Oracle FS System release version</td>
<td>For Oracle Axiom, release 5.4, or later</td>
</tr>
<tr>
<td></td>
<td>For Oracle FS System, release 6.1 or later.</td>
</tr>
<tr>
<td>VMware ESX virtual host</td>
<td>4.0 or 4.1</td>
</tr>
<tr>
<td></td>
<td>5.0 or 5.5</td>
</tr>
<tr>
<td>VMware Tools</td>
<td>Same version as VMware ESX software</td>
</tr>
<tr>
<td><strong>Note:</strong> Hypervisor support is limited to the supported OS.</td>
<td></td>
</tr>
<tr>
<td>VM login credentials</td>
<td>Host IP address where the DPM VMI is installed</td>
</tr>
<tr>
<td></td>
<td>vCenter server Hyper-V Server host login username and password</td>
</tr>
<tr>
<td></td>
<td>HTTPS communications port to the DPM VMI</td>
</tr>
</tbody>
</table>
Hyper-V Support for DPM Description

Oracle FS 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 and later 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

<table>
<thead>
<tr>
<th>Legend</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DPM VMI Service</td>
</tr>
<tr>
<td>2</td>
<td>Windows 2008 R2 or later server with Hyper-V enabled</td>
</tr>
<tr>
<td>3</td>
<td>Oracle FS System</td>
</tr>
<tr>
<td>4</td>
<td>Virtual Machine guest running DPM with any of the following applications:</td>
</tr>
<tr>
<td></td>
<td>• SQL database</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Exchange</td>
</tr>
<tr>
<td>6</td>
<td>DPM VMI API calls</td>
</tr>
<tr>
<td>7</td>
<td>HyperV/Windows service and Oracle FS System access</td>
</tr>
<tr>
<td>8</td>
<td>WebCLI</td>
</tr>
<tr>
<td>9</td>
<td>Mapped LUN information</td>
</tr>
<tr>
<td>• Oracle database</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>5 Pass-through LUNs access</td>
<td>10 HBA</td>
</tr>
</tbody>
</table>

In the above illustration, a Windows 2008 R2 or later 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.

Related Links

*DPM Virtual Environment Overview*

*Run Data Protection Manager for the First Time*

*Install the DPM VMI Service*

*Download the Data Protection Manager Software*

*Download Utility Software*
CHAPTER 2

Install DPM

Software Installation Overview

The installation package for the Oracle FS Data Protection Manager (DPM) contains the files necessary to install the main program.

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 operating systems, 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 Links

Data Protection Manager Requirements
Download the Data Protection Manager Software
Download Utility Software
Install DPM for Windows
Install DPM for Linux
Install DPM for Solaris

Download the Data Protection Manager Software

Download Oracle FS Data Protection Manager (DPM) and any necessary utilities from Oracle Technical Network (OTN) so that you can install the software on a host.

Prerequisite: Access to Oracle Technical Network.

2. Navigate to Server and Storage Systems > SAN Storage > Downloads.
3. Locate the Data Protection Manager 3.5 for Solaris, Linux, and Windows software package.
4. Follow the online instructions to download the software.
Install DPM

Install DPM for Windows

Install Oracle FS Data Protection Manager by installing the software that you downloaded to your host system.

**Prerequisites:**
- You are logged in as administrator on the workstation.
- No previous versions of Data Protection Manager and Volume Shadow Copy Service (VSS) hardware provider exists on the system. Uninstall any previous version before installing a new version.

Java must be installed on the server with the Java Development Kit path configured in either the `JAVA_HOME` or `JRE_HOME` variables.

When you install DPM, the procedure also installs VSS hardware provider.

1. Locate the downloaded DPM installation package on your system and decompress the file to a folder.

   **Note:** The filename for the DPM installation package is `DPM_n.n.n.zip`, where `n` is the version number such as `3.5.0`.

2. Run the `ofsdpm_win_n.n.n.exe`, where `n` is the version number such as `3.5.0`, to install the program.

   **Note:** Oracle recommends accepting the default installation folder location.

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

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

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

**Related Links**
- Software Installation Overview
- Download Utility Software
- Install DPM for Windows
- Install DPM for Linux
- Install DPM for Solaris

---

Install DPM

Install Oracle FS Data Protection Manager by installing the software that you downloaded to your host system.

**Prerequisites:**
- You are logged in as administrator on the workstation.
- No previous versions of Data Protection Manager and Volume Shadow Copy Service (VSS) hardware provider exists on the system. Uninstall any previous version before installing a new version.

Java must be installed on the server with the Java Development Kit path configured in either the `JAVA_HOME` or `JRE_HOME` variables.

When you install DPM, the procedure also installs VSS hardware provider.

1. Locate the downloaded DPM installation package on your system and decompress the file to a folder.

   **Note:** The filename for the DPM installation package is `DPM_n.n.n.zip`, where `n` is the version number such as `3.5.0`.

2. Run the `ofsdpm_win_n.n.n.exe`, where `n` is the version number such as `3.5.0`, to install the program.

   **Note:** Oracle recommends accepting the default installation folder location.

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

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

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

**Related Links**
- Software Installation Overview
- Download the Data Protection Manager Software
Install DPM for Linux

You can install the Oracle FS 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.
- Java must be installed on the server with the Java Development Kit path configured in either the `JAVA_HOME` or `JRE_HOME` variables.

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.
   ```
   
   Data Protection Manager installs to the default directory, which is shown below:

   ```
   $/Applications/System Tools/Oracle FS System Data Protection Manager
   ```

3. Set the security permissions to the DPM executable file to restrict access to Data Protection Manager to only authorized personnel.
   For example:
   ```
   $ chmod -744 "/opt/ofsdpm/bin/runHostAgentManager.sh"
   ```

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

**Related Links**

*Software Installation Overview*

*Download the Data Protection Manager Software*

Install DPM for Solaris

You can install the Oracle FS Data Protection Manager package on Solaris Sparc or Solaris Intel architectures.

**Prerequisite:** Java must be installed on the server with the Java Development Kit path configured in either the `JAVA_HOME` or `JRE_HOME` variables.

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.
   
   ```bash
   $ pkgadd -d InstallPackageName
   ```

   Data Protection Manager installs to the default directory which is shown below:

   ```
   $/Applications/Utilities/Oracle FS System Data Protection Manager
   ```

3. Set the security permissions to the DPM executable file to restrict access to Data Protection Manager to only authorized personnel. For example:
   
   ```bash
   $ chmod -744 "/opt/ofsdpm/bin/runHostAgentManager.sh"
   ```

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

**Related Links**

- [Software Installation Overview](#)
- [Download the Data Protection Manager Software](#)

**Install the DPM VMI Service**

When installing Oracle FS 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
  ```

- Java must be installed on the server with the Java Development Kit path configured in either the \( \text{JAVA\_HOME} \) or \( \text{JRE\_HOME} \) variables.

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:** Oracle recommends 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**.

   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 Links**

- Hyper-V Support for DPM Description
- DPM Virtual Environment Overview
- Run Data Protection Manager for the First Time
- Download the Data Protection Manager Software
- Download Utility Software

---

**Data Protection Manager Security Overview**

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

The DPM software:

- Prevents passwords from being displayed in clear text within the GUI or command line.
- Stores passwords in an internal database and secures the data with a customer-supplied encryption key.
- Enables an administrator to set an encryption key during the initial startup or change when required.
- Transmits data over a secure socket layer (SSL).

**Related Links**

- 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 Oracle FS 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 or an encryption key was not created yet. The encryption key is a character string the user defines and enters once. The user does not need to re-enter the encryption key. The encryption key ensures that DPM does not encrypt data using a standard value which would be identical across all systems.

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

The system displays the Update Encryption Key dialog.

