Oracle® Enterprise Manager

Oracle Exadata Database Machine Getting Started Guide

13c Release 3

F19101-01

June 2019

ORACLE®

Oracle Enterprise Manager Oracle Exadata Database Machine Getting Started Guide, 13c Release 3

F19101-01

Contents

Preface

What's New

1   Introduction to the Plug-in

5   Oracle Exadata Database Machine Administration

6   Virtualized Exadata Database Machine

7   Exadata Metrics

8   Troubleshooting the Exadata Plug-in

Index

Preface

Oracle Enterprise Manager provides the tools to effectively and efficiently manage your Oracle Exadata Database Machine. With a consolidated view of the Exadata Database Machine, Oracle Enterprise Manager provides a consolidated view of all the hardware components and their physical location with indications of status. Oracle Enterprise Manager also provides a software view of the databases residing on it and their resource consumption on compute node and Exadata Storage Cell.

This document provides the installation and administration instructions to set up Oracle Enterprise Manager to monitor and manage your Oracle Exadata Database Machine.

Audience

This system monitoring installation guide is for users who perform administrative and problem-resolution tasks on Oracle Exadata Database Machine.

Documentation Accessibility

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

Access to Oracle Support

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

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's Changed

This table provides a brief overview of the document changes for the latest publication of the *Oracle® Enterprise Manager Managing and Monitoring an Exadata Database Machine*:

Part Number	Change Summary
E56534-01	Updated for support of Enterprise Manager Cloud Control 13*c*.

What's New

The Oracle Exadata plug-in provides a consolidated view of the Exadata Database Machine within Oracle Enterprise Manager, including a consolidated view of all the hardware components and their physical location with indications of status.

This chapter highlights the significant features and enhancements provided by the Oracle Exadata plug-in in the following release summaries:

- Features and Enhancements for Oracle Exadata Plug-in 13.2.0.1.0

Features and Enhancements for Oracle Exadata Plug-in 13.2.0.1.0

Oracle Exadata Plug-in Release 13.2.0.1.0 includes a variety of bugs fixed and enhancements implemented for the following feature areas:

- Supported Hardware and Software Configurations — What's New for 13.2.0.1.0
- Exadata Virtualization Provisioning
- Support for Exadata Flash Cache Features
- Enhanced Exadata Hardware Management
- Patching Automation Support of the Exadata Stack
- ORAchk/EXAchk Integration
- Auto Service Request (ASR) Integration: Fault Telemetry
- Support for IPv6 Environments

Supported Hardware and Software Configurations — What's New for 13.2.0.1.0

As Oracle releases new hardware and software, the Oracle Exadata plug-in is updated, tested, and certified to accommodate the new products. For complete hardware and software support details, see Oracle Exadata Database Machine Supported Hardware and Software in Introduction to the Plug-in .

Oracle Exadata Plug-in Release 13.2.0.1.0 supports the following hardware and software:

- X6, including certification of Exadata Storage Server 12.1.2.3.1

    - X6–2

    - X6–8

Exadata Virtualization Provisioning

Provisioning involves repeatable, reliable, automated, unattended, and scheduled mass deployment of a RAC Cluster including virtual machines (VMs), Oracle Database (DB), Grid Infrastructure, and ASM on Virtualized Exadata.

With the Exadata plug-in's virtualization provisioning functionality, you can:

- Create and delete a RAC Cluster including VMs, Oracle Database (DB), Grid Infrastructure, and ASM.

- Scale up and scale down a RAC Cluster by adding or removing VMs including DB, Grid Infrastructure, and ASM.

See Exadata Virtualized Provisioning for the details.

Support for Exadata Flash Cache Features

The Exadata plug-in provides the following features in support of Exadata Flash Cache:

- Monitor "Extreme Flash" introduced from X5 onwards:

  - Enhanced Database Machine schematic diagram.

  - Enhanced incident details page for disk failure.

  - Enhanced capacity reporting, I/O Resource Management (IORM), and performance charts.

- Flash I/O Resource Monitoring and Management, including:

  - Flash Cache space usage monitoring.

  - Administration of flash IORM.

  - New charts on Cell and Grid home page and Performance page.

  - I/O Resource consumption and performance monitoring for Flash.

Enhanced Exadata Hardware Management

The Exadata plug-in has been enhanced to provide improved monitoring details for all Exadata Database Machine components, this is made possible via the System Infrastructure target type. These details include:

- ILOM overview details and health status.

- Updated the schematic diagram to enhanced views into your Exadata Database Machine, including:

  - Photo-realistic hardware view. From this view, administrators have visibility into hardware and can correlate errors across tools (like an intermittent error with Exadata performance).

  - Logical view, which shows additional CPU details and status.

  - Energy view.

  - Network connectivity.

  - Service processor (SP) configuration.

Patching Automation Support of the Exadata Stack

The Exadata plug-in support additional patching features in support of the entire Exadata stack, including:

- Compute nodes: Firmware and operating system (OS).

- Exadata Storage Server cells: Firmware and cell software.

- InfiniBand network: Switch firmware.

- Quarterly Full Stack Patch Download (QFSDP) is released every quarter. Primary components are:

  – Database (Database, Clusterware).

  – Infrastructure includes Exadata Storage Server, InfiniBand Switch, and PDU.

- Exadata systems patching includes:

  – Comprehensive overview of the maintenance status and needs.

  – Proactive patch recommendations for the quarterly full stack patches.

  – Supports auto patch download, ability to patch either in rolling or non-rolling modes.

  – Ability to schedule runs.

  – Proactive notification of the status updates.

  – Granular step-level status tracking with real-time updates.

  – Log monitoring and aggregation, supporting quick filing of support issues with pre-packaged log dumps.

For more details, see the following documents:

- *Updating Exadata Storage Servers* and *Updating Exadata InfiniBand Switches* in *Oracle® Enterprise Manager Lifecycle Management Administrator's Guide*.

- *Exadata Database Machine and Exadata Storage Server Supported Versions* (Doc ID 888828.1) in My Oracle Support:

  https://support.oracle.com/rs?type=doc&id=888828.1

ORAchk/EXAchk Integration

The ORAchk/EXAchk utility proactively scans for the most significant problems across the various layers within Oracle Database and Exadata Database Machine. The Exadata plug-in integrates the ORAchk/EXAchk utility and provides the following features through Enterprise Manager Cloud Control:

- Install, set up, upgrade, and schedule the ORAchk utility within Enterprise Manager.

- View all ORAchk/EXAchk results as Enterprise Manager Compliance Standard violations.

- Allows you to review and implement ORAchk/EXAchk best practices.

The ORAchk/EXAchk utility provides a comprehensive list of checks and alerts, including:

- Verify Disk Cache Policy on Database Server

- Verify Database Server disk controllers use writeback cache

- Verify RAID Controller Battery Condition (Database Server)

- Verify RAID Controller Battery Temperature (Database Server)

- Verify Database Server Virtual Drive Configuration

- Verify Database Server Physical Drive Configuration

- Imageinfo version comparison across database and storage servers

- Verify Hardware and Firmware on Database and Storage Servers (`CheckHWnFW-Profile`) (Database Server)

- Verify Software on Storage Servers (`CheckSWProfile.sh`)

- NFS Mount Point - Attribute Caching

- Verify `/conf/configvalid` File

- Backend Check

- ORAchk not running

- Results and Exception file(s) missing

- Metric Parsing Failed

For details about the ORAchk plug-in, see the ORAchk Healthchecks Plug-in Overview and Requirements in *Enterprise Manager ORAchk Healthchecks Plug-in User's Guide*.

Auto Service Request (ASR) Integration: Fault Telemetry

Oracle Auto Service Request (ASR) provides auto-case generation when common hardware component faults occur. ASR is designed to enable faster problem resolution by eliminating the need to initiate contact with Oracle Support Services for common hardware component failures, reducing both the number of phone calls needed and overall phone time required.

The Exadata plug-in integrates with Oracle ASR to provide the following benefits:

- Enables ASR capability for Exadata Database Machine. Creates a Service Request (SR) automatically and updates the SR number to Enterprise Manager.

- Installs and deploys quickly with the `emcli` command.

- Includes ASR Incidents for viewing within the Enterprise Manager Incident Manager.

- Works for all Engineered Systems that are certified for ASR.

Enterprise Manager recognizes the following three fault telemetry types:

- Integrated Lights Out Manager (ILOM): Provides fault information, power and environmental, CPU, and memory fault information from the service processor (SP).

- Exadata-detected Events (HALRT): Provides fault coverage for disks, flash, and PCI cards within Oracle Exadata Database Machine.

- Fault Management Architecture (FMA): Provides CPU and memory fault information from the host.

For more details about using Oracle ASR with Enterprise Manager, see Introduction to Oracle Auto Service Request (ASR) in *Enterprise Manager Managing and Monitoring Oracle Auto Service Request (ASR) Assets User's Guide*.

For product details about Oracle ASR, see `http://oracle.com/asr`.

Support for IPv6 Environments

The Oracle Exadata plug-in 13.2.0.1.0 now supports monitoring and management of all Exadata components using IPv6, except for InfiniBand Switches which use IPv4.

For details, see Enable Support for IPv6 Environments.

1

Introduction to the Plug-in

This chapterchapter provides a general overview of the Oracle Exadata plug-in, including supported hardware and software. The following topics are discussed:

- Oracle Exadata Plug-in Features
- Oracle Exadata Database Machine Supported Hardware and Software

Oracle Exadata Plug-in Features

Highlights of the Oracle Exadata plug-in release 13.1.0.0.0 include the following features:

- Monitoring and Notification Features
- Hardware Support Features
- Exadata Software Support
- Target Discovery Features
- Exadata Storage Server Grid Home Page and Server Home Page Features
- Exadata Performance Page Features
- Exadata Metrics Features

Monitoring and Notification Features

With the Oracle Exadata plug-in, you can monitor Exadata targets through Enterprise Manager Cloud Control 13*c*. The plug-in provides seamless integration with supported Exadata software so that you can receive notification on any Exadata target. Features include:

- Monitoring of the Exadata Database Machine as an Enterprise Manager target.
- Monitoring of the Exadata target, including the Exadata Cell, within Enterprise Manager's I/O Resource Management (IORM) feature.
- Support SNMP notification for Exadata cell.
- Support dashboard report creation from Enterprise Manager Cloud Control, including a simplified configuration of the service dashboard.
- Support of client network hostnames for compute nodes.
- Enhanced InfiniBand network fault detection and InfiniBand schematic port state reporting.
- Modification of Enterprise Manager monitoring agents as needed for all Exadata Database Machine components.
- IORM for multi-tenancy database (CDB/PDB) environment:
    - CDB-level I/O Workload Summary with PDB-level details breakdown.

– I/O Resource Management for Oracle Database 12*c*.

– Exadata Database Machine-level physical visualization of I/O Utilization for CDB and PDB on each Exadata Storage Server.

– Integration link to Database Resource Management UI.

• Support discovery of locked down storage servers.

Hardware Support Features

You can use the Oracle Exadata plug-in to optimize the performance of a wide variety of Exadata targets, including:

• Oracle SuperCluster, including:

– Versions: SuperCluster V1.1, V1.0.0 + October Quarterly Maintenance Update (QMU)

– Configurations:

* LDOM: Control domain, IO/guest domain

* Zone: Global, non-global

– Discover, monitor, and manage Exadata Database Machine-related components residing on SuperCluster Engineering System

– See Oracle SuperCluster Support - Exadata Plug-in Release 12.1.0.4.0 and Later for more details.

• Multi-Rack support:

– Supports discovery use cases: Initial discovery, add a rack

– Side-by-side rack schematic

• Support for Storage Expansion Rack hardware.

• Full partition support:

– Logical splitting of an Exadata Database Machine Rack into multiple Database Machines.

– Each partition is defined through a single OneCommand deployment.

– Compute nodes are not shared between partitions.

– Multiple partitions connected through the same InfiniBand network.

– Compute nodes in same partition share the same Cluster.

– Ability to specify a customized DBM name during discovery of the target.

– User can confirm and select individual components for each DBM.

– Flexibility to select "small-p" targets for individual partitions.

– Flexibility to select some or all of the InfiniBand switch as part of monitored network, including the ability to add switches post discovery.

– Flexibility to select some or all of the Cells to be shared among Exadata Database Machines.

• Support for the increasing types of Exadata Database Machine targets. See Oracle Exadata Database Machine Supported Hardware and Software for a complete list of supported hardware.

- InfiniBand Switch Sensor fault detection, including power supply unit sensors and fan presence sensors.
- Support for on-demand refresh of InfiniBand schematic.

Exadata Software Support

Through the Oracle Enterprise Manager Cloud Control interface, you can use the Oracle Exadata plug-in to access Exadata Storage Software functionality to efficiently manage your Exadata hardware. Support includes:

- Integration with Exadata Storage Software.
- Support for the latest Exadata Server Versions 12.1.2.3.1 and earlier:
  - 11.2.3.3.1 or earlier.
  - A plug-in that supports 12.1.1.1.0 and beyond will have support for Oracle database 12*c*.
  - 12.1.2.1.0.
  - 12.1.2.1.1.
  - 12.1.2.1.1 release and patch 2024004. See Doc ID 1959143.1 in My Oracle Support:

    https://support.oracle.com/rs?type=doc&id=1959143.1

  - 12.1.1.1.2.
  - 12.1.1.1.2 release and patch 20699031. See Doc ID 1995937.1 in My Oracle Support:

    https://support.oracle.com/rs?type=doc&id=1995937.1

  - 12.1.2.2.0. See Doc ID 2038073.1 in My Oracle Support for details:

    https://support.oracle.com/rs?type=doc&id=2038073.1

  - 12.1.2.3.0. See Doc ID 2031447.1 in My Oracle Support for details:

    https://support.oracle.com/rs?type=doc&id=2031447.1

> **Note:**
>
> For latest supported configurations please refer to Doc ID 1626579.1 in My Oracle Support

Target Discovery Features

The target discovery process is streamlined and simplified with the Oracle Exadata plug-in. Features include:

- Automatically push the Exadata plug-in to agent during discovery.

- Discovery prerequisite checks updates, including:
  - Check for critical configuration requirements.
  - Check to ensure either `databasemachine.xml` or `catalog.xml` files exist and are readable.
  - Prevent discovered targets from being rediscovered.
- Credential validation and named credential support.
- Ability to apply a custom name to the Exadata target.
- Support enabled for discovery using the client access network.
- Automate SNMP notification setup for Exadata Storage Server and InfiniBand Switches.
- Support discovery of compute nodes with client network host names.
- Support discovery using the new `catalog.xml` file generated from the OEDA Java-based Configurator.
- Additional credential validation and named credential support.
- Support customization of Exadata Database Machine name.
- Support discovery of locked down storage servers.

> **Note:**
>
> Exadata Database Machine targets are configured with OOB default thresholds for the metrics. No additional template is provided by Oracle.

Exadata Storage Server Grid Home Page and Server Home Page Features

The Exadata Storage Server Grid home page and Server home page provides the following features:

- Provides a fine-grained performance summary for flash and hard disk.
- Provides new usage statistics to highlight flash cache and Smart Scan efficiency.
- Provides a new, detailed summary of flash space usage.
- Provides new metrics for:
  - I/O time distribution by flash and hard disk.
  - IORM wait per database.

Exadata Performance Page Features

The Performance home page provides the following features:

- Side-by-side comparison of flash and hard disk performance.
- Performance comparison between multiple Exadata Storage Servers.

- Performance utilization for flash and hard disk to identify workload reaching hardware limit.
- Provides Exadata Storage Server performance charts to help with diagnosing performance issues when I/O reaching hardware limits.

Exadata Metrics Features

Metrics reports are critical to manage your Oracle Exadata Database Machine effectively. With the metrics, you can determine where additional resources are needed, when peak usage times occur, and so forth.

- Enhanced metric scalability in large environment to reduce time out by reducing `cellcli` calls.
- Reduce metric collection error for the Exadata HCA metric. Improvements to combine the HCA port data collection in a single `cellcli` call to reduce chances of time out.
- Reduced metric collection error from Exadata IORM Status metric. The metric was removed, and the user interface now uses the available configuration data.

Oracle Exadata Database Machine Supported Hardware and Software

The following sections describe the supported hardware and software by the Oracle Exadata plug-in:

- Exadata Database Machine Configuration Support
- Oracle SuperCluster Support - Exadata Plug-in Release 12.1.0.4.0 and Later
- Supported Component Versions
- Supported Operating Systems
- Oracle Exadata Database Machine Hardware Not Supported

Exadata Database Machine Configuration Support

Enterprise Manager Cloud Control 13*c* is supported on the following Exadata Database Machine configurations:

- Supported Exadata Database Machine Types
- Multi-Rack Support
- Partitioned Support

> ✎ **Note:**
>
> Unless otherwise noted, support is provided for all versions of Oracle Exadata plug-in Release 13.1.

Supported Exadata Database Machine Types

The following Exadata Database Machine types are supported:

- V2

  > **Note:**
  >
  > V2 machines discovered in Enterprise Manager Cloud Control 12*c* are still supported in 13*c*. However, discovery of V2 machines in Enterprise Manager Cloud Control 13*c* is not supported.

- X2
    - X2-2: Full rack, half rack, and quarter rack
    - X2-8: Full rack
- X3
    - X3-2: Full rack, half rack, quarter rack, and eighth rack (requires release 12.1.0.3 or higher)
    - X3-8: Full rack
- X4
    - X4-2
- X5
    - X5-8
- X6
    - X6–2
    - X6–8
- Oracle SuperCluster, including (requires release 12.1.0.4 or higher):
    - Support for Oracle SuperCluster V1.1 on LDOM and Zone (Global & Non-Global)
    - Support for Oracle SuperCluster V1.0.1 with October QMU on LDOM and Zone

Multi-Rack Support

Enterprise Manager supports managing multiple connected racks of Oracle Database Machine of the supported machine types listed above (Supported Exadata Database Machine Types). Also, the following two racks can be monitored in a multi-rack as these cannot exist as a standalone single rack:

- Storage Expansion Rack (requires release 12.1.0.4 or higher)
- Compute Node Expansion Rack (requires release 12.1.0.4 or higher)

Partitioned Support

The following partitioned configurations are supported:

- Partitioned Exadata Database Machine - the logical splitting of a Database Machine Rack into multiple Database Machines. The partitioned Exadata Database Machine configuration must meet the following conditions to be fully supported by Enterprise Manager Cloud Control 13*c*:

  - Each partition is defined through a single OneCommand deployment.

  - Cells and compute nodes are not shared between partitions.

  - Multiple partitions are connected through the same InfiniBand network.

  - Compute nodes in same partition share the same Cluster.

  The expected behavior of a partitioned Exadata Database Machine includes:

  For Oracle Exadata plug-in Release **12.1.0.3.0 and later**:

  - The target names for the Exadata Database Machine, Exadata Grid, and InfiniBand Network will be generated automatically during discovery (for example, Database Machine `dbm1.mydomain.com`, Database Machine `dbm1.mydomain.com_2`, Database Machine `dbm1.mydomain.com_3`, etc.). **However, users can change these target names at the last step of discovery.**

  - All InfiniBand switches in the Exadata Database Machine must be selected during discovery of the first Database Machine partition. They will be included in all subsequent Database Machine targets of the other partitions. The KVM, PDU, and Cisco switches can be individually selected for the DB Machine target of each partition.

  - User can confirm and select individual components for each Database Machine.

  For Oracle Exadata plug-in Release **12.1.0.2.0 and earlier**:

  - The target names for the Exadata Database Machine, Exadata Grid, and InfiniBand Network will be generated automatically during discovery (for example, Database Machine `dbm1.mydomain.com`, Database Machine `dbm1.mydomain.com_2`, Database Machine `dbm1.mydomain.com_3`, etc.). **Users cannot specify these target names.**

  - All shared components (such as, KVM, PDU, Cisco switch, and InfiniBand switches) must be selected during discovery of the first Database Machine partition. They will be included in all subsequent Database Machine targets of the other partitions.

  - User can confirm and select individual components for each Database Machine.

Oracle SuperCluster Support - Exadata Plug-in Release 12.1.0.4.0 and Later

Only Oracle SuperCluster with software Version 1.1 with DB Domain on Control LDOM-only environments are supported. Earlier versions of Oracle SuperCluster can be made compatible if you update to the October 2012 QMU release. You can confirm this requirement by looking at the version of the `compmon pkg` installed on the system

(using either `pkg info compmon` or `pkg list compmon` commands to check). You must have the following minimum version of compmon installed:

```
pkg://exa-family/system/platform/exadata/comp-
mon@0.5.11,5.11-0.1.0.11:20120726T024158Z
```

The following **hardware configurations** are supported:

- Oracle SuperCluster:

  – T5-8 server

  – T4-4 server

The following **software configurations** are supported:

- LDOM

  – Control Domain

  – IO/Guest Domain

- Zone

  – Global

  – Non-Global

The following **software versions** are supported:

- Oracle SuperCluster V1.1

- Oracle SuperCluster V1.0.1 + October QMU

The following issues have been fixed for the 12.1.0.4.0 release of the Oracle Exadata plug-in:

- **Exadata Storage Server monitoring:** If multiple DB clusters share the same Exadata Storage Server, in one Enterprise Manager management server environment, you can discover and monitor the first DB Machine target and all its components. Also, for additional DB Machine targets sharing the same Exadata Storage Server, the Oracle Exadata Storage Server Grid system and the Oracle Database Exadata Storage Server System will now show all Exadata Storage Server members.

  This issue reported in the plug-in's 12.1.0.3.0 release has been fixed in 12.1.0.4.0.

- **HCA port error monitoring:** If the `perfquery` command installed in the Oracle SuperCluster has version 1.5.8 or later, a bug (ID 15919339) was reported where most columns in the HCA Port Errors metric in the host targets for the compute nodes will be blank.

  If there are errors occurring on the HCA ports, it is now reported in Enterprise Manager.

  To check your version, run the following command:

  ```
  $ perfquery -V
  ```

  This issue reported in the plug-in's 12.1.0.3.0 release has been fixed in 12.1.0.4.0.

Oracle SuperCluster Known Issues

The following known issues have been reported for the Oracle SuperCluster:

- PAGE13 is empty in the `/opt/oracle.SupportTools/onecommand/catalog.xml` file. This issue prevents Enterprise Manager from displaying the schematic diagram on the Database Machine home page. (Bug 16719172)

  Workaround: Manually replace the PAGE13 section by the one listed below:

```
<PAGE13>
  <RACKS>
    <RACK ID="0">
      <MACHINE TYPE="203"/>
      <ITEM ID="1">
          <TYPE>ibs</TYPE>
          <ULOC>1</ULOC>
          <HEIGHT>1</HEIGHT>
      </ITEM>
      <ITEM ID="2">
          <TYPE>cell</TYPE>
          <ULOC>2</ULOC>
          <HEIGHT>2</HEIGHT>
      </ITEM>
      <ITEM ID="3">
          <TYPE>cell</TYPE>
          <ULOC>4</ULOC>
          <HEIGHT>2</HEIGHT>
      </ITEM>
      <ITEM ID="4">
          <TYPE>cell</TYPE>
          <ULOC>6</ULOC>
          <HEIGHT>2</HEIGHT>
      </ITEM>
      <ITEM ID="5">
          <TYPE>cell</TYPE>
          <ULOC>8</ULOC>
          <HEIGHT>2</HEIGHT>
      </ITEM>
      <ITEM ID="6">
          <TYPE>comp</TYPE>
          <ULOC>10</ULOC>
          <HEIGHT>8</HEIGHT>
      </ITEM>
      <ITEM ID="7">
          <TYPE>ibl</TYPE>
          <ULOC>18</ULOC>
          <HEIGHT>1</HEIGHT>
      </ITEM>
      <ITEM ID="8">
          <TYPE>cisco</TYPE>
          <ULOC>19</ULOC>
          <HEIGHT>1</HEIGHT>
      </ITEM>
      <ITEM ID="9">
          <TYPE>zfs</TYPE>
          <ULOC>20</ULOC>
          <HEIGHT>4</HEIGHT>
      </ITEM>
      <ITEM ID="10">
          <TYPE>ibl</TYPE>
          <ULOC>24</ULOC>
          <HEIGHT>1</HEIGHT>
      </ITEM>
      <ITEM ID="11">
```

```
            <TYPE>head</TYPE>
            <ULOC>25</ULOC>
            <HEIGHT>1</HEIGHT>
        </ITEM>
        <ITEM ID="12">
            <TYPE>head</TYPE>
            <ULOC>26</ULOC>
            <HEIGHT>1</HEIGHT>
        </ITEM>
        <ITEM ID="13">
            <TYPE>comp</TYPE>
            <ULOC>27</ULOC>
            <HEIGHT>8</HEIGHT>
        </ITEM>
        <ITEM ID="14">
            <TYPE>cell</TYPE>
            <ULOC>35</ULOC>
            <HEIGHT>2</HEIGHT>
        </ITEM>
        <ITEM ID="15">
            <TYPE>cell</TYPE>
            <ULOC>37</ULOC>
            <HEIGHT>2</HEIGHT>
        </ITEM>
        <ITEM ID="16">
            <TYPE>cell</TYPE>
            <ULOC>39</ULOC>
            <HEIGHT>2</HEIGHT>
        </ITEM>
        <ITEM ID="17">
            <TYPE>cell</TYPE>
            <ULOC>41</ULOC>
            <HEIGHT>2</HEIGHT>
        </ITEM>
        <ITEM ID="18">
            <TYPE>pdu</TYPE>
            <ULOC>0</ULOC>
            <HEIGHT>0</HEIGHT>
        </ITEM>
        <ITEM ID="19">
            <TYPE>pdu</TYPE>
            <ULOC>0</ULOC>
            <HEIGHT>0</HEIGHT>
        </ITEM>
      </RACK>
    </RACKS>
  </PAGE13>
```

- The Assert OK power sensor raises a critical alert in Enterprise Manager. (Bug 17445054)

> **Note:**
>
> This bug does not apply to X3-2 and X4-2 machines.

- Wrong machine names in the `databasemachine.xml` file. When the database is installed in a local zone on a Oracle SuperCluster T5-8, the `databasemachine.xml`

file ends up with the machine name of the global zone rather than that of the local zone that the database is installed into.

Workaround: Manually edit the file to change the hostnames for the database nodes to those of the zone name.

(Bug 17582197)

- In Enterprise Manager, the Schematic & Resource Utilization report will display only one LDOM per server.

- Enterprise Manager will not report hard disk predictive failure on compute node in an Oracle SuperCluster environment.

- The pre-requisite check script `exadataDiscoveryPreCheck.pl` that is bundled in Exadata plug-in 12.1.0.3.0 does not support the `catalog.xml` file. Please download the latest `exadataDiscoveryPreCheck.pl` file from My Oracle Support as described in Download the Discovery Precheck Script.