3 From the Update Encryption Key dialog, enter the key, then click Submit.
   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 Oracle FS System Manager (GUI) overview page.

Related Links
DPM Virtual Environment Overview
Data Protection Manager Security Overview
Set the Data Protection Manager Encryption Key
Download the Data Protection Manager Software
Install the DPM VMI Service

Set the Data Protection Manager Encryption Key

You can set the Oracle FS Data Protection Manager (DPM) encryption key at any time. When a new key is created, data is re-encrypted using that encryption key.

1 From the Manager menu, click Update Encryption Key.
2 From the Update Encryption Key dialog box, type an encryption value, then click OK. You must type a minimum of one character. Though there
are no additional data entry requirements for the encryption value you should follow the security policies established by your corporation. DPM stores the key and uses the key to encrypt and decrypt data.

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

**Note:** The encryption key is stored in the same database that stores other DPM information; DPM maintains this database. If the database is deleted, all data is lost and DPM starts as if from a new installation. Existing checkpoints and persistence rules are lost. The database is not intended to be manually changed by the user.

**Related Links**

*Data Protection Manager Security Overview*
*Run Data Protection Manager for the First Time*

**Modify Virtual Machine Credentials**

Update the virtual machine login credentials for the Oracle FS 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**.

   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.
Accessing DPM Overview

You can run Oracle FS 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. 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. If a service is busy, such as a scheduled checkpoint is starting, this can cause a delay in the GUI being refreshed.

For example, if you create a schedule using the CLI, that schedule may not immediately appear in the GUI. Oracle recommends that you refresh the GUI. If the schedule does not appear in the GUI, then restart the GUI DPM application to display any objects created with the CLI.

Start the DPM GUI

After you have set the encryption key and default environment, you can start the Oracle FS Data Protection Manager GUI to perform tasks.

1. Log in to the computer where DPM is installed.
2. Launch the DPM application.
   - For Windows, navigate to Start > All Programs > Oracle Corporation > Oracle Flash Storage Data Protection Manager > Oracle Flash Storage Data Protection Manager.
   - For Linux, navigate to Applications > System Tools > Oracle Flash Storage Data Protection Manager.
   - For Solaris, navigate to Applications > Utilities > Oracle Flash Storage Data Protection Manager.
The Data Protection Manager GUI opens the Oracle FS System Manager (GUI) overview page, or the page you visited when you last logged off.

**Related Links**

*Software Installation Overview*

*Download the Data Protection Manager Software*

**DPM CLI Description**

The Oracle FS Data Protection Manager (DPM) provides a command-line interface called the `ofsdpmcli`. The `ofsdpmcli` enables you to configure and manage DPM functions on the command line or through custom scripts.

Information on how to access and run DPM CLI commands is provided in this document; this section describes the CLI features.

Below are listed some of the features 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 Oracle FS System 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.
### Configure Storage System Access Overview

To create and manage checkpoints, you must grant permission to the Oracle FS Data Protection Manager (DPM) so the application can access the Oracle FS System or Oracle Axiom system.

DPM lists each Oracle FS System or Oracle Axiom system that is accessible from the host. DPM discovers the Oracle FS System or Oracle Axiom system using either SCSI inquiries (real systems) or DPM VMI queries (VMs). In the VM case, it is the DPM VMI, running on the VM server (either HyperV or VMWare) that provides the information.

Initially, DPM displays the Oracle FS System 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 Oracle FS System or Oracle 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 Oracle FS System or Oracle Axiom system.

You can set the **Oracle Storage System Access Enabled** option and enter the storage system credentials from the **Configure Oracle Storage System Access** option. Setting the storage system access option enables you to view applications and consistency group LUNs on the storage system.

The **Clear Storage System Access** option removes the login credentials to any Oracle FS System or Oracle Axiom system. Clearing the login credentials causes DPM to lose visibility to the applications and consistency group LUNs that reside on the storage system. Reinstate the credentials by using the **Configure Oracle Storage System Access** option.

### Related Links

- **Configure Oracle Storage Systems Access Page**
- **Oracle Storage Systems Overview Page**
- **Configure Storage System Access**
- **Clear Oracle Storage System Access**
- **Refresh the List of Oracle Storage Systems**
Configure Storage System Access

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

**Prerequisite:** Oracle recommends that you create a unique Oracle FS System or Oracle Axiom system user account, with an Administrator 1 role, that is used only with DPM. The reason for this is if this user account, for DPM, becomes locked out of the Oracle FS System, this does not affect the ability to manage the Oracle FS System.

1. From the DPM left navigation pane, click **Oracle Storage Systems**.
2. From the Oracle Storage Systems overview page, select the name of an Oracle FS System or Oracle Axiom system to access.
3. Select **Actions > Configure Oracle Storage System Access**.
4. To enable DPM access to the Oracle FS System or Oracle Axiom system, select the **Oracle Storage System Access Enabled** option.
   
   **Note:** Selecting Oracle Storage System Access Enabled allows you to view applications and consistency group LUNs on the Oracle FS System or Oracle Axiom system.

5. Type the **Login name** for accessing the Oracle FS System or Oracle Axiom system.
6. Type the **Password** for accessing the Oracle FS System or Oracle Axiom system.
7. To save the settings, click **OK**.

**Related Links**

- [Configure Storage System Access Overview](#)
- [Configure Oracle Storage Systems Access Page](#)
- [Oracle Storage Systems Overview Page](#)
- [Clear Oracle Storage System Access](#)
- [Refresh the List of Oracle Storage Systems](#)

Clear Oracle Storage System Access

You can remove the Oracle FS System or Oracle Axiom system login credentials that the Oracle FS Data Protection Manager (DPM) uses.

1. From the DPM left navigation pane, click **Oracle Storage Systems**.
2. From the Oracle Storage Systems overview page, select the name of a Oracle FS System or Oracle Axiom system.
3. Select **Actions > Clear Storage System Access** to remove login information.
4. Click **OK**.
Refresh the List of Oracle Storage Systems

You can update the list of Oracle FS System or Oracle Axiom systems that are connected to the Oracle FS Data Protection Manager (DPM).

When DPM starts, the program automatically updates the list of available Oracle FS System or Oracle 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 Oracle Storage Systems.
2. Click OK.
   A list of connected Oracle FS System or Oracle Axiom systems appears on the page.

Related Links
Configure Storage System Access Overview
Configure Oracle Storage Systems Access Page
Oracle Storage Systems Overview Page
Configure Storage System Access
Refresh the List of Oracle Storage Systems
CHAPTER 3

Manage Checkpoints

Application Consistency Groups Overview

When you log into Oracle FS Data Protection Manager (DPM) that has access to the connected Oracle FS System or Oracle 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 databases (formerly known as storage groups)
- Microsoft SQL Server database instances
- Oracle database instances
- Oracle Automatic Storage management (ASM) disk groups

**Note:** Microsoft removed the use of Storage Groups from Microsoft Exchange 2010 Server and later. Microsoft Exchange Servers 2003 and 2007 still group databases (mailboxes) into Storage Groups, which DPM backs up for those applications. The best practice is to place a single database (mailbox) per Storage Group. With Microsoft Exchange 2010 Server and later, there are just Databases (mailboxes) which are displayed as the databases for Microsoft Exchange 2010 and 2013 Server versions.


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 Links

Applications Overview Page
Oracle Storage Systems Overview Page
Oracle Database Requirements
Oracle Automatic Storage Management Requirements
View Consistency Group, Oracle Databases Tab
Restore Checkpoint Dialog
View Consistency Group Details
Refresh the List of Oracle Storage Systems

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 Oracle FS 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 backup. 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 an Oracle FS System or Oracle 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 Oracle FS System or Oracle 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 Links

Verify a Consistency Group
View Consistency Group Details

You can review the details of a selected consistency group. For example, if the group consistency 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.
4. From the View Consistency Group dialog, click the available tabs to review the consistency group details.
5. When finished, click Close.

Related Links
- 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
- Microsoft SQL and Exchange 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.
4. Review the information on the dialog and then click OK.

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

Related Links
- Application Consistency Groups Overview
- LUN Configuration for Data Consistency
- Verify Consistency Group Dialog
- Refresh Applications
- Hide a Consistency Group
- Set the Oracle Database Username
**Hide a Consistency Group**

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

**Prerequisite:** There cannot be an existing checkpoint or schedule for a consistency group that you want to hide. If you need to hide a consistency group, you must remove any checkpoint or schedule first.

1. From the left navigation pane, click **Applications**.
2. From the Applications page, select a consistency group from the list.
3. Select **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 Links**

- [Application Consistency Groups Overview](#)
- [Applications Overview Page](#)
- [Refresh Applications](#)

**Set the Oracle Database Username**

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

**Prerequisites:** The consistency group status must be one of the following:

- Username required
- Set Oracle Username
- Invalid Username
- You need the Oracle database user name which is the operating system user id with administrator privileges for the database.

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. Select **Actions > Manage Consistency Group > Set Oracle Database Username**.
   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 Links**

- Application Consistency Groups Overview
- 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.

**Prerequisites:**

- The consistency group or application status must be the following:
  - ASM Credentials Required
- You need the ASM user name which is the operating system user id with administrator privileges for ASM.

The database login is only applicable for Solaris and Linux operating systems.

If ASM is managing more than one Oracle database, Oracle FS 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. Select **Actions > Set ASM Username**. 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 Links**

- Application Consistency Groups Overview
- Oracle Automatic Storage Management Requirements
- Oracle Database 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 Oracle FS 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. Select Actions > Refresh Applications.
3. Click OK.

Related Links
Microsoft SQL and Exchange Resources
Applications Overview Page
Microsoft SharePoint Database Requirements
Verify a Consistency Group
Hide a Consistency Group

Checkpoints Overview

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

Creating a checkpoint instructs Oracle FS Data Protection Manager to create Clone LUNs of the specified consistency group, 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, Oracle recommends 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 Links**
- Checkpoint Schedules Overview
- Checkpoint Retention Policy Overview
- Restore Checkpoint Dialog
- 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. Select **Actions > Plan Checkpoint**.
4. (Optional) If you want the checkpoint to override the default consistency group retention policy, select **Permanent**.
5. (Optional) From the Plan Checkpoint dialog, enter a description for the schedule in the **Description** field.
   **Note:** If you are scheduling checkpoints, this field is used for all checkpoints created by the schedule.
6. (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.
7. 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 Links
Checkpoints Overview
Transportable Checkpoints Overview
Applications Overview Page
Checkpoints 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. Select Actions > View Checkpoint.
4. Review the information listed in the Checkpoint tab.
5. Click the Clone LUNs tab.
   A list of Clone LUNs created for the checkpoint appears.
6. Click Close when you are finished reviewing the information.

Related Links
Checkpoints Overview
Modify Checkpoint Dialog
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. Select Actions > Modify Checkpoint.
4. Type a new description in the Description field.
5. To save the change, click OK.

Related Links
Checkpoints Overview
Checkpoint Retention Policy Overview
Modify Checkpoint Dialog
Delete Checkpoints

Deleting a checkpoint removes the checkpoint Clone LUNs from the Oracle FS System or Oracle 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. For example, if you set the maximum checkpoint retention policy to 1, then only one checkpoint is saved. You can adjust the policy to determine how many checkpoints you want to keep before deletion.

1. From the left navigation pane, click **Checkpoints**.
2. In the Checkpoints list, select the checkpoint that you want to delete.
3. Select **Actions > Delete Checkpoint**.
   The Delete dialog appears prompting you to confirm the deletion of the checkpoint.
4. When prompted to delete the checkpoint, click **Yes**.
   The Oracle FS System or Oracle Axiom system removes the Clone LUNs that are associated with the checkpoint.

**Related Links**

*Checkpoint Retention Policy Overview*
*Set Retention Policy Dialog*

Transportable Checkpoints Overview

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 Oracle FS 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 Oracle FS System. You can import the Clone LUNs of a transportable checkpoint to a host if that host is connected to the Oracle FS 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 dependent 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 2008 server or Windows 2008 R2 server with 32-bit or 64-bit architecture can be imported on a target host of the same OS of any architecture.

• Transportable checkpoints that are created on a Windows 2012 server or Windows 2012 R2 server with 32-bit or 64-bit architecture can be imported on a target host of the same OS of any architecture.


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 communicates with the same Oracle FS System or Oracle 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 Links
Import Transportable Checkpoint, Import Checkpoint Dialog
Import Transportable Checkpoint, Mount Snapshots Dialog
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 Oracle FS 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
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 Links**
- Transportable Checkpoints Overview
- Checkpoints Overview
- Import Transportable Checkpoint, Import Checkpoint Dialog
- Import Transportable Checkpoint, Mount Snapshots 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 Backup Document 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.

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 Links
Transportable Checkpoints Overview
Checkpoints Overview
Import Transportable Checkpoint, Import Checkpoint Dialog
Import Transportable Checkpoint, Mount Snapshots Dialog

Restoring Checkpoints Overview

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

Restoring from a checkpoint reverts a consistency group to a particular point-in-time. The restore process uses the Clone LUNs on the Oracle FS System or Oracle Axiom system to restore the LUNs. For more information about restoring a LUN from a Clone LUN, refer to the Oracle Flash Storage System 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 Oracle FS System or Oracle Axiom system.

When restoring a checkpoint for an Oracle database, the Oracle database must be in the open state for DPM to restore a checkpoint. In the open state, DPM can restore (recover) data to a point-in-time snapshot of the database. DPM communicates with the database to ensure that the database is stopped, dismounted, and LUNs are restored. After the LUNs are restored, the database is remounted, the state is changed from backup mode, which is the state of the database during the backup, and opened using auto recovery. The database is then left in the online state.

For Windows-based systems, Microsoft Volume Shadow Copy Service (VSS) manages the consistency group during checkpoint restore process. When the restore process completes, the consistency group is brought back online and, if necessary, the restored data is verified.

Note: For Microsoft Exchange Server 2013, a checkpoint restore can fail for consistency groups due to an inability to lock the underlying volume. This failures displays as an event with this message:
Generating Operation Exclusive Volume Access
To resolved this issue, you need to stop the Microsoft Exchange Search Host Controller service. In addition, if the Microsoft Exchange 2013 Server has Database Availability Groups (DAG) enabled, it can be necessary to also stop the
Microsoft Exchange Replication service while the checkpoint restore is in process. Both services can be restarted after the restore process is complete.

**Related Links**
- Checkpoints Overview
- 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. Select **Actions > Restore**.
4. To restore the checkpoint, click **OK**.