- On the Oracle SuperCluster Zone while deploying the Management Agent, the agent prerequisite check may fail with the following error:

> **✎ Note:**
>
> The error can be ignored and you can continue to proceed with installation of the Management Agent.

```
@ During the agent install, the prereq check failed:
@
@ Performing check for CheckHostName
@ Is the host name valid?
@ Expected result: Should be a Valid Host Name.
@ Actual Result: abc12345678
@ Check complete. The overall result of this check is: Failed <<<<
@
@ Check complete: Failed <<<<
@ Problem: The host name specified for the installation or retrieved from the
@ system is incorrect.
@ Recommendation: Ensure that your host name meets the following conditions:
@ (1) Does NOT contain localhost.localdomain.
@ (2) Does NOT contain any IP address.
@ (3) Ensure that the /ect/hosts file has the host details in the following
@ format.
@ <IP address> <host.domain> <short hostname>
@
@ If you do not have the permission to edit the /etc/hosts file,
@ then while invoking the installer pass the host name using the
@ argument
@ ORACLE_HOSTNAME.
```

Supported Component Versions

Table 1-1 shows the component versions supported by the Oracle Exadata plug-in Release 12.1:

Table 1-1   Supported Component Versions

Component	Firmware/Software Versions	Exadata Plug-in Version Support
Storage Server	12.1.2.3.1, 12.1.2.3.0, 12.1.2.2.2 or below	13.1.0.0.0 , 12.1.0.6.0
		✐ Note: EM 12c PS3 is tested with Exadata Server Software 12.1.2.2.0. SSH Lock down will not be a supported configuration under 12c PS3/PS4, however, it is certified to work with 13c.
	11.2.3.3.0	12.1.0.6.0 and later
	12.1.1.1.0	12.1.0.5.0 with following patches applied (not cell related): • Agent platform: Patch ID 17872949 • OMS plug-in: Patch ID 17861041 • Agent plug-in: Patch ID 17965602
	11.2.3.2.1.130109	12.1.0.4.0 and later
	11.2.3.2.0.120713	12.1.0.3.0 and later
	11.2.2.3.0 11.2.2.3.2 11.2.2.3.5 11.2.2.4 11.2.3.1.0 11.2.3.1.1	All versions
InfiniBand Switch	2.1.3-4 2.0.6-1 (for SuperCluster)	12.1.0.4.0 and later
	1.1.3-2 1.3.3-2	All versions

Table 1-1   (Cont.) Supported Component Versions

Component	Firmware/Software Versions	Exadata Plug-in Version Support
Integrated Lights Out Manager (ILOM)	3.1 or later	13.1 and later
	v3.0.16.15.a r73751 or later (v2) v3.0.16.10.d or later (X2) v3.0.16.20.b or later (X2-8) v3.0.16.20.b or later (X3-8) v3.1.2.10 r74387 or later (X3-2)	12.1.0.4.0 and later
	v3.0.9.19.c r63792	All versions
ILOM ipmitool	Linux: 1.8.10.3 or later Oracle Solaris: 1.8.10.4 or later	All versions
Power Distribution Unit (PDU)	1.04 or later	13.1 and later
	1.05 1.06	12.1.0.4.0 and later
	1.01 1.02 (default version after reimage) 1.04	All versions
Avocent MergePoint Unity KVM Switch	Application: 1.2.8.14896 Boot: 1.4.14359	All versions
Cisco Switch	15.1(2)SG2	12.1.0.6.0 and later
	12.2(31)SGA9	All versions

Supported Operating Systems

The following operating systems (where OMS and agent is installed on) are supported by the Oracle Exadata plug-in 13.2:

- Management Server plug-in (all OMS-certified platforms):
  - IBM AIX on POWER Systems (64-bit)
  - HP-UX Itanium
  - Linux x86 and x86-64
  - Microsoft Windows x64 (64-bit)
  - Oracle Solaris on SPARC (64-bit)
  - Oracle Solaris on x86-64 (64-bit)
- Agent plug-in:
  - Linux x86-64
  - Oracle Solaris on x86-64 (64-bit)
  - Oracle Solaris on SPARC (64-bit)

Oracle Exadata Database Machine Hardware Not Supported

The following Oracle Exadata Database Machine hardware configurations are **not** supported for Enterprise Manager Cloud Control Exadata plug-in 13.x:

- V1 hardware
- V2 hardware

> **Note:**
>
> V2 machines discovered in Enterprise Manager Cloud Control 12*c* are still supported in 13*c*. However, discovery of V2 machines in Enterprise Manager Cloud Control 13*c* is not supported.

2

Installation and Deployment

This chapter provides the instructions for deployment of the Oracle Exadata plug-in. The following topics are discussed:

- Oracle Exadata Plug-in Deployment Prerequisites
- User Roles
- Install Enterprise Manager Agent
- Manually Deploy Exadata Plug-in

Oracle Exadata Plug-in Deployment Prerequisites

Before deploying the Oracle Exadata plug-in, make sure the following prerequisites are met:

- Create a Database Server ILOM Service Processor User
- Verify Software Versions
- Verify Names Resolution
- Verify Firewall Configuration
- Oracle SuperCluster Prerequisites

Create a Database Server ILOM Service Processor User

For the Enterprise Manager agent to communicate with an ILOM service processor, there must be a specific user ID established on the ILOM service processor.

> ✏ **Note:**
>
> Adding the specific user ID requires administrator level privilege on the ILOM service processor.

The specific ILOM user ID can be added in the ILOM service processor web interface, ILOM CLI, or with the `ipmitool` command. This example uses ILOM CLI.

For security reasons, the password to the ILOM service processor root user ID does not appear in the ILOM CLI commands in this example.

1. Log in to the Service Processor as root:

   ```
   # ssh root@[Service Processor IP]
   Password:
   ```

2. Change to the `users` directory:

   ```
   # cd /SP/users
   ```

3. Create the `oemuser` user and password:

```
# create oemuser

Creating user...
Enter new password: ********
Enter new password again: ********

Created /SP/users/oemuser
```

4. Change to the new user's directory and set the role:

```
# cd oemuser
/SP/users/oemuser

set role='cro'
Set 'role' to 'cro'
```

5. Test the ILOM user ID created in step 3 by listing the last 10 system events:

   • For Exadata X2 through X4:

   ```
   # ipmitool -I lan -H <ilom_hostname> -U oemuser -P oempasswd -L USER sel
   list last 10
   ```

   • For Exadata X5-2 (requires the `-I lanplus` command option):

   ```
   # ipmitool -I lanplus -H <ilom_hostname> -U oemuser -P oempasswd -L USER sel
   list last 10
   ```

6. Repeat steps 1 through 5 for the rest of the compute node ILOM service processors in your Oracle Database Machine.

Verify Software Versions

Verify the following software versions:

• Exadata Storage Server Software

• ILOM ipmitool

• InfiniBand Switch

• PDU Firmware

• KVM Application

• Grid Infrastructure/DB Cluster

Exadata Storage Server Software

The supported version is Exadata Storage Server Software 11*g* Release 2 (see Exadata Software Support for specific release version details). To verify the cell software version on the Exadata cell, `ssh` to the Exadata cell as the `root`, `celladmin`, or `cell-monitor` user. Run:

```
# cellcli -e 'list cell detail'
```

Look for "releaseVersion" in the output.

ILOM ipmitool

Enterprise Manager requires a minimal ipmitool software version of 1.8.10.4 or later for Oracle Solaris and 1.8.10.3 for Oracle Linux. To view the software version:

- For Oracle Linux, run the following command as the `root` user on one of the database servers in the cluster:

```
# dcli -g ~/dbs_group -l root ipmitool -V
```

> **Note:**
>
> The `dbs_group` file contains the list of compute node hostnames, one on each line. If the file does not exist, you can create it before running the `dcli` command.

- For Oracle Solaris, run the following command on each of the database servers in the cluster:

```
# /opt/ipmitool/bin/ipmitool -V
```

InfiniBand Switch

To verify the version of the InfiniBand switch firmware in your environment:

1. Log on to the management interface for the InfiniBand Switch (using ssh).

2. Run the following command:

```
# nm2version
```

The output should be similar to this:

```
# nm2version
Sun DCS 36p version: 1.1.3-2
```

This example shows a supported configuration for deploying the plug-in to monitor.

3. If the `nm2version` command returns output similar to this:

```
# nm2version
NM2-36p version: 1.0.1-1
```

Then you must upgrade your InfiniBand switch firmware. Follow the instructions listed in My Oracle Support (MOS) Document 888828.1:

https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&doc-type=REFERENCE&id=88882

PDU Firmware

The PDU firmware version must be 1.04 or later. The current version can be obtained by logging into the web interface of the PDU. On the left side of the screen, click **Module Info** to view the PDU firmware version.

Software updates for the PDU are available at:

https://updates.oracle.com/Orion/PatchDetails/process_form?
patch_num=12871297

KVM Application

The KVM Application software version must be 1.2.8 or later. The current version can be obtained by logging into the web interface of the KVM. On the left side of the screen under Unit View, Appliance, Appliance Settings, click **Versions** to view the Application software version.

See Avocent MergePoint Unity Switches Software Downloads for the latest updates.

Grid Infrastructure/DB Cluster

Grid Infrastructure/DB Cluster is required to be up and running before discovery.

Verify Names Resolution

The Enterprise Manager OMS server(s) require direct network access to each of the compute nodes. If the names of the compute nodes are not registered in the OMS nodes' DNS, then they will have to be manually entered in the `/etc/hosts` file for each OMS.

Each compute node should be verified to be able to resolve the hostnames of the ILOM servers, PDU's, storage cell nodes, and InfiniBand and Cisco switches. Again, if the names of those components are not registered in DNS, then entries can be added to the `/etc/hosts` file of each compute node.

To manage the Exadata Database Machine components from Enterprise Manager Cloud Control 13*c*, it is necessary for your local machine to be able to resolve the host name of Cloud Control 13*c*.

To access any of the Exadata Database Machine components directly from your local machine, it is also necessary for your local machine to be able to resolve the names of those components.

Verify Firewall Configuration

To verify the firewall configuration:

1. Allow `ping`

   In many secure network environments, it is normal for the `ping` service to be disabled. Enterprise Manager uses `ping` to establish the basic availability and status of the Exadata Database Machine components.

   - The compute nodes need to have the `ping` service and port enabled from the OMS Server(s).

   - All other Exadata Database Machine components (ILOM servers, PDU's, storage cell nodes, InfiniBand switches, and Cisco switch) need to have the `ping` service and port enabled from the compute nodes (where the agents are running).

> **✎ Note:**
>
> The `ping` traffic overhead is minimal. The agent pings the targets every five minutes.

2. Open Database Ports

   The database listener ports must be opened for the Enterprise Manager OMS server(s). Note that Exadata Database Machine databases will use SCAN listeners; so, ports will need to be opened for the base compute node, the compute node virtual IP, and scan listeners addresses.

   For example, if an Exadata Database Machine quarter rack has been configured with two compute nodes - `exadbnode1.example.com` and `exadbnode2.example.com` - and the listeners are using port 1521, then port 1521 will have to be opened to the Enterprise Manager Server for the following addresses:

   - The compute node hostnames - `exadbnode1.example.com` and `exadbnode2.example.com`

   - The virtual IPs for each compute node - `exadbnode1-vip.example.com` and `exadbnode1-vip.example.com`

   - The scan listener hostname - `scan-exadatadb`

3. Open Enterprise Manager Upload Port

   The Enterprise Manager Cloud Control 13*c* agents require access to the Enterprise Manager Servers upload service, normally configured on port 4889 for HTTP uploads and 4900 for HTTPS. To verify the ports assigned, run the following command on the OMS server command line.

   ```
   $ emctl status oms -details
   ```

   These ports will need to be opened for each of the compute nodes.

4. Open Agent Ports

   The OMS server(s) will need to be able to connect to the Enterprise Manager Cloud Control 13*c* Agent HTTP/HTTPS port on each compute node. The Agent port defaults to 3872. If port 3872 is not available, the next available port starting from port 1830 is used.

   To identify the port used:

   - Run the following command on the compute node command line:

     ```
     $ emctl status agent
     ```

   - Alternatively, you can look for the value of the `EMD_URL` property in the `emd.properties` file the following directory:

     ```
     <AGENT_HOME>/agent_inst/sysman/config
     ```

5. Open SSH Ports (port **22**)

   The Enterprise Manager Cloud Control 13*c* Agents require `ssh` access to the Exadata Database Machine components they monitor. As the Agents will run on the compute nodes the ssh ports, 22, on each of the storage cells, ILOMs, PDUs, KVMs, InfiniBand switches, and Cisco switch will need to be opened for each of the compute nodes.

> **Note:**
>
> The `emkit` configures `ssh` access but still requires the ports to be opened first.

6. Allow UDP Traffic (SNMP Ports) (Port **162**)

   All Exadata Database Machine components need to be able to send SNMP traps to the Agents running on the compute nodes. SNMP uses the UDP protocol so the Agent port and port 162 need to be opened for UDP traffic between the Storage Cells, ILOMs, InfiniBand Switches, Cisco Switch, and the Agent.

Table 2-1   Firewall Ports

Component	Ping service and port	SNMP*	SSH (port 22)	Notes
PDU	From remote agent	Yes	Yes	
Compute node ILOM	From remote agent	Yes	Yes	1. Remote agent needs to be able to SSH to dom0. 2. Needs to access ipmitool. 3. Need SNMP port open on dom0.
dom0	From EM OMS server	Yes	Yes	
Cell	From remote agent	Yes	Yes	
InfiniBand Switch	From remote agent	Yes	Yes	
Cisco Switch	From remote agent	Yes	Yes	
KVM	From remote agent		Yes	May not be required, if X5 does not have KVM
OMS			Yes	Upload http/https port - usually 3872
Agent				The OMS server(s) will need to be able to connect to the Enterprise Manager Cloud Control 12c Agent HTTP/HTTPS port on each compute node. The Agent port defaults to 3872. If port 3872 is not available, the next available port starting from port 1830 is used.

* SNMP uses the UDP protocol; so, the Agent port and port 162 need to be opened for UDP traffic.

Enable Support for IPv6 Environments

> **Note:**
>
> Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet.

To perform an Exadata Database Machine discovery on IPv6-based client or management network, you must deploy agents on a host that supports dual stack (IPV4 and IPV6).

If the compute node hosts are pure IPv6-based hosts, then deploy the agent on a remote host that supports both IPV4 and IPV6 and perform "remote agent" based discovery.

This agent deployment is needed for monitoring those components in DB Machine that do not yet support IPV6 (for example, Infiniband Switch and PDU. For more details, see IPv6 support status on Exadata Database Machine (Doc ID 2056895.1), available in My Oracle Support:

https://support.oracle.com/rs?type=doc&id=2056895.1

> **Note:**
>
> For a virtualized DB Machine, the VI target discovery should be done first as described in Discovering Virtualized Exadata Database Machine.

Oracle SuperCluster Prerequisites

Table 2-2 shows the required versions of OneCommand and Config-O-Matic (COM) supported by the Oracle SuperCluster hardware configurations.

Table 2-2   Oracle SuperCluster Prerequisites

Hardware Configuration	OneCommand Version	Config-O-Matic Version
M6-32 `databasemachine.xml` *only*	14.063 and later	1.6.4 and later
T5-8 `databasemachine.xml`	14.042 and later	1.5.8 COM and later
T5-8 `catalog.xml` (non-Java One-Command)	n/a	1.5.4 COM and earlier

Table 2-2   (Cont.) Oracle SuperCluster Prerequisites

Hardware Configuration	OneCommand Version	Config-O-Matic Version
T4-4 `catalog.xml` *only* Note: Because the T4-4 Oracle SuperCluster is at its "end of life," this entry is *only* for existing systems.	n/a	1.1.6 COM and earlier

User Roles

To manage the Exadata Storage Server, you need to create roles and then assign roles to administrators. Creating these roles restricts the privileges that each user has, for example in deleting the plug-in or accessing reports. See Oracle Exadata Database Machine Administration .

Install Enterprise Manager Agent

> **Note:**
>
> Enterprise Manager Exadata discovery supports the use of either management network hostname or client network hostname for the compute nodes. When installing the Enterprise Manager agent on the compute nodes, you should use the same hostname as used in Oracle Clusterware.
>
> You can identify the hostname of the nodes in the cluster by running the `olsnodes` command on one of the compute nodes. It is recommended that a fully qualified hostname, including the domain name, be used when specifying an Enterprise Manager agent hostname.

There are two methods for installing the Enterprise Manager Agent. Chose the one that works best for your environment:

• Install Agents and Set Up Exadata Monitoring Using Automated Kit

• Install Enterprise Manager Agent Using the Push Method

> **Note:**
>
> - Make sure any prerequisites are met. See Agent Installation Prerequisite - Solaris 11 Only.
>
> - The Enterprise Manager agent must be deployed to all compute nodes of the Database Machine. The host target name of the compute node must be the fully qualified host name, for example, `dbm1db01.mydomain.com`.
>
> - Non-fully qualified hostname (for example, `dbm1db01`) or IP address must **not** be used for the host target name of the compute node.
>
> - The same version of the Enterprise Manager agent and the same version of the Exadata plug-ins should be deployed on all compute nodes within the same Database Machine.

Agent Installation Prerequisite - Solaris 11 Only

If you are running Exadata Storage Server Software Release 11g Release 2 (11.2.3.1) on Oracle Solaris, follow the steps below before installing the agent.

1. Log in to the compute node host as agent user and execute the `ppriv $$` command. This command displays the **E** (Effective), **P** (Permitted), **I** (Inherited), and **L** (Limited) privileges.

   Generally, **E**, **P**, and **I** have the same set of basic privileges and for any normal user.

2. Assuming that output of the above command shows basic privileges, add the `priv_sys_net_config` privilege to the agent user so that InfiniBand commands can be executed.

   Log in as root and run:

   ```
   # usermod -K defaultpriv=basic,priv_sys_net_config <agent_user>
   ```

   This command adds `sys_net_config` to the agent user.

3. Log in as the agent user again and run the `ppriv $$` command to verify if the privileges are set. The output will show the `sys_net_config` privilege along with the existing (basic) set of privileges.

Install Agents and Set Up Exadata Monitoring Using Automated Kit

The Oracle Enterprise Manager Cloud Control 13*c* Setup Automation kit is available for download from My Oracle Support as a patch. The kit simplifies the process of deploying the agents on each of the compute nodes considerably, allowing agents to be deployed to all of the compute nodes, in one go, from one of the compute nodes, using one simple command. Instructions for using the kit to deploy agents on the compute nodes are provided in the patch `README.txt`.

To download the Automation kit for your platform, see Doc ID 1440951.1 in My Oracle Support:

https://support.oracle.com

Oracle Enterprise Manager Cloud Control 13*c* uses a holistic approach to manage the Exadata Database Machine and provides comprehensive lifecycle management from monitoring to management and ongoing maintenance for the entire engineered system.

The patch README provides instructions for how to install Management Agents on an Oracle Exadata Database Machine and point them to an existing Cloud Control environment or install a new stand alone Enterprise Manager environment and deploy the Management Agents pointing to this new environment. This standalone environment can be used when you do not want to take the corporate environment offline to apply the patches needed to monitor Oracle Exadata Database Machine.

The following procedures described in the README can be performed at any time, such as during initial configuration of Oracle Exadata Database Machine, or later:

- Preparing a corporate Oracle Enterprise Manager Cloud Control server to monitor Oracle Exadata Database Machine

- Installing Oracle Enterprise Manager Cloud Control 13*c* on a standalone server to monitor Oracle Exadata Database Machine

- Installing Oracle Enterprise Manager Cloud Control 13*c* Management Agents on Oracle Exadata Database Machine

- Removing Oracle Enterprise Manager Cloud Control 13*c* Management Agents from Oracle Exadata Database Machine when using a standalone server

- Removing Oracle Enterprise Manager Cloud Control 13*c* from a standalone server

Install Enterprise Manager Agent Using the Push Method

The installation instructions were captured on a Quarter Rack configuration (for example, 2 compute nodes, 3 cells).

1. Add the Exadata Database Machine compute nodes as host targets to Oracle Enterprise Manager Cloud Control 13*c*. From the Enterprise Manager home page, click the **Setup** menu (upper right corner), **Add Target**, then **Add Targets Manually.**

2. On the *Add Host Targets: Host and Platform* screen, specify a session name. Then identify the fully qualified hostnames and select the platform.

> **Note:**
>
> If the Agent software is not available for your platform, go to the Extensibility page and download it first.

Figure 2-1 shows how the selection should look for the Linux x86-64 platform.

Figure 2-1   Add Host Targets
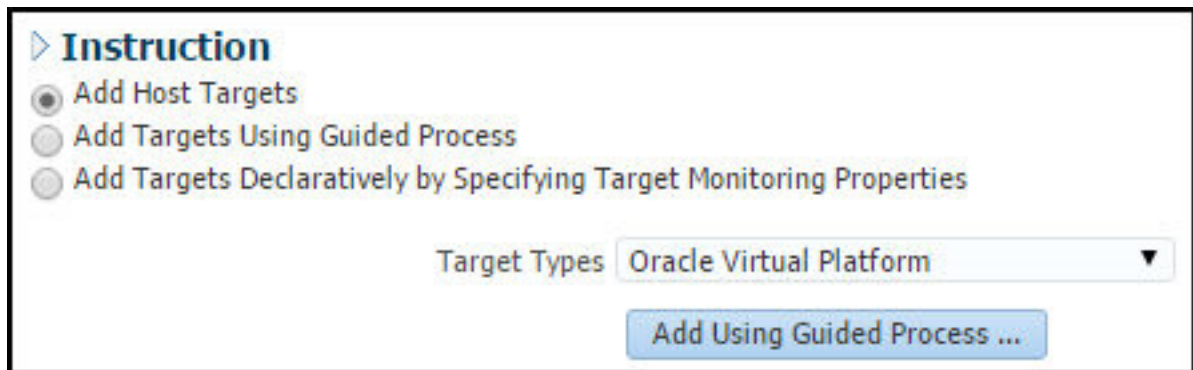
3. Click **Next** to add the details for the host.

4. On the *Installation Details* screen, provide the following information:

    •   Installation Base Directory

    •   Instance Directory

    •   Named Credential

    •   For Port, leave this field blank. As part of the installation process, an available port will be selected automatically.

5. Click **Next** to review the details about the host.

6. Click **Deploy Agent** to start the agent deployment process.

7. As the deployment process continues, remote prerequisite checks are automatically checked. If there are no issues, you will be presented with an Agent Deployment Summary with an indication that the agent deployment has passed. Figure 2-2 shows an example of a successful agent deployment.

Figure 2-2   Agent Deployment Summary

> **Note:**
>
> If the `root.sh` was not executed during deployment, then make sure to execute it on all compute nodes.

Installing Oracle Management Agent in Silent Mode Option

You can install Oracle Management Agent in silent mode as an alternative to installing it using the Add Host Target Wizard. Silent mode requires you to use a response file for providing the installation details and a deployment script for silently installing the Management Agent using the information supplied in the response file.

See *Installing Oracle Management Agent in Silent Mode* in *Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide*.

Manually Deploy Exadata Plug-in

Under the following conditions, you may need to manually deploy the Exadata plug-in on each of the compute nodes:

- For a new or fresh installation: Deploy the plug-in manually if you did **not** deploy the agent using Automation kit or push the latest version of the agent through OMS.

- For an upgrade to an existing installation: Deploy the Exadata plug-in manually if an older version of the Exadata plug-in has been deployed to the agent already and you would like to upgrade to the latest version of the Exadata plug-in.

To determine if the Exadata plug-in is deployed on each compute node and what version it is, you have two options:

- From a terminal window, run the following command:

  ```
  emctl listplugins agent
  ```

  > **Note:**
  >
  > The `emctl listplugins agent` command must be run on the compute node using the `emctl` in the agent installation directory.

- From Enterprise Manager Cloud Control, click the **Setup** menu (upper right corner), **Extensibility**, and then **Plug-ins**.

To manually deploy the Exadata plug-in:

1. From the Enterprise Manager home page, click the **Setup** menu (upper right corner), **Extensibility**, and then **Plug-ins**.

2. On the *Plug-ins* page, select Oracle Exadata from the Name list.

> **✎ Note:**
>
> The selected version should be for Release 12.1.0.1.0, 12.1.0.2.0, or 12.1.0.3.0. Oracle recommends that you deploy the latest version of the Exadata and Database plug-ins to the agent.

3. With Oracle Exadata selected, click **Deploy On**, then **Management Agent**.

4. On the *Deploy Plug-in on Management Agent* pop-up, click **Add**. A search pop-up will appear to allow you to search for targets to add. In the Target Type drop-down, select **Agent**, then click **Search**.

   Select a Target name from the results list and click **Select**. Repeat for each agent target.

5. After you have added the agents, click **Next** on the *Deploy Plug-in on Management Agent* screen to review and verify the agent information.

6. Click **Deploy** to deploy the plug-in to the agents.

7. Once the plug-in has been deployed to all agents, a confirmation screen will appear. Click **OK** to dismiss the pop-up or **Show Status** to display the status of the agent in the Enterprise Manager *Deployment Activities* screen.

ORACLE

3
Exadata Database Machine Discovery

This chapter provides instructions for discovery of the Oracle Exadata Database Machine through Enterprise Manager Cloud Control 13*c*.
The following sections describe how to discover the Exadata Database Machine and other supported targets:

1. Running the Discovery Precheck Script
2. Discovering an Exadata Database Machine
3. Discover Oracle SuperCluster as an Exadata Database Machine
4. Discovering Grid Infrastructure and RAC
5. Switch from Using CellCLI to ExaCLI after Storage Server Locked Down

Running the Discovery Precheck Script

Before you begin the guided discovery process, there are several checks you should perform to ensure a smooth discovery. A discovery precheck script is available to automatically verify many of the common problem areas prior to discovery.

Some Exadata discoveries in Oracle Enterprise Manager 13*c* may run into issues because of various configuration mismatches in software setup. This discovery precheck script helps to resolve the most common configuration problems. Run the script before all Database Machine discovery and examine the output thoroughly before proceeding with Discovering an Exadata Database Machine.

Follow the steps below to run the discovery precheck script:

1. Secure Storage for Target Monitoring Credentials.
2. Download the Discovery Precheck Script.
3. Run the Discovery Precheck Script.
4. Automatic Verification.
5. Manual Verification.

Secure Storage for Target Monitoring Credentials

As you begin the discovery process, cell monitoring requires log in and password credentials to be entered. These credentials are handled in the following manner:

- For the `cellmonitor` user: SSH equivalence is set up for between the `cellmonitor` user and the `agent` user. The root credentials being prompted for during discovery are not needed for metric collection afterwards. You can optionally choose to store the cell root password as a named credential in the Enterprise Manager repository.

- For the cell ILOM user (`oemuser`): This monitoring credential is encrypted and stored in the Enterprise Manager repository and in the `targets.xml` file on the agent.

- For the InfiniBand Switch user (`nm2user`): SSH equivalence is set up for between the `nm2user` user and the `agent` user. The `nm2user` credentials being prompted for during discovery are not needed for metric collection afterward. You can optionally choose to store the `nm2user` password as a named credential in the Enterprise Manager repository.

Download the Discovery Precheck Script

You can obtain the script in one of the following ways

- Access the script as part of Exadata plug-in 13.1.0.0.0 after the plug-in is deployed to the agent:

```
<agent installation directory>/plugins/oracle.sysman.xa.discov-
ery.plugin_12.1.0.3.0/discover/dbmPreReqCheck/exadataDiscoveryPreCheck.pl
```

> **Note:**
>
> The Exadata plug-in includes an additional script that enables enhanced monitoring through Enterprise Manager Cloud Control 13*c*.