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

**Related Links**
- Restoring Checkpoints Overview
- Restore Checkpoint Dialog

**Checkpoint Retention Policy Overview**

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 Oracle FS System. Refer to the *Oracle Flash Storage System 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 Links**
- Checkpoint Schedules Overview
- Checkpoints Overview
- Applications Overview Page
- Checkpoints Overview Page
- Set Retention Policy Dialog
- Create an Immediate Checkpoint
- Plan and Create 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 Oracle FS 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. Select **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.
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. Select Actions > Modify Checkpoint.
4. Select the Permanent option.
5. To save the change, click OK.
Chapter 4

Manage Checkpoint Schedules

Checkpoint Schedules Overview

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 Oracle FS 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 Links

- Checkpoints Overview
- Checkpoint Retention Policy Overview
- Schedules Overview Page
- Display All Checkpoint Schedules
- Plan and Create a Checkpoint Schedule
- Modify a Checkpoint Schedule
- Refresh All Checkpoint Schedules
Plan and Create a Checkpoint Schedule

You can plan 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
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:** You can only schedule your checkpoint start time to no more than three weeks in the future. DPM does not allow schedules to be created for further out than three weeks from the current date.
9. To close the calendar dialog, click OK.
10. Select a frequency for your schedule. Valid frequencies include:
    - Hourly
    - Daily
    - Weekly
11. Select 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. Your schedule is listed on the Schedules overview page.
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. Select 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) Select a new frequency for your schedule.
8. (Optional) Select 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 Links
Checkpoint Schedules Overview
Modify Checkpoint Dialog
Plan and Create a Checkpoint Schedule
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. Select 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 Links
Checkpoint Schedules Overview
View Checkpoint Schedule Dialog
Plan and Create a Checkpoint Schedule

Refresh All Checkpoint Schedules

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

1. From the left navigation pane, click Schedules.
2. Select Action > Refresh Schedules.
   The system updates the list of available schedules and provides the latest status.

Related Links
Checkpoint Schedules Overview
Modify 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. Select Actions > Delete Schedule.
4. When prompted to confirm the deletion, click OK.

Related Links
Checkpoint Schedules Overview
Modify Schedule Dialog
Display All Checkpoint Schedules

You can view a list of checkpoint schedules for the Oracle FS 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 correct.

Related Links
- Checkpoint Schedules Overview
- Schedules Overview Page
- Plan and Create a Checkpoint Schedule
- Display All Checkpoint Schedules
Data Protection Manager Events Overview

Oracle FS Data Protection Manager (DPM) records in the event log significant events that are related to both the program and the operating system. DPM does not log events in the Oracle FS System 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 Oracle FS 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 Links
- Checkpoints Overview
- Checkpoint Schedules Overview
- Events Overview Page
- Display All Events
- 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 Oracle FS Data Protection Manager.

1. From the left navigation pane, click Events.
2. Review the event details to ensure that the information is correct.
Refresh the List of Events

Under normal conditions, the Oracle FS 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. Select **Actions** > **Refresh Events**.
3. Review the list of events to ensure that the information is correct.

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. Select **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**.
Applications Overview Page

Enables you to review the applications that are used with Oracle FS Data Protection Manager (DPM) to manage checkpoints. The Applications overview page also provides status information about existing checkpoints. Options accessed from this page enable 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 statuses are:

**ASM Credentials Required**  Indicates that DPM requires an Oracle ASM login credential to display additional database information. This is the operating system user id with administrator privileges for ASM

**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.
| **Oracle Storage Systems Access Required** | Indicates that DPM requires the Oracle FS System or Oracle 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 Oracle FS System or Oracle Axiom system. Sharing LUNs across consistency groups is not a DPM best practice for configuring applications on the system. |
| **Multiple Storage Systems** | Indicates that the consistency group uses LUNs from more than one Oracle FS System or Oracle Axiom system. |
| **Non-Oracle Storage System LUNs** | Indicates that the consistency group contains LUNs that do not reside on a Oracle FS System or Oracle 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. This is the operating system user id with administrator privileges for the database. |
| **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.
- **Ready to Restore**: Indicates that the checkpoint is ready to be restored.
- **Restoring**: Indicates that DPM is restoring the Clone LUNs that represent the checkpoint.

**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 Links
- Application Consistency Groups Overview
- Checkpoints Overview
- Transportable Checkpoints Overview
- LUN Configuration for Data Consistency
- LUN Configuration for Applications
- Microsoft SQL and Exchange Resources
- Create an Immediate Checkpoint
- Plan and Create a Checkpoint Schedule

Oracle Storage Systems Overview Page

Allows you to view the connection and access status for the Oracle FS System and Oracle Axiom that are visible and managed by the Oracle FS Data Protection Manager (DPM). Options on this page allow you to enable access and to provide the login credentials to the Oracle FS System and Oracle Axiom.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Number</td>
<td>Identifies the Oracle FS System or Oracle Axiom system serial number. Serial numbers for Oracle Axiom systems begin with A00; serial numbers for Oracle FS System begin with A99.</td>
</tr>
<tr>
<td>Connected</td>
<td>Indicates whether the Oracle FS System or Oracle Axiom system is physically connected to the host.</td>
</tr>
<tr>
<td>Oracle Storage Systems Access Enabled</td>
<td>Indicates whether the Oracle FS System or Oracle Axiom system is managed by DPM. To enable or disable access to the Oracle FS System or Oracle Axiom system, use the Actions menu. Access to the Oracle FS System or Oracle Axiom requires login credentials.</td>
</tr>
<tr>
<td>Login Name</td>
<td>Identifies the username that can be used to access and manage the Oracle FS System or Oracle Axiom system. This account must have Administrator 1 or Administrator 2 privileges to create and manage Clone LUNs. Refer to the Oracle Flash Storage System Administrator’s Guide. Oracle recommends to create and use a specific administrator account to manage DPM and not the primary administrator account used to manage the storage system.</td>
</tr>
</tbody>
</table>

Related Links
- Configure Storage System Access Overview
- Application Consistency Groups Overview
- Configure Storage System Access
- Clear Oracle Storage System Access
- Refresh the List of Oracle Storage Systems
- View Consistency Group Details
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 Links
- Checkpoints Overview
- Transportable Checkpoints Overview
- Create an Immediate Checkpoint
- Plan and Create a Checkpoint Schedule

Configure Oracle Storage Systems Access Page

Enables you to enter the Oracle FS System or Oracle Axiom system login name and password which are needed by Oracle FS Data Protection Manager (DPM) for access to LUNs used by the managed applications.

**Login Name**
Identifies the username that can be used to access and manage the Oracle FS System or Oracle Axiom system. This account must have Administrator 1 or Administrator 2 privileges to create and
manage Clone LUNs. Refer to the *Oracle Flash Storage System Administrator’s Guide*.

**Password**
Identifies the Oracle FS System or Oracle Axiom system login password that is associated with the user account that was entered for Login Name. Passwords are case sensitive. Blank passwords are not permitted.

**Oracle Storage Systems Access Enabled**
Specifies whether to allow DPM to have access to the Oracle FS System or Oracle Axiom system LUNs that are used by the managed applications.

Valid access options:

**Enabled**
Indicates that DPM has permission to access the Oracle FS System or Oracle 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 Oracle FS System or Oracle 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 Links**
- Configure Storage System Access Overview
- Configure Storage System Access
- Clear Oracle Storage System Access
- Refresh the List of Oracle Storage Systems

**Events Overview Page**
Allows you to review entries in the Oracle FS Data Protection Manager (DPM) 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 and deletes the oldest events when DPM reaches 4032 events.
**Type**
Displays the severity level of the entries in the Oracle FS System 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 Links**

*Data Protection Manager Events Overview*
*Display All Events*
*View Event Details*
*Refresh the List of Events*

**Import Transportable Checkpoint, Import Checkpoint Dialog**

Enables 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.
Import Transportable Checkpoint, Mount Snapshots 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 to a specific 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 on the source system for diagnostic purposes, 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.
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 Links

Checkpoints Overview
Checkpoint Retention Policy Overview
Modify a Checkpoint Description
Make a Checkpoint Permanent

Modify Schedule Dialog

Enables 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 6: Schedule recurrence intervals

<table>
<thead>
<tr>
<th>Recurrence interval</th>
<th>Valid values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hourly</td>
<td>1 through 24</td>
</tr>
<tr>
<td>Daily</td>
<td>1 through 7</td>
</tr>
<tr>
<td>Weekly</td>
<td>1 through 52</td>
</tr>
</tbody>
</table>

Permanent  
Identifies whether the checkpoint overrides the retention policy.