- Download the script from *Prerequisite script for Exadata Discovery in Oracle Enterprise Manager Cloud Control 12c* (Doc ID 1473912.1) in My Oracle Support:

  https://support.oracle.com/rs?type=doc&id=1473912.1

- Access the script as described in *Obtaining the Oracle Enterprise Manager Setup Automation kit for Exadata* (Doc ID 1440951.1) in My Oracle Support for more information on the kit:

  https://support.oracle.com/rs?type=doc&id=1440951.1

Run the Discovery Precheck Script

To run the script:

```
$ <agent installation directory>/plugins/oracle.sysman.xa.discovery.plugin_<plugin
version>/discover/dbmPreReqCheck/
$ $ORACLE_HOME/perl/bin/perl ./exadataDiscoveryPreCheck.pl
```

As the script runs, you will be prompted for various inputs. It will execute all the built-in checks and will display all messages on standard output along with an execution log.

Automatic Verification

The discovery precheck script checks for the following information:

- Verifies that the user who is running the Enterprise Manager agent has read and execute permissions on at least one of the 11.2 (or later) Database Oracle home directory `<ORACLE_HOME>/bin/kfod` binaries.

- Verifies the management server and cell server is up and running on the Exadata cell. You can verify the status by running:

```
$ cellcli -e 'list cell attributes cellsrvStatus,msStatus'
```

- Verifies log in credentials. These credentials are required to complete the discovery process. **Make sure you have the information of the following credentials before starting the discovery process:**

  – Agent host credentials: the username and password of the user running the agents on the compute nodes

  – Monitoring credentials:

  - * Cell Root Password or ExaCLI credentials if you plan to use ExaCLI

  - * InfiniBand Switch Nm2user Password

  - * ILOM username and password

  – InfiniBand Switch root credentials: Username and Password

- Verifies the Database Machine schematic file requirements for Exadata Release 11.2.3.1, 11.2.3.2, and later, including:

  – That the schematic file should exist on the agent host selected for discovering the Exadata Database Machine at:

    `/opt/oracle.SupportTools/onecommand/databasemachine.xml`

  – That the schematic file has the world-readable privilege so that it is readable by the agent user.

  – That the version is **503** or later. The schematic file version is in the header of the file.

  – That the values of `<ADMINNAME>` and `<ADMINIP>` in the schematic file should be the current host names and management IP addresses of the compute nodes, Exadata cells, InfiniBand switches, KVM, PDU, and Cisco switch.

- Verifies the Database Machine schematic file requirements for Exadata Release 11.2.3.2 and later:

  – Verifies that the schematic file exists on the agent host selected for discovering the Exadata Database Machine at:

    `/opt/oracle.SupportTools/onecommand/catalog.xml`

  – Verifies that the schematic file has the world-readable privilege so that it is readable by the agent user.

  – Verifies that the schematic file version is **868** or later. The schematic file version is in the header of the file.

  – In addition, the values of `<ADMINNAME>` and `<ADMINIP>` in the schematic file should be the current host names and management IP addresses of the compute nodes, Exadata cells, InfiniBand switches, KVM, PDU, and Cisco switch.

    Client network naming is *only* supported in Exadata plug-in Release 12.1.0.3.0 and later.

> **Note:**
>
> If the Database Machine schematic file does not exist or its version does not meet the requirement, open a Service Request with Oracle Support to get the latest version of the schematic file.

Manual Verification

After running the discovery precheck script, you will still need to perform the following checks manually:

1. Use the 11.2 (or later) Database Oracle home directory when prompted for in Discovering an Exadata Database Machine.

2. Pre-requirements for platform and Database Machine version.

3. Compute node needs to be first discovered as Enterprise Manager host targets by installing the Enterprise Manager agents on these hosts.

    - The Enterprise Manager agent must be deployed to all compute nodes of the Exadata Database Machine. The host target name of the compute node must be the fully qualified host name (for example, `dbm1db01.mydomain.com`). Non-fully qualified hostnames (for example, `dbm1db01`) or IP addresses must not be used for the host target name of the compute node.

    - If you are using Exadata plug-in Release 12.1.0.1.0 or 12.1.0.2.0, the target name of the compute node host target should be the host name in the management network, not the client network.

    - If you are using Exadata plug-in Release 12.1.0.3.0 or later, the target name of the compute node host target can be the host name in the management network or the client network.

4. The host names of the compute nodes and Exadata cells in each individual Database Machine should have a unique prefix. In other words, Exadata Database Machine racks that are not connected by the same InfiniBand network to form one DB Machine should not share the same prefix for the host names.

5. For users of Oracle Enterprise Manager Cloud Control 12*c* Release 12.1.0.1.0 or if the installed version has been upgraded to Release 12.1.0.2.0 from 12.1.0.1.0 of the plug-in, you must manually push the Exadata plug-in to the agent.

6. For IPV6-based Exadata Database Machine, verify the following information in the schematic files:

> **Note:**
>
> The schematic files are usually located in the `/opt/oracle.Support-Tools/onecommand` directory on the compute nodes, and are named `databasemachine.xml, catalog.xml` or `exdatabasemachine.xml`.

   a. Check if all the `ADMINNAME`, `ILOMNAME` and `CLIENTNAME` entries are valid host names.

   b. Check if the `ADMINIP` and `ILOMIP` are in IPv6 format for the cells, compute nodes, and Cisco switch entries.

   c. As an example, the entries would be formatted like this:

```
<ITEM ID="2">
      <TYPE>cellnode</TYPE>
      <ADMINNAME>XXXXXceladm04</ADMINNAME>
```

```
                    <ADMINIP>XXXX:YYYY:XXXX:YYYY:XXXX:YYYY:XXXX:YYYY</ADMINIP>
                    <ILOMNAME>XXXXXceladm04-ilom</ILOMNAME>
                    <ILOMIP>XXXX:ZZZZ:XXXX:ZZZZ:XXXX:ZZZZ:XXXX:ZZZZ</ILOMIP>
                    <ULOCATION>2</ULOCATION>
                    <UHEIGHT>2</UHEIGHT>
            </ITEM>
```

d. Ensure that the IPv4 address is used for InfiniBand Switch and PDU as they do not support IPV6. For more details, see IPv6 support status on Exadata Database Machine (Doc ID 2056895.1), available in My Oracle Support:

https://support.oracle.com/rs?type=doc&id=2056895.1

Discovering an Exadata Database Machine

To discover a Database Machine target, follow these steps:

1. From the Enterprise Manager home page, select the **Setup** menu (upper right corner), **Add Target**, and then **Add Targets Manually**.

2. On the Add Targets Manually page (Figure 3-1), click **Add Targets Using Guided Process**. From Add Using Guided Process window, select **Oracle Exadata Database Machine** from the list and click **Add** (Figure 3-2).

Figure 3-1   Add Targets Manually
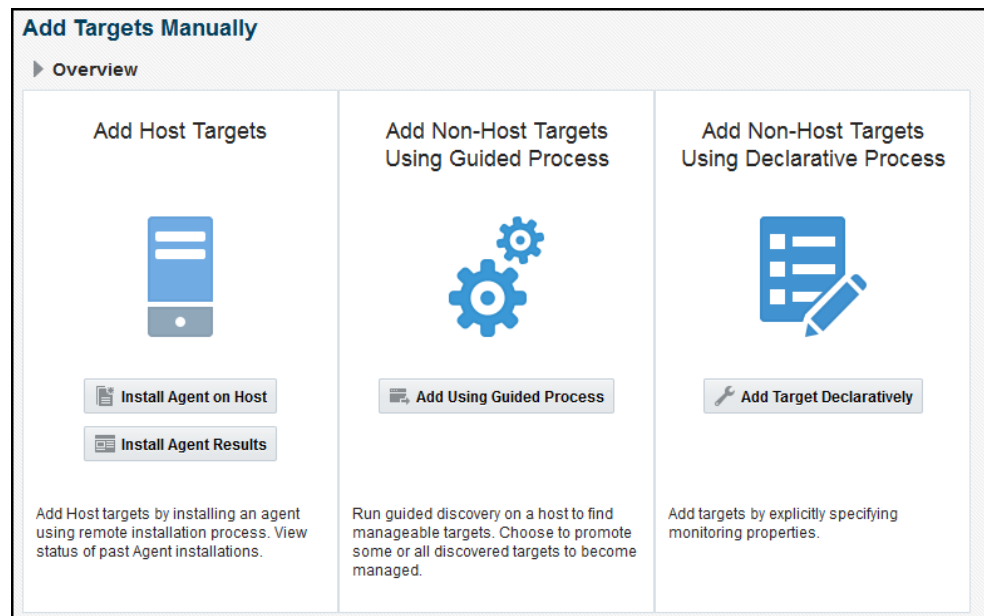
Figure 3-2   Select Oracle Exadata Database Machine
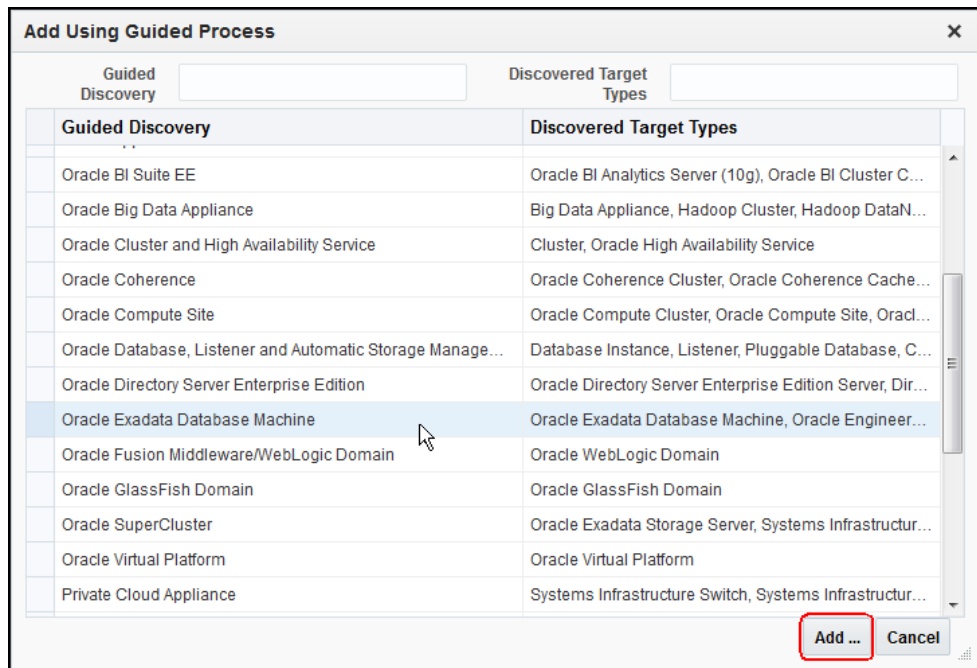
3. On the Oracle Exadata Database Machine Discovery page (Figure 3-3), select one of the following tasks:

    •   Discover a new Database Machine and its hardware components as targets. With this selection, choose one of the following monitoring options:

        –   **13c target type**. With this target type, enhanced monitoring is available through Enterprise Manager Cloud Control 13*c* (additional credentials are required).

            Enhanced monitoring of the 13*c* target type allows the Exadata plug-in to monitor the Exadata Storage Server and KVM, and the Enterprise Manager Systems Infrastructure (EMSI) plug-in monitors of all other hardware targets with the Exadata rack. The EMSI plug-in is included with your installation of Enterprise Manager.

        –   **12c target type**.

        After you select the monitoring type, the table will update to show the target types and the credentials required for discovery.

    •   Discover newly added hardware components in an existing Database Machine as targets. Select a Database Machine from the drop-down menu. The table will update to show the target types and the credentials required for discovery.

Figure 3-3   Oracle Exadata Database Machine Discovery Page

Click **Discover Targets**. The Exadata Discovery Wizard begins.

4. On the Discovery Inputs page (Figure 3-4), enter the following information:

   • For the Discovery Agents section:

     – **Agent URL:** The Agent deployed on compute node. Click the search icon to select from available URLs.

     > **Note:**
     >
     > For IPv6-based DB Machines, select the agents that are de-ployed on hosts with dual stack (IPv4 and IPv6) support.

   • For the Schematic Files section:

     – Once you have specified the Agent URL, a new row (hostname and sche-matic file information) is automatically added. The default schematic file, `databasemachine.xml`, describes the hardware components of the Exada-ta Database Machine.

     – Click **Set Credential** to set the credentials for the host.

     – Check/modify the schematic file location.

     – Select the schematic file name from drop-down menu.

> **Note:**
>
> You only need to customize the Schematic file location if one of the following is true:
>
> – The Schematic file is not in the default location.
>
> – The Database Machine contains a Storage Expansion Rack.
>
> – The hardware components are specified in multiple schematic files.