Related Links
Checkpoint Schedules Overview
Modify a Checkpoint Schedule
Refresh All Checkpoint Schedules

Modify Virtual Machine Server Credentials Dialog (Step 1)
Enables 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 enables you to modify the existing information.

Related Links
DPM Virtual Environment Overview
Modify Virtual Machine Credentials

Modify Virtual Machine Server Credentials Dialog (Step 2)
Enables 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 Links
DPM Virtual Environment Overview
Modify Virtual Machine Credentials

Plan Checkpoint, Checkpoint Tab
Enables 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**
Enables 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 the Transportable Checkpoint option.

**Related Links**
- [Checkpoint Schedules Overview](#)
- [Plan and Create a Checkpoint Schedule](#)
- [Display All Checkpoint Schedules](#)
- [Delete a Checkpoint Schedule](#)

## Plan Checkpoint, Schedule Tab
Enables you to create a checkpoint schedule. You can create the schedule and not enable it, if desired. Oracle FS Data Protection Manager (DPM) 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 tab.
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 Links
*Checkpoint Schedules Overview*
*Plan and Create a Checkpoint Schedule*
*Display All Checkpoint Schedules*
*Delete a Checkpoint Schedule*

**Restore Checkpoint Dialog**

Allows you to restore 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 Overview and the Checkpoint Overview pages is displayed as **restoring**. When the system completes the checkpoint restoration, Oracle FS Data Protection Manager updates the Events Overview 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 Links**
- Restoring Checkpoints Overview
- Restore a Checkpoint

**Schedules Overview Page**
Enables you to review a summary of the Oracle FS 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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Identifies the name of the scheduled operation.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Identifies whether the schedule is enabled.</td>
</tr>
<tr>
<td></td>
<td>Valid states:</td>
</tr>
<tr>
<td>Yes</td>
<td>Indicates that the schedule is active.</td>
</tr>
<tr>
<td>No</td>
<td>Indicates that the schedule is inactive.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Identifies the time and date that Oracle FS Data Protection Manager is scheduled to start a scheduled job.</td>
</tr>
<tr>
<td>Next Run Time</td>
<td>Identifies the time and date of the next scheduled job.</td>
</tr>
<tr>
<td>Frequency</td>
<td>Specifies the frequency by which the scheduled operation runs.</td>
</tr>
<tr>
<td></td>
<td>Examples include:</td>
</tr>
<tr>
<td></td>
<td>• Every 12 hours</td>
</tr>
<tr>
<td></td>
<td>• Every 2 days</td>
</tr>
<tr>
<td></td>
<td>• Every 4 weeks</td>
</tr>
<tr>
<td>Applies To</td>
<td>Identifies the name of the application or consistency group to which the schedule applies.</td>
</tr>
</tbody>
</table>

**Related Links**
- Checkpoint Schedules Overview
- Plan and Create a Checkpoint Schedule
- Display All Checkpoint Schedules
- Delete a Checkpoint Schedule
Set Retention Policy Dialog

Enables you to configure the retention policy for all checkpoints that are associated with the selected application consistency group. Setting a retention policy determines how long checkpoints are stored on the storage system.

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 Links
- Checkpoint Retention Policy Overview
- Set a Checkpoint Retention Policy
- Make a Checkpoint Permanent
- Delete Checkpoints

Verify Consistency Group Dialog

Enables you to make the consistency group available to Oracle FS 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 Oracle FS System or Oracle Axiom system.

**LUN Device Name** Identifies the LUN name that was assigned by the operating system.

**Related Links**
- Application Consistency Groups Overview
- Checkpoints Overview
- Checkpoint Schedules Overview
- Create an Immediate Checkpoint Plan and Create a Checkpoint Schedule

**View Checkpoint, Checkpoint Tab**
Enables 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 Links

Checkpoints Overview
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 Oracle FS 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 Oracle FS System.

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

Related Links

Checkpoints Overview
View Checkpoint Details

View Checkpoint Schedule Dialog

Enables 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 Links**

- *Checkpoint Schedules Overview*
- *View a Checkpoint Schedule*

**View Consistency Group, Consistency Group Tab**

Enables you to review the details of the Oracle FS Data Protection Manager (DPM) application consistency group.

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

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

**Note:** Microsoft removed the use of Storage Groups from Microsoft Exchange 2010 Server and later. Microsoft Exchange Servers 2003 and 2007 still group databases (mailboxes) into Storage Groups, which DPM backs up for those applications. The best practice is to place a single database (mailbox) per Storage Group. With Microsoft Exchange 2010 Server and later, there are just Databases (mailboxes) which are displayed as the databases for Microsoft Exchange 2010 and 2013 Server versions.


**Name**

Identifies the name of the consistency group.
<table>
<thead>
<tr>
<th><strong>Consistency Group ID</strong></th>
<th>Displays the consistency group unique identifier.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Consistency Status</strong></td>
<td>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 statuses are:</td>
</tr>
</tbody>
</table>

| **ASM Credentials Required** | Indicates that DPM requires an Oracle ASM login credential to display additional database information. This is the operating system user id with administrator privileges for ASM. |
| **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. |
| **Oracle Storage Systems Access Required** | Indicates that DPM requires the Oracle FS System or Oracle 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 Oracle FS System or Oracle Axiom system. Sharing LUNs across consistency groups is not a DPM best practice for configuring applications on the system. |
| **Multiple Storage Systems** | Indicates that the consistency group uses LUNs from more than one Oracle FS System or Oracle Axiom system. |
### Non-Oracle Storage System LUNs
Indicates that the consistency group contains LUNs that do not reside on an Oracle FS System or Oracle 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. This is the operating system user id with administrator privileges for the database.

## Checkpoint Status
Identifies the status of the checkpoint.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating</td>
<td>Indicates that DPM is creating checkpoints from the consistency group.</td>
</tr>
<tr>
<td>Deleting</td>
<td>Indicates that DPM is removing checkpoints from the consistency group.</td>
</tr>
<tr>
<td>Ready to Restore</td>
<td>Indicates that DPM can create checkpoints from the consistency group.</td>
</tr>
<tr>
<td>Not Restorable</td>
<td>Indicates that the checkpoint contains consistency errors that prevents DPM from restoring the checkpoint.</td>
</tr>
<tr>
<td>Restoring</td>
<td>Indicates that DPM is restoring the consistency group from a checkpoint.</td>
</tr>
<tr>
<td>Unknown</td>
<td>Indicates that DPM cannot determine the checkpoint status.</td>
</tr>
</tbody>
</table>

## 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 Links
View Consistency Group Details
Refresh Applications

View Consistency Group, LUNs Tab
Enables 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 Oracle FS 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 Oracle FS System or Oracle Axiom system.

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

Related Links
View Consistency Group Details
Refresh Applications

View Consistency Group, Schedules Tab
Enables 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 Links
View Consistency Group Details
Refresh Applications

View Consistency Group, Retention Policy Tab
Enables 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 retained 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 Links
View Consistency Group Details
Refresh Applications

View Consistency Group, Oracle Databases Tab
Enables 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 disk group.

**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 Links**
- Application Consistency Groups Overview
- Oracle Database Requirements
- Oracle Automatic Storage Management Requirements
- Applications Overview Page
- View Consistency Group Details
- Refresh Applications
- Set the Oracle Database Username
- Set the ASM Username

**View Event Properties Dialog**
Enables 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 Oracle FS System 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 Links
Data Protection Manager Events Overview
Display All Events
View Event Details
Refresh the List of Events
DPM CLI Command Reference

DPM CLI Commands Overview

Oracle FS Data Protection Manager installs with a command line interface (CLI) utility called the 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, 10/11/2014 01:02:03 PM specifies a date of 3 seconds after 1:02 PM, October 11, 2014.

**Related Links**

- *Software Installation Overview*
- *DPM CLI Supported Platforms*
- *help*
- *Issue an ofsdpmcli Command for Windows*
- *Issue an ofsdpmcli Command for Solaris and Linux*
DPM CLI Supported Platforms

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

Table 7: DPM CLI supported platforms

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Required version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Microsoft Windows Server 2008 (32 and 64 bit)</td>
</tr>
<tr>
<td></td>
<td>Microsoft Windows Server 2008, R2 (32 and 64 bit)</td>
</tr>
<tr>
<td></td>
<td>Microsoft Windows Server 2012</td>
</tr>
<tr>
<td></td>
<td>Microsoft Windows Server 2012 R2</td>
</tr>
<tr>
<td>Solaris</td>
<td>Solaris Sparc 10 U10 (32 and 64 bit) and higher</td>
</tr>
<tr>
<td></td>
<td>Solaris 11 and higher (64 bit)</td>
</tr>
<tr>
<td>Linux</td>
<td>Oracle Linux 5.8 and higher</td>
</tr>
<tr>
<td></td>
<td>Oracle Linux 6.2 and higher</td>
</tr>
<tr>
<td></td>
<td>Red Hat Enterprise Linux 7.0 and higher</td>
</tr>
</tbody>
</table>

Related Links

*DPM CLI Commands Overview*

Set the DPM Encryption Key for CLI

Set or update the encryption key for the Oracle FS Data Protection Manager (DPM) to ensure secure transactions with the Oracle FS System.

1. Open a command console.
2. Change directories to the DPM installation folder.
3. Set the encryption key.

```
$ ofsdpmcli settings -setEncryptionKey encryptionKey
```

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

Issue an ofsdpmcli Command for Windows

The DPM CLI utility is installed with the Oracle FS Data Protection Manager product. You issue ofsdpmcli 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\Oracle FS System Data Protection Manager”

3. Issue a DPM CLI command.

   To see a list of the available subcommands, issue the following command:
C: \> ofsdpmcli
The CLI displays a list of all of the available subcommands and their options.

Related Links
DPM CLI Commands Overview
Issue an ofsdpmcli Command for Solaris and Linux

Issue an ofsdpmcli Command for Solaris and Linux
The DPM CLI utility is installed with the Oracle FS Data Protection Manager product. You issue ofsdpmcli commands for the CLI from a console window.

Prerequisite: The ofsdpmid service must be running for DPM CLI commands to be run.

DPM commands can be issued on Oracle Linux, Red Hat Enterprise Linux, and Solaris operating systems.

1. Open a command console window.
2. From the command prompt, change directories to the installation folder.
   
   chdir DPMInstallFolder/bin
   
   The DPMInstallFolder variable is the directory path to the Data Protection Manager files.
3. Launch the ofsdpmcli program.
   
   $ /opt/ofsdpm/bin/ofsdpmcli
4. Issue a DPM CLI command.

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

   $ ofsdpmcli
   
   The CLI displays a list of all of the available subcommands and their options.

Related Links
DPM CLI Commands Overview
Issue an ofsdpmcli Command for Windows

**application**

Lists all of the available applications that are managed by Oracle FS Data Protection Manager.

**SYNOPSIS**

ofsdpmcli application -help
ofsdpmcli application -list [-details]
[-application applicationIdentifier [-options]]
DESCRIPTION
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.

SUBCOMMANDS
- **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:

    ```
    $ ofsdpmcli 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.

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

Results:

Oracle FS Systems Data Protection Manager - CLI v3.5.0

Restore Checkpoint Options:

```xml
<data />
```

Import Checkpoint Options:

```xml
<data />
```

Create Checkpoint Options:

```xml
<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>
```

```xml
<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>

</data>

Related Links

checkpoint
event

system

Manages the Oracle FS System that is connected to the Oracle FS Data Protection Manager (DPM).

SYNOPSIS

ofsdpmcli system -help

ofsdpmcli system -list [-details] [-oraclefs serialNumber]

ofsdpmcli system -modify-system serialNumber -username username

[-isManaged {true | false}]

ofsdpmcli system -delete -system serialNumber

DESCRIPTION

Manages the Oracle FS System that is connected to the Oracle FS Data Protection Manager (DPM).

Use the system subcommand to perform any of the following actions:

- List the details of the specified Oracle FS System or Oracle Axiom system that is managed by DMP.
- Change the login credentials for the specified Oracle FS System or Oracle Axiom system.
• Remove the login credentials for the specified Oracle FS System or Oracle 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 Oracle FS System or Oracle 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 Oracle FS System or Oracle Axiom system. You can set the -isManaged parameter and provide the oraclefs credentials. Setting the -isManaged option allows DPM to display applications and consistency group LUNs that belong to the Oracle FS System or Oracle Axiom system.

**SUBCOMMANDS**

- **-help** Displays the system subcommand help documentation.
- **-list** Displays a list of Oracle FS System or Oracle Axiom system that are managed by DPM.
  
  Valid options:

  - **-details** Provides additional details about the Oracle FS System or Oracle Axiom system
  - **-system** Specifies the Oracle FS System or Oracle Axiom system for which you want to list information.

- **-modify** Modifies and stores the Oracle FS System or Oracle Axiom system administrative login credentials that are managed by DPM.
  
  Valid options:

  - **-system** Specifies the serial number of the Oracle FS System or Oracle Axiom system that you want to modify.
  - **-username** Specifies the new user name to use with the Oracle FS System or Oracle Axiom system. The ofsdpmcli prompts you for the password to manage the Oracle FS System.
  - **-isManaged** Specifies whether DPM displays applications and consistency group LUNs of the Oracle FS System or Oracle Axiom system.
  
  Valid options:

  - **true** Indicates that the applications, checkpoints, and consistency groups that belong to the Oracle FS System or Oracle
Axiom system are managed by DPM.

false Indicates that the applications, checkpoints, and consistency groups that belong to the Oracle FS System or Oracle Axiom system are not managed by DPM.

-delete Clears the Oracle FS System or Oracle 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 Oracle FS System or Oracle Axiom system. Reinstate the credentials by using the system-modify command.

Valid options:

-system Specifies the Oracle FS System or Oracle Axiom from which you want to remove system administrative credentials from DPM. This prevents DPM from accessing the system.

EXAMPLE

Run the system command to display the details of a managed Oracle FS System or Oracle Axiom system.

$ ofsdpmcli system -list -system A001650XYZ

Results:

Oracle FS System Data Protection Manager - CLI v3.5.0
<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 Links

application

checkpoint

Manages checkpoints on Oracle FS Data Protection Manager (DPM).

SYNOPSIS

ofsdpmcli checkpoint -help

ofsdpmcli checkpoint -create-id consistencyGroupOrAppIdentifier [-application] [-description description] [-permanent {true | false}] [-optionName1:value,optionName2:value,...]

ofsdpmcli checkpoint -list [-checkpoint checkpointIdentifier] [-details]

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

ofsdpmcli checkpoint -delete-checkpoint checkpointIdentifier

ofsdpmcli checkpoint -restore [-checkpoint checkpointIdentifier] [-optionName1:value,optionName2:value,...]

ofsdpmcli checkpoint -import-file absolutePathToFile [-options optionName1:value, optionName2:value,...]

ofsdpmcli checkpoint -mount-file absolutePathToFile [-snapshots snapshotId1:mountPoint1, snapshotId2:mountPoint2,...]

DESCRIPTION

Manages checkpoints on Oracle FS 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 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.
SUBCOMMANDS

- **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 consistencygroup or application parameter, which specifies the identifier of the consistency group or application. Obtain the value by issuing one of the following commands:
    - `$ ofsdpmcli consistencygroup-list`
      Use the guid value that is returned by the CLI.
    - `$ ofsdpmcli 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:

  - `$ ofsdpmcli application -list -application associatedApplicationId -options`
  - `$ ofsdpmcli consistencgroup -list -consistencygroup guid -options`

  **-list** 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:

```
$ ofsdpmcli 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:

  ```
  $ ofsdpmcli 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:
  
  ```
  $ ofsdpmcli 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 Oracle FS System or Oracle Axiom system to restore the LUNs. For more information about restoring a LUN from a Clone LUN, refer to the *Oracle Flash Storage System 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 Oracle FS System or Oracle Axiom system.