Figure 3-4   Database Machine Discovery: Discovery Inputs
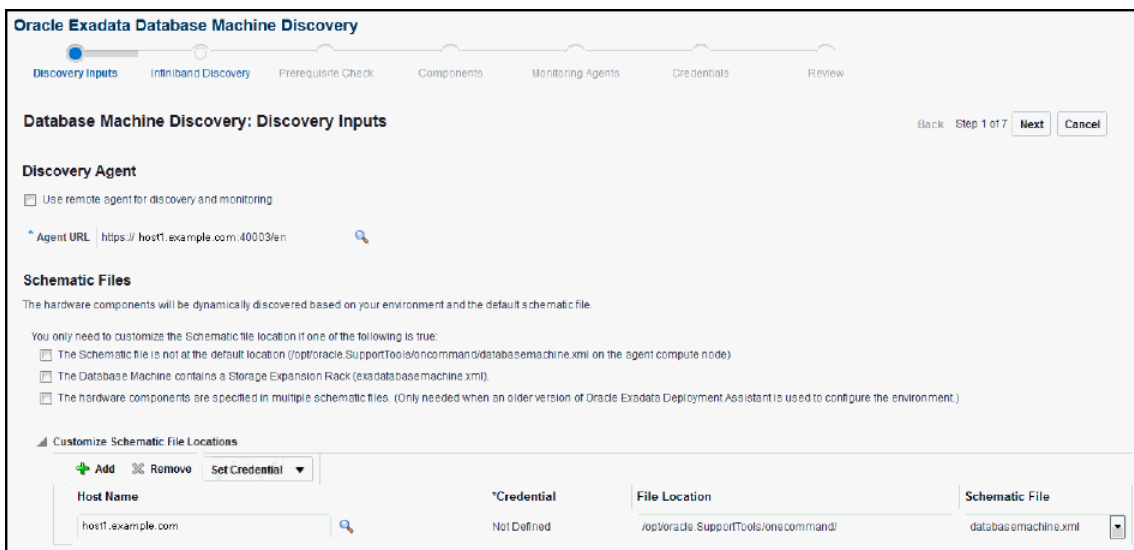
Click **Next**.

5. On the InfiniBand Discovery page (Figure 3-5), enter the following information:

   • **IB Switch Host Name:** The InfiniBand switch host name. The IB Switch host name is usually pre-populated.

   • **InfiniBand Switch ILOM host credential:** The user name (usually `ilom-admin` or `ilom-operator`) and password for the InfiniBand switch ILOM host.

**Figure 3-5   Database Machine Discovery: InfiniBand Discovery**
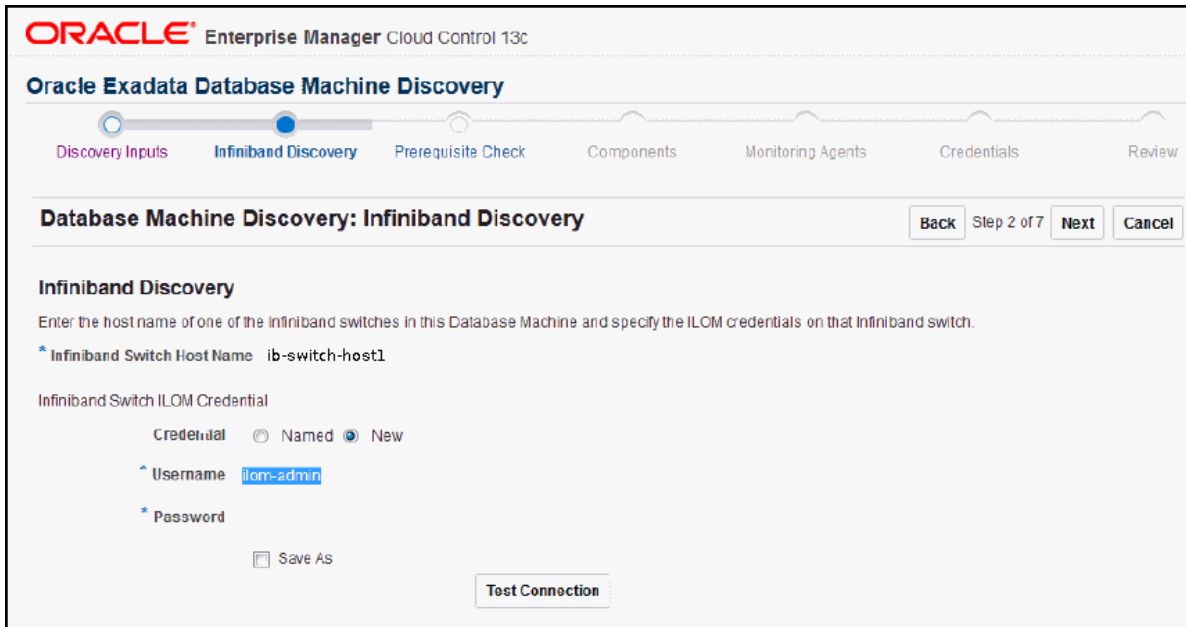
Click **Next**.

6. On the Prerequisite Check page (Figure 3-6), Enterprise Manager will try to dis-
cover hardware components dynamically based on your environment. If any criti-
cal issues are encountered, then you can click **Back** to resolve them. Enterprise
Manager will the show the problem and its severity (Info, Warning, or Critical).

Any warning issues or informational messages may also be displayed. These do
not interfere with the discovery process.

**Figure 3-6   Database Machine Discovery: Prerequisite Check**
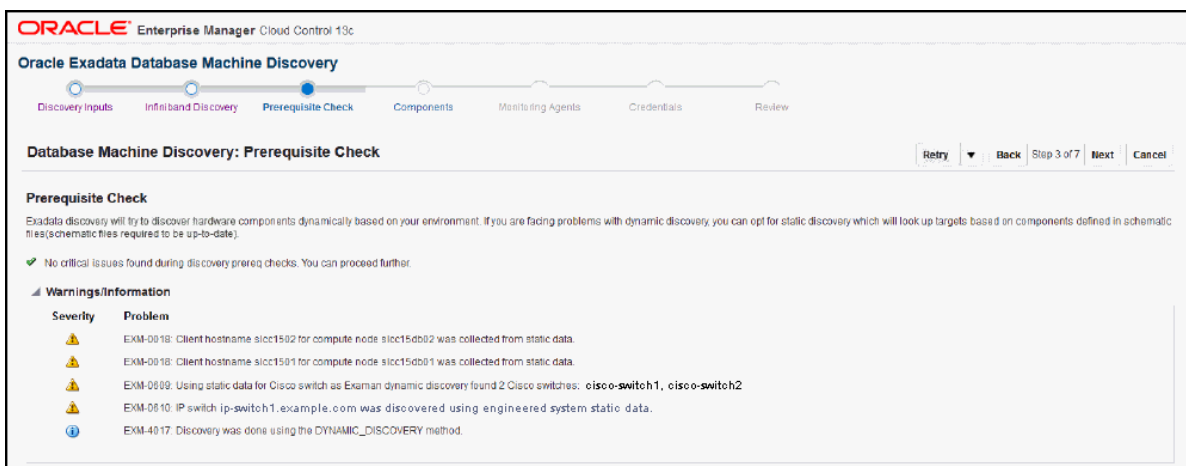
Click **Next**.

7. On the Components page (Figure 3-7), the components below are pre-selected. You can deselect any unwanted component. Components include, but are not limited to, the following:

- **Compute Node:** Select the hosts that are compute nodes in the Oracle Exadata Database Machine.

- **Oracle Exadata Storage Server:** Select the Oracle Exadata Storage Servers that are part of this Oracle Exadata Database Machine target.

- **InfiniBand Switch:** Select the InfiniBand Switches that are part of the Oracle Exadata Database Machine. These also will be added as managed targets.

- **Ethernet Switch:** Select the Ethernet switches that are part of the Oracle Exadata Database Machine. The Ethernet switches will be added as managed targets.

- **Compute Node ILOM:** Select the Integrated Lights Out Managers (ILOM) of the compute nodes that are part of this Oracle Exadata Database Machine. These ILOMs will be added as managed targets.

- **KVM:** Select the KVM switches that are part of the Oracle Exadata Database Machine. The KVM switches will be added as managed targets.

> **Note:**
>
> A partitioned rack can list other components that should be deselected manually (for example, compute nodes).

**Figure 3-7   Database Machine Discovery: Components**
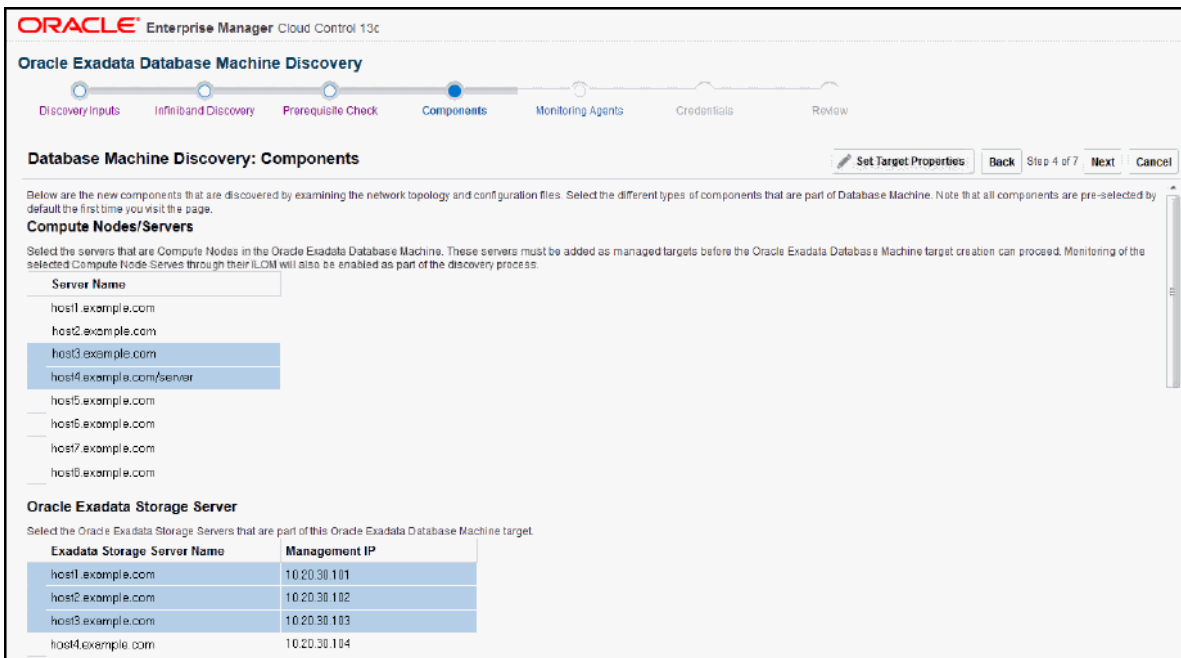
Click **Next**.

8. On the Monitoring Agents page (Figure 3-8), select an agent for the Monitoring Agent, and then one for the Backup Monitoring Agent from the drop-down selection.

> **Note:**
>
> A Warning will be thrown if only one agent is used as monitoring and backup agents. Click **Select Agents** to add more agents, if available.

**Figure 3-8   Database Machine Discovery: Monitoring Agents**
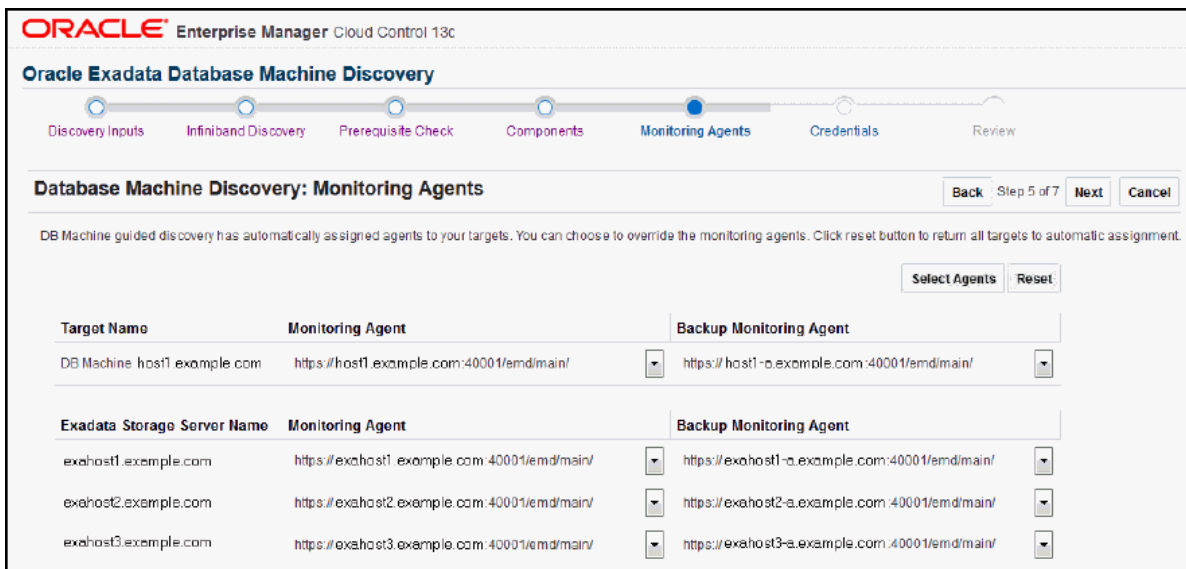
> **Note:**
>
> **Reminder:** For IPv6-based DB Machines, select the agents that are deployed on hosts with dual stack (IPv4 and IPv6) support.

Click **Next**.