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:
  
  ```
  $ ofsdpmcli 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:
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 Oracle FS System. You can import the Clone LUNs of a transportable checkpoint to a host if that host is connected to the Oracle FS 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 dependent 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 2008 server or Windows 2008 R2 server with 32-bit or 64-bit architecture can be imported on a target host of the same OS of any architecture.

- Transportable checkpoints that are created on a Windows 2012 server or Windows 2012 R2 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:

- `$ ofsdpmcli application-list -application associatedApplicationId -options`
- `$ ofsdpmcli consistencgroup-list -consistencygroup guid -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.

```
$ ofsdpmcli 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.

```
$ ofsdpmcli checkpoint -list
```

```
Oracle FS System Data Protection Manager - CLI v3.5.0
<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 />n
      </member>
      <member>
        <name>timestamp</name>
        <value>03/29/2014 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>3/30/2014 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>CLI Checkpoint 4</value>
      </member>
      <member>
        <name>guid</name>
        <value>{7FBC98C3-B4FA-AE6277BE065E}</value>
      </member>
      <member>
        <name>name</name>
        <value />n
      </member>
      <member>
        <name>timestamp</name>
        <value>3/30/2014 3:04:39 PM</value>
      </member>
    </struct>
  </value>
</data>
```
Related Links
application
consistencygroup
event
schedule

**consistencygroup**

Manages the consistency groups on Oracle FS Data Protection Manager (DPM).

**SYNOPSIS**

ofsdpmcli consistencygroup -help

ofsdpmcli consistencygroup -list [-details] [-showDiscovered] [-consistencygroup consistencyGroupIdentifier]

ofsdpmcli consistencygroup -hide -consistencygroup consistencyGroupIdentifier

ofsdpmcli consistencygroup -unhide -consistencygroup consistencyGroupIdentifier

ofsdpmcli consistencygroup -verify -consistencygroup consistencyGroupIdentifier

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

**DESCRIPTION**

Manages the consistency groups on Oracle FS Data Protection Manager (DPM).
Use the `consistencygroup` subcommand to perform any of the following actions:

- List consistency groups visible to 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.

**SUBCOMMANDS**

- **-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 consistency group, 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 `consistencyGroupId` identifier. To obtain the `consistencyGroupId` value issue the following command:

    ```
    $ ofsdpmcli consistencygroup-list.
    ```

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

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

- **-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 `consistencyGroupId` identifier. To obtain the `consistencyGroupId` value issue the following command:

    ```
    $ ofsdpmcli consistencygroup-list.
    ```

    Use the `guid` 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:

  ```bash
  $ ofsdpmcli consistencygroup-list.
  
  Use the `guid` value that is returned by the CLI.
  
-verify Verifies that DPM displays the Consistency Group that was configured for the application instance or Consistency Group.

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:

  ```bash
  $ ofsdpmcli consistencygroup-list.
  
  Use the `guid` 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:

  ```bash
  $ ofsdpmcli consistencygroup-list.
  
  Use the `guid` value that is returned by the CLI.

-username Specifies the user name of the managed consistency group. The ofsdpmcli 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 Oracle FS System. Refer to the Oracle Flash Storage System 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:
Use the guid 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.

```
$ ofsdpmcli consistencygroup -list -showDiscovered
```

Results:

```
Oracle FS System 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>
    </struct>
  </value>
</data>
```
<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>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>
Related Links
application
checkpoint
event

dpvmvi

Manages the virtual machine interface (VMI) connection for Oracle FS Data Protection Manager (DPM).

SYNOPSIS
ofsdpmcli dpvmvi -help
ofsdpmcli dpvmvi -add-ipAddress ipAddress-port port-username username
ofsdpmcli dpvmvi -list [-details] [-ipAddress ipAddress]
ofsdpmcli dpvmvi -modify-ipAddress ipAddress [-port port] [-username username]
ofsdpmcli dpvmvi -delete -ipAddress ipAddress

DESCRIPTION
Manages the virtual machine interface (VMI) connection for Oracle FS Data Protection Manager (DPM).

Use the dpvmvi 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.
### SUBCOMMANDS

- **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 Oracle FS System management interface. If the ESX host loses communication with an Oracle FS 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.

Within a virtualized environment, DPM communicates with DPMVMI, and then DPMVMI communicates with either the VMware vCenter Server or Hyper-V Server to obtain the responses required by DPM. Neither DPM nor the DPMVMI service communicates directly with the ESX Hosts.
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 the VMI 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.

Once a VMI service is removed, DPM cannot complete any tasks until another VMI service is registered. Only one VMI service can be registered with 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.

```bash
$ ofsdpmcli dmpvmi -list
```

Results:

```
Oracle FS Systems Data Protection Manager - CLI v3.5.0
<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 Links**

- **event**
- **settings**
event

Displays system events that occur with Oracle FS Data Protection Manager (DPM).

SYNOPSIS

ofsdpmcli event -help

ofsdpmcli event -list [-timestamp timestamp] [-details] [-event eventNumber]

DESCRIPTION

Displays system events that occur with Oracle FS 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

SUBCOMMANDS

-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.

```bash
$ ofsdpmcli event -list -event 41
```

Results:

Oracle FS Systems Data Protection Manager - CLI v3.5.0
<data>
<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>
```
Related Links
application
checkpoint
consistencygroup
dpmvmi
schedule

help

Displays a list of all supported Oracle FS Data Protection Manager (DPM) subcommands and options. The -help subcommand also provides detailed information about a specific subcommand.

SYNOPSIS
ofsdpmcli -help
ofsdpmcli command-name -help

DESCRIPTION
Displays a list of all supported Oracle FS Data Protection Manager (DPM) subcommands and options. The -help subcommand also provides detailed information about a specific subcommand.

The syntax conventions used for ofsdpmcli 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 ofsdpmcli commands for ease of reading. Entering commands is not case-sensitive. You can use either camel case or lowercase.
SUBCOMMANDS

Help is available for the following commands:

• application
• consistencygroup
• checkpoint
• dpmvmi
• event
• schedule
• settings
• system

EXAMPLE

Use the help command to display a list of all ofsdpmcli commands and options.

$ ofsdpmcli help

Results:
Oracle FS System Data Protection Manager - CLI v3.5.0
No Parameters Given.
Application Usage:
    application -help
    application -list
        [-details]
        [-application applicationIdentifier [-options]]

System Usage:
    System -help
    System -list
        [-details]
        [-system serialNumber]
    System -modify
        -system serialNumber
        -username username
        [-isManaged {true|false}]
    System -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
schedule

Manages Oracle FS Data Protection Manager (DPM) checkpoint schedules to be performed in the future during specified intervals.

SYNOPSIS

ofsdpmcli schedule -help

ofsdpmcli schedule -create[-application] -id consistencyGroupOrAppIdentifier -name scheduleName -begin beginTime -frequency frequency -recurrence recurrence [-permanent {true | false}] [-enabled {true | false}] [-recurrenceDays recurrenceDays] [-options optionName1:value,optionName2:value,...]

ofsdpmcli schedule -list -schedule scheduleIdentifier [-details]

ofsdpmcli schedule -modify -schedule scheduleIdentifier [-name scheduleName] [-begin beginTime] [-frequency frequency] [-recurrence recurrence] [-permanent {true | false}] [-enabled {true | false}]

Related Links

application
system
checkpoint
consistencygroup
dpmvmi
event
schedule
settings
ofsdpmcli schedule -delete -schedule scheduleIdentifier

DESCRIPTION
Manages Oracle FS 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

SUBCOMMANDS

- **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:

- $ ofsdpmcli application -list -application associatedApplicationId -options
- $ ofsdpmcli consistencgroup -list -consistencygroup guid -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 creates a checkpoint every two weeks from the Oracle application at 1:00 am every other Sunday.

```
$ ofsdpmcli schedule -create -id "Oracle (Need default name defined)" -application -begin "04/05/2014 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:

```
Oracle FS System Data Protection Manager - CLI v3.5.0
<data>
  <value>
    <struct>
      <member>
        <name>affectedObjectIdentifier</name>
        <value>Oracle database</value>
      </member>
      <member>
        <name>affectedObjectType</name>
        <value>Application</value>
      </member>
    </struct>
  </value>
```

<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 Links

* checkpoint
* consistencygroup

settings

Manages the host agent settings for Oracle FS Data Protection Manager (DPM).

**SYNOPSIS**

```
ofsdpmcli settings -help
ofsdpmcli settings -isEncryptionInitialized
ofsdpmcli settings -setEncryptionKey
ofsdpmcli settings -getEncryptionKey
ofsdpmcli settings -setVirtualStatus [true | false]
ofsdpmcli settings -getVirtualStatus
```
DESCRIPTION
Manages the host agent settings for Oracle FS 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
- Oracle FS System

SUBCOMMANDS
- -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 passkey 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.

$ ofsdpmcli settings -getVirtualStatus

Results:
Oracle FS System Data Protection Manager - CLI v3.5.0
<data>
  <value>
    <struct>
      <member>
        <name>isVirtual</name>
        <value>true</value>
      </member>
    </struct>
  </value>
</data>

Related Links

system
dpmvmi
event
Index

A
accessing DPM
   accessing CLI or GUI 32
   Data Protection Manager 32
description 32
Affected Object controls 82
application
description 85–87
application consistency groups, see consistency groups
application instance 15
applications
   configure LUNs for 16
   create checkpoints 43
   plan checkpoints 43
   refresh list 42
   set retention policy 50
   view consistency groups 39
Applications overview page
description 59
ASM, see automatic storage management (ASM).
ASM Credentials Required
   consistency status 59, 77
ASM instances
   set username 41
ASM Parameter File
   consistency status 59, 77
automatic storage management (ASM)
description 18
requirements 18
Axioms overview page
description 62

B
best practice resources 20

C
checkpoint
description 91, 92, 98
checkpoint schedules
   create 53
   delete 55
   modify 54
   plan 53
   view 55
checkpoints (continued)
description 42
   make permanent 51
   permanent 49, 102
   rename 44
   restore 49
   restore overview 48
   retention policy 43
   schedules 43
   set retention policy 50
   status 42
   status messages 60, 78
   transportable, see transportable checkpoints
   view details 44
   where to create 42
Checkpoints overview page
description 63
checkpoints, transportable, see transportable checkpoints
CLI
   operating systems supported 84
   platforms supported 84
command line interface
description 33
   issue commands for Solaris 85
   issue commands for Windows 84
   limitations 33
commands
   application 85–87
   checkpoint 91, 92, 98
   consistencygroup 99, 100, 103
dpmvmi 105, 106, 108
event 109, 110
help 111, 112
schedule 114, 115, 119
settings 120–122
system 88–90
configuration
   LUNs for applications 16
Configure Oracle Storage Systems Access page
field definitions 63
consistency
   about 38
   configuring LUNs for 38
   requirement 37
   status messages 59, 77
   tests for 38
consistency group
   setup credentials 101
consistency groups
   configure LUNs for 16
database instances 17
consistency groups (continued)
description 37
display details 39
Exchange Server storage groups 16
hide 40
SQL Server database instances 17
verify 39
view details 39
Consistency Status Unknown
description 60, 77
consistencygroup
description 99, 100, 103
hide 100
list 100
modify 102
unhide 101
verify 101
contact information 9
contacts, Oracle 9
conventions
command syntax 10
typographical 10
customer support 9

D
Data Protection Manager
access to systems 34
description 12
install for Linux 27
install for Solaris 27
install for Windows 26
requirements 13
run for the first time 30
start 32
Data Protection Manager host agent
install for Windows 26
Data Protection Manager software
description 25
database instance, see consistency groups
database requirements
Oracle 19
Database Shutdown
description status 60, 77
Delete
checkpoint status 61
display
checkpoints 44
consistency groups 39
event details 58
events 57
schedules 56
documentation
feedback 9
DPM
start up in virtual environment 21, 107
with virtual environment 20, 106
DPM security
description 29
DPM VMI
install for Hyper-V 28
install for vSphere 28
dpmvmi
create 106
delete 108
description 105, 106, 108
display 107
modify 107

E
education programs 9
encryption
description 29
encryption key
create 30
how to
update using CLI 84
ESX host 20, 106
event
description 109, 110
events
about 57
display 57
display details 58
examples of 57
how to
list 109
refresh list 58
update list 58
Events overview
field definitions 64
Exchange Server
storage groups 16

F
feedback, documentation 9
field definitions
Affected Object controls 82
Applications overview page 59
Axioms overview page 62
Checkpoints overview page 63
Configure Axiom Access page 63
Events overview 64
Import Transportable Checkpoint 65
Maximum Checkpoints Retention Policy controls 73, 80
Maximum Duration Retention Policy 73
Maximum Duration Retention Policy controls 80
Modify Checkpoint 66
Modify Checkpoint Schedule 67
Modify Virtual Machine Server Credentials 68
Mount Snapshot 66
View Consistency Group (continued)
  View Event Properties 81, 82

H
  help
    description 111, 112
  Hyper-V server 21, 106
  Hyper-V support
    description 23

I
  Import Transportable Checkpoint
    field definitions 65
  Invalid Username
    consistency status 60, 77
  isEncryptionInitialized
    determine 121

L
  Last checkpoint
    status 61
  login credentials
    administrative roles requirements 62, 63
    modify for virtual machine 31

M
  Maximum Checkpoints Retention Policy
    controls 80
    field definitions 73
  Maximum Duration Retention Policy
    controls 80
    field definitions 73
  Modify Checkpoint
    field definitions 66
  Modify Schedule
    field definitions 67
  Modify Virtual Machine Server Credentials
    field definitions 68
  Mount Snapshot
    field definitions 68
  Multiple Applications
    consistency status 60, 77
  Multiple storage systems
    consistency status 60, 77

N
  Non-Oracle Storage System LUNs
    consistency status 60, 78
  Not In Archivelog Mode
    consistency status 60, 78
  Not Verified
    consistency status 60, 78
transportable checkpoints (continued)
  stored information 45
  storing 45
 typographical conventions 10

U
Username Required
  consistency status 60, 78

V
vCenter server 21, 106
Verify Consistency Group
  field definitions 74
view
  event notification details 58
View Checkpoint
  field definitions
    Checkpoint tab 74
    Clone LUNs tab 75
View Checkpoint Schedule
  field definitions 75
View Consistency Group
  LUNs tab 79
View Event Properties
  field definitions 81
virtual environment
  DPM VMI 21, 106
  ESX host 20, 106
  Hyper-V server 21, 106
  start up 21, 107
  vCenter server 21, 106
  with DPM 20, 106
virtual machine
  requirements 22
  update login credentials 31
VMI
  install for Hyper-V 28
VSS Provider
  definition 14
  Plug-In 15