9. On the Monitoring Credential page, select either **ExaCLI** or **CellCLI** for monitoring and set the monitoring credentials appropriately. ExaCLI is recommended as it allows SSH access to the Exadata Storage Server to be locked down for higher security. Select from the following:

   • Monitor using ExaCLI where the credentials are the same for all cells. For example:
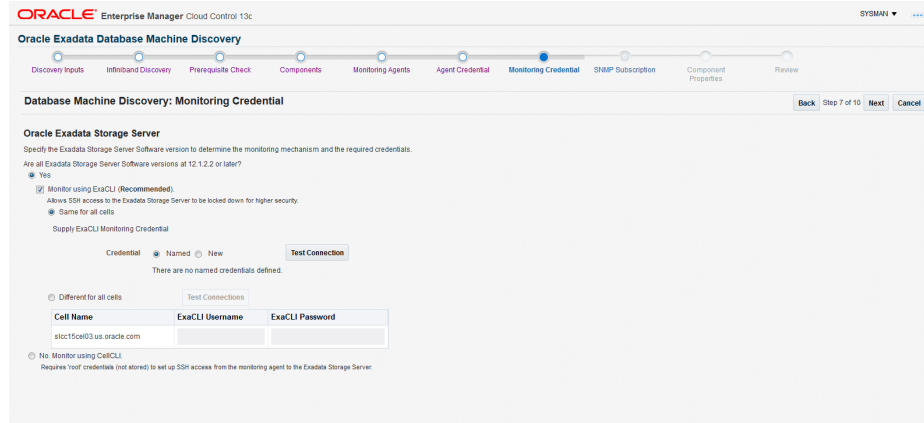
- Monitor using ExaCLI where the credentials are different for all cells. For example:
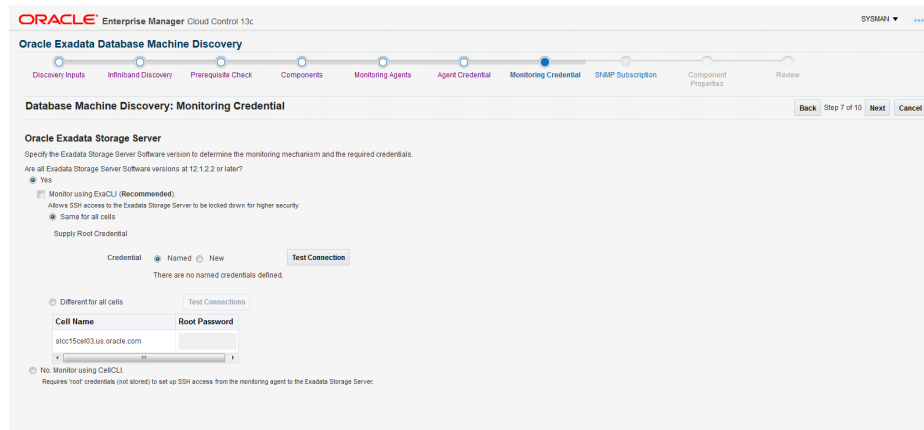
- Monitor using CellCLI. If you select CellCLI, then you must supply the root credentials (which are not stored) to set up SSH access from the monitoring agent to the Exadata Storage Server.
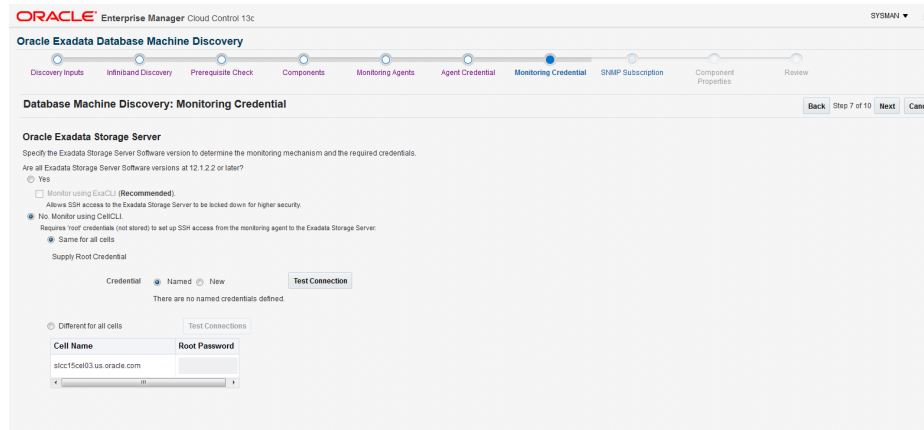
10. On the Agent Credential page, set the credentials for all components within the Exadata Database Machine (for example, the Storage Server, PDU, InfiniBand Switch, and so forth).

Click **Set Credential** to set the credential for the component. If the users and passwords are the same, choose **Same for all** and enter the user and password combination.

Select **Set up ASR subscription** option for receiving Oracle Auto Service Request (ASR)-oriented traps in Enterprise Manager. This option is needed if you are using Enterprise Manager to raise a Service Request (SR) instead of using ASR Manager on the cell.

Depending on the component, you may need to provide additional information. For example, in the Exadata Storage Server Credentials window, you must enter the SNMP Credentials as well as the Root Credentials (Figure 3-9):

Figure 3-9   Example: Set Oracle Exadata Storage Server Credentials

> **Note:**
>
> For IPv6 environments, only SNMPV3 credential type (SNMPV3Creds) is supported.
>
> The SNMP community String is like a password. It is sent along with each SNMP Get-Request, allow or deny access to device. Please check with your network administrator to get the community string details for your enterprise.
>
> The Agent requires SSH access to the Cisco Ethernet switch. You must specify this SSH access credentials when setting credentials for the Ethernet switch.

Click **OK** and set the credentials for all other components. Once all credentials are set, the Set Credentials page will update to show the credentials set (as shown in Figure 3-10):

Figure 3-10   Database Machine Discovery: Credentials

Click **Next**.

11. On the Review page, verify each section is correct. Figure 3-11 shows an example of an accurate review.

Figure 3-11   Database Machine Discovery: Review
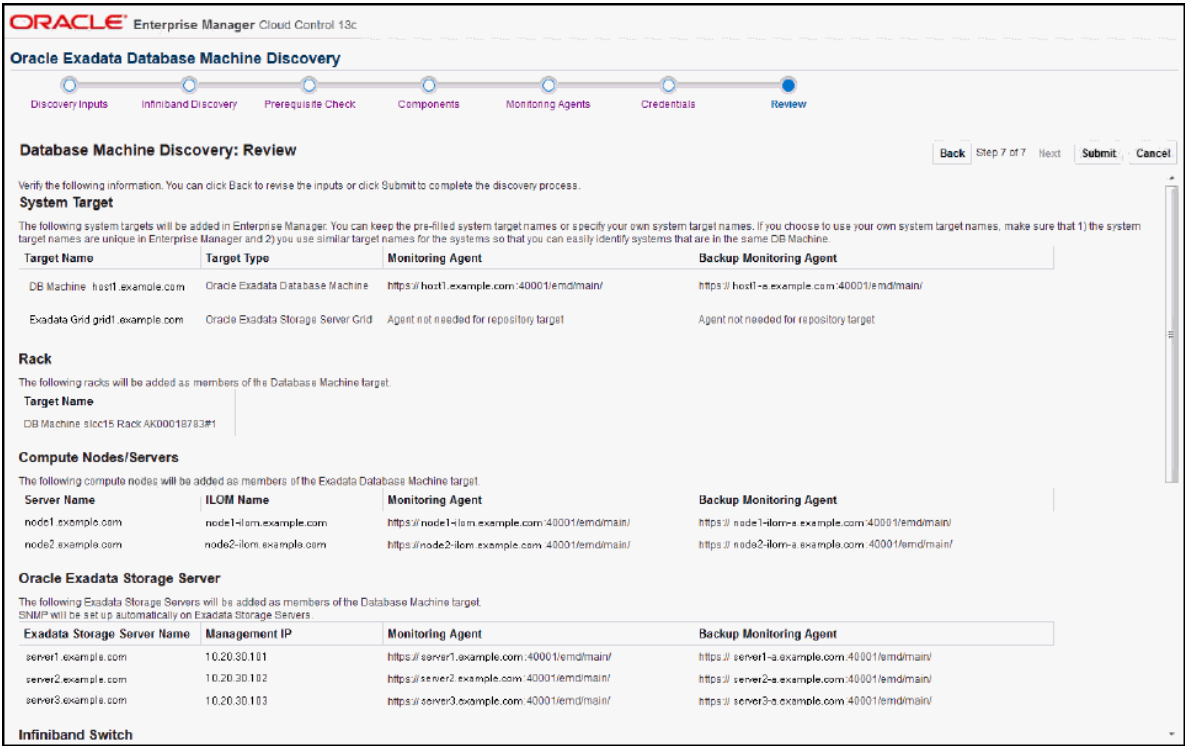
Click **Submit**.

12. After the Database Machine components are promoted, a Target Creation Summary page displays to show all discovered targets and components. If there are any errors, the Status column will display a red flag. Place your cursor over the flag for a pop-up window for additional information about the error (Figure 3-12):

Figure 3-12   Database Machine Discovery: Target Creation Summary

The discovery of the Oracle Exadata Database Machine is complete.

Discover Oracle SuperCluster as an Exadata Database Machine

You can use the Exadata plug-in to discover and monitor an Oracle SuperCluster system. You can monitor *only* the Database and Exadata components of the Oracle SuperCluster installed on LDOM and Zones. To monitor specific LDOM or virtualization configurations at the operating system level, please use Oracle Enterprise Manager Ops Center 12*c*.

To discover the Oracle SuperCluster as an Exadata Database Machine:

1. See *Discovering and Promoting Oracle Solaris Zones* in *Oracle® Enterprise Manager Cloud Control Administrator's Guide* for completing the prerequisite of pushing the agent to the control domain and zones.

2. Open a Service Request (SR) and upload the following files from your first 11gR2 LDOM:

   ```
   /opt/oracle.SupportTools/onecommand/onecommand.params
   /opt/oracle.SupportTools/onecommand/config.dat
   ```

> **Note:**
>
> Make a backup of your `/opt/oracle.SupportTools/onecommand` directory as you will overwrite it with the new configurations.

3. Oracle Support will provide you the file(s) generated based on the information provided in your configuration files. Copy all files into your `/opt/oracle.Support-Tools/onecommand` directory.

4. Ensure that READ permissions are open for all files in this directory as well as in the `/opt/oracle.SupportTools/em` directory. The agent must be able to read these files during discovery.

5. Run Self Update from Enterprise Manager to download the Solaris SPARC agent software on the OMS. Apply that download to the OMS to make it available for deployment:

   a. From Enterprise Manager, click **Setup**, then **Extensibility**, and finally **Self Update**. Click **Agent Software**.

   b. Select **Oracle Solaris on SPARC (64-bit)**.

   c. If the status is Available, then click **Download** from the Actions menu.

   d. Once downloaded, you must Apply it to the OMS from the same Self Update page.

   For more details on Self Update in Online or Offline mode, see *Updating Cloud Control* in *Oracle® Enterprise Manager Cloud Control Administrator's Guide*.

6. Install an agent on each of the Database nodes of the Oracle SuperCluster:

   a. From Enterprise Manager, select **Setup**, then **Add Target**, and finally **Add Targets Manually**.

   b. Select **Add Host Targets** (selected by default) and click **Add Host**.

   c. Continue with the installation wizard and ensure that you run `root.sh` on *each* node once installation is completed.

> **Note:**
>
> You may run into a known issue where you have to edit the Ciphers entry in `/etc/ssh/sshd_config` and restart ssh (see bug 13822068 for details). See *SSHD Connection Errors After Upgrading To Exadata Version 11.2.3.1.0* (Doc ID 1437596.1) in My Oracle Support:
>
> https://support.oracle.com/rs?type=doc&id=1437596.1

7. Configure the database nodes for Database Machine discovery.

   This step is needed to set descriptions of each DB node by updating the DB node IP address, Host Channel Adapter ID, and management hostname in the InfiniBand configurations using `set_nodedesc.sh`. Enterprise Manager Agents look for this information when discovering the Database Machine.

   Run:

```
# ibnetdiscover | grep your_db_nodes
```

If no output is not returned, then run the following command to set the node descriptions from all database nodes:

```
# /bin/ib_set_node_desc_ssc.sh
```

8. Discover Exadata Database Machine from Enterprise Manager using Manual Discovery wizard. This discovery process is the same as any other Exadata DBM target. See Discovering an Exadata Database Machine.

9. Discover the HA RAC Cluster and the cluster databases and configure each target as usual.

Discovering Grid Infrastructure and RAC

The following sections provide instructions for discovering Grid Infrastructure and Oracle Real Application Clusters targets:

- Discover Grid Infrastructure (Cluster) Targets
- Discover Oracle Real Application Clusters Targets

Discover Grid Infrastructure (Cluster) Targets

1. From the Setup menu, select **Add Targets**, then **Add Targets Manually**.

2. In the Add Targets Manually page, select **Add Non-Host Targets Using Guided Process (Also Adds Related Targets)** and **Target Type as Oracle Cluster and High Availability Services**.

3. Click **Add Using Guided Discovery** and follow the wizard.

4. On the Add Cluster Target: Specify Host page, select the first database node and click **Continue**.

5. The cluster home details are displayed. Ensure that all database nodes are shown in Selected Hosts section.

6. Click **Add**.

Discover Oracle Real Application Clusters Targets

1. From the Setup menu, select **Add Targets**, then **Add Targets Manually**.

2. In the Add Targets Manually page, select **Add Non-Host Targets Using Guided Process (Also Adds Related Targets)** and **Target Type as Oracle Database, Listener and Automatic Storage Management**.

3. Click **Add Using Guided Discovery** and follow the wizard.

4. In the wizard pages, configure Cluster Databases (`dbsnmp` password required) and Cluster ASM (`asmsnmp` password required).

Switch from Using CellCLI to ExaCLI after Storage Server Locked Down

You can at any time lock down an Exadata Storage Server and switch to ExaCLI for monitoring/administration (See Exadata Storage Server User Guide to know more about ExaCLI). From the Exadata Storage Server menu, select Target Setup, then select Monitoring Configuration, as shown in Figure 3-13:

Figure 3-13   Monitoring Credentials Menu Item
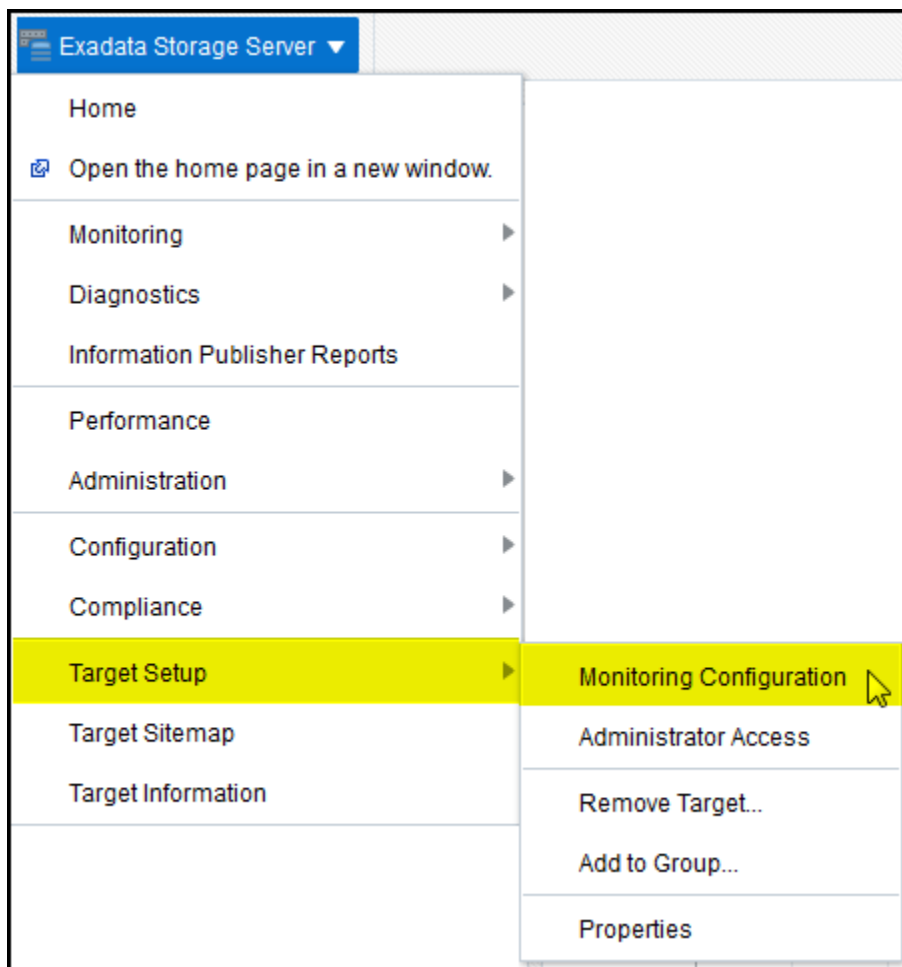
On the Monitoring Configuration page, set the **Support ExaCLI** value to **1** (the default is 0), as shown in Figure 3-14:

Figure 3-14   Monitoring Configuration: Set to Monitor Using ExaCLI

4

Post-Discovery Configuration and Verification

discoverypost-discovery configuration and verificationOnce the Oracle Exadata Database Machine has been discovered through Enterprise Manager Cloud Control 13*c*, you must complete post-discovery configuration on the following targets:

- Set Up SNMP Trap Forwarding on Compute Node
- Configure Storage Cell SNMP for Enterprise Manager Monitoring
- Configure and Verify SNMP for InfiniBand Switch Targets
- Configure the Compute Node ILOM SNMP for Enterprise Manager Monitoring
- Verify Configuration for Oracle ILOM Server
- Set Up SNMP for Cisco Ethernet Switch Targets
- Set Up SNMP for Power Distribution Unit (PDU) Targets
- Set Up SNMP for KVM Targets
- Accessing Oracle Support Workbench for Exadata Storage Server
- Oracle Exadata Database Machine Dashboard Creation

> **Note:**
>
> You must remove the SNMP notification on the cell, InfiniBand switch, ILOM, Cisco switch, PDU, and KVM **manually** if you remove these targets from Enterprise Manager.
>
> Starting with Exadata plug-in Release 12.1.0.3.0, when the Exadata Database Machine target is deleted through Enterprise Manager Cloud Control, there is an option to remove the SNMP notification from the cells and InfiniBand switches.

> **Note:**
>
> View a video of how to monitor your Exadata environment:
>
> https://apex.oracle.com/pls/apex/f?p=44785:24:0::NO:24:P24_CON-
> TENT_ID,P24_PREV_PAGE:5664,1

Set Up SNMP Trap Forwarding on Compute Node

> **Note:**
>
> If you do not need to monitor KVM, then you can skip this section.

The traps from the KVM will be sent to UDP port **162** on the monitoring agent host. For the Enterprise Manager Agent to receive traps from the KVM, SNMP trap forwarding must be set up on the host where the Enterprise Manager Agent is running so that the `snmptrapd` daemon can receive traps using port **162** and forward the trap to the agent receivelet's listening port.

Ideally, you should perform the steps on all compute nodes in preparation for a scenario when monitoring is moved to a compute node that was not previously being used to monitor the KVM targets.

- Set Up Compute Node Agent - Linux
- Set Up Compute Node Agent - Solaris

Set Up Compute Node Agent - Linux

The following commands must be run as `root` user:

1. Get the port value from `EMD_URL` property in the `<AGENT_INST>/sysman/config/emd.properties` file. This is the port at which receivelet will listen over UDP for traps (for this example, the port value is **3872**).

2. Confirm that the receivelet is listening on this port over UDP. An entry should be seen in the below command's output:

   ```
   # netstat -an | grep 3872 | grep udp
   ```

3. Run the following command to stop the SNMP trap daemon:

   ```
   # service snmptrapd stop
   ```

   Typically, the `service` command will be located in the `/sbin` directory.

4. Add the following entry to the `/etc/snmp/snmptrapd.conf` configuration file:

   ```
   authcommunity log,execute,net <community string>
   forward default udp:localhost:3872
   ```

   > **Note:**
   >
   > If the `/etc/snmp/snmptrapd.conf` file does not exist, create one and add the lines as described above.

5. Edit the `/etc/hosts.allow` file to add the following line:

   ```
   snmptrapd : ALL
   ```

6. Run the following command:

```
# chkconfig snmptrapd on
```

7. Run the following command to start the SNMP trap daemon:

```
# service snmptrapd start
```

Set Up Compute Node Agent - Solaris

The following commands must be run as `root` user:

1. Get the port value from `EMD_URL` property in the `<AGENT_INST>/sysman/config/emd.properties` file. This is the port at which receivelet will listen over UDP for traps (for this example, the port value is **3872**).

2. Confirm that the receivelet is listening on this port over UDP. An entry should be seen in the below command's output:

```
# netstat -an | grep 3872 | grep udp
```

3. Run the following command to stop the SNMP trap daemon:

```
# svcadm disable snmptrapd
```

You may see the following message. If so, then you can ignore it:

```
svcadm: Pattern 'snmptrapd' doesn't match any instances
```

Typically, the `svcadm` command will be located in the `/usr/sbin` directory.

4. Add the following entry to the `/etc/net-snmp/snmp/snmptrapd.conf` configuration file:

```
authcommunity log,execute,net <community string>
forward default udp:localhost:3872
```

> **Note:**
>
> If the `/etc/net-snmp/snmp/snmptrapd.conf` file does not exist, create one and add the lines as described above.

5. Create a `/tmp/snmptrapd.xml` file with the following content:

```
<?xml version="1.0"?>
<!DOCTYPE service_bundle SYSTEM
"/usr/share/lib/xml/dtd/service_bundle.dtd.1">
<service_bundle type='manifest' name='snmptrapd'>
  <service name='application/management/snmptrapd' type='service' version='1'>
    <create_default_instance enabled='true' />
    <single_instance />
    <dependency name='network' grouping='require_all' restart_on='none'
type='service'>
      <service_fmri value='svc:/milestone/network:default' />
    </dependency>
    <exec_method type='method' name='start' exec="/usr/sbin/snmptrapd -Lsd -
p /var/run/snmptrapd.pid" timeout_seconds ="60"/>
    <exec_method type='method' name='stop' exec=':kill' timeout_seconds='60'/>
    <stability value='Evolving' />
    <template>
```

```
        <common_name>
            <loctext xml:lang='C'>net-snmp SNMP trap daemon</loctext>
        </common_name>
      </template>
    </service>
</service_bundle>
```

6. Validate the `/tmp/snmptrapd.xml` file you have just created in step 5:

    ```
    # svccfg validate /tmp/snmptrapd.xml
    ```

7. Import the `/tmp/snmptrapd.xml` file:

    ```
    # svccfg import snmptrapd.xml
    ```

8. Make sure that the `snmptrapd` daemon is running:

    ```
    # svcs snmptrapd
    ```

    An example of the output is:

    ```
    STATE          STIME    FMRI
    online         16:20:00 svc:/application/management/snmptrapd:default
    ```

9. If needed, you can start the `snmptrapd` daemon with the following command:

    ```
    # svcadm enable snmptrapd
    ```

Configure Storage Cell SNMP for Enterprise Manager Monitoring

Exadata Storage Cell SNMP configuration is performed using the `cellcli` command and can be run in batch using `dcli` from a compute node.

> **Note:**
>
> - For Enterprise Manager Cloud Control 12*c* Bundle Pack 1 (BP1):
>
>   The SNMP trap subscription for Exadata Storage Cells is done automatically after finishing the guided discovery process.
>
> - For Exadata plug-in Release 12.1.0.2.0 and later:
>
>   During the discovery process, you can optionally provide the necessary `root` credentials to subscribe for SNMP traps from Exadata Storage Cells. If you have done so, then you can skip the remaining steps of this section and proceed with Configure and Verify SNMP for InfiniBand Switch Targets.
>
> - While the `public` string is used for the SNMP examples in the following sections, it is supported to use any valid SNMP community string.
>
> - Because of a limitation with the V1 protocol and JDMK API, if an IPv6 component sends SNMPv1 traps, then the sender's IP address is always `0.0.0.0`. Therefore, if the Exadata Storage Server environment is IPv6, then the `snmpv1` subscription should not be allowed.
>
> - Use an SNMP V3 subscription for IPv6-based cell targets because of the limitation in SNMP V1 protocol.

Using the `ALTER CELL` Command

While using the `ALTER CELL` command, all existing subscribers should be specified along with the new subscriber being added. Similarly, you can also modify the `notificationPolicy` or `notificationMethod` attributes.

While using the `ALTER CELL` command, the `host=` and `community=` attribute values should be quoted, and `type=` is NOT quoted.

If you are using the DCLI utility to set up SNMP alerting, then any command containing punctuation, which will be interpreted by the local shell, must be enclosed with double quotation marks. If the command includes the following characters, then outer quotation marks and escape characters are required:

```
$ (dollar sign)
' (quotation mark)
< (less than)
> (greater than)
( ) (parentheses)
```

The backslash (\) is the escape character that allows the characters to be passed to the CellCLI utility without being interpreted by the remote shell.

Check Current SNMP Configuration

Check the current SNMP configuration using the following `cellcli` commands:

1. To list the current subscribers for SNMP:

```
# cellcli -e list cell attributes snmpSubscriber
```

When correctly configured, this command should list the primary and backup agents for the cell target, for example:

```
# cellcli -e list cell attributes snmpSubscriber
((host=[hostname.mycompany.com],port=3872,community=public),
(host=[hostname2.mycompany.com],port=3872,community=public))
```

2. To list the currently configured notification methods:

```
# cellcli -e list cell attributes notificationMethod
```

Possible values are **snmp**, **mail** and **snmp,mail**. When correctly configured, this command should return either `snmp` or `snmp,mail`, for example:

```
# cellcli -e list cell attributes notificationMethod
snmp,mail
```

3. To list the currently configured notification policy for SNMP:

```
# cellcli -e list cell attributes notificationPolicy
```

Possible values are any or all of **Critical**, **Warning**, and **Clear**. When correctly configured, this command should return `Critical, Warning, Clear`, for example:

```
# cellcli -e list cell attributes notificationPolicy
Critical,Warning,Clear
```

Configure SNMP Values Using `cellcli`

To set the values of `snmpSubscriber`, `notificationMethod` and `notificationPolicy`:

1. Set the `snmpSubscriber` value:

   • **SNMP V1**

   ```
   # cellcli -e "alter cell snmpSubscriber=((host='[host name]',port=[port]),
   (host='[host name]',port=[port]))"
   ```

   Where `[host name]` and `[port]` values are Agents monitoring your cell targets.

   • **SNMP V3**

   The process is same as above, but along with the host and port, an SNMP V3 user and type must be provided:

   ```
   ALTER CELL snmpSubscriber=((host='host1.example.com',port=[port], snmpUs-
   er='[v3user]', type=V3))
   ```

   Before you run the command, make sure that a `v3user` is a valid SNMP user on the cell. You can check by running following command:

   ```
   cellcli -e "list cell attributes snmpUser"
   ```

   If there is no valid SNMP user on the cell, then add a V3 user with the following command:

   ```
   ALTER CELL snmpUser=((name='[v3user]', authProtocol='MD5', authPass-
   word='[passwd]', privProtocol='DES', privPassword='[passwd]'))
   ```

> **✎ Note:**
>
> The Enterprise Manager Agent supports only DES and MD5/SHA combination as of now. AES is not supported.

- **Oracle Auto Service Request (ASR) subscription**

  The above two steps describe the process of adding an SNMP subscription for cell traps in MS MIB format. If you want to subscribe for SNMP traps in the Oracle Auto Service Request (ASR) format as well, then along with the entries mentioned above you must add another entry with `type=ASR` (for V3, it is `type=V3ASR`).

  For example, for SNMP V1:

  ```
  ALTER CELL snmpSubscriber=((host='host1.example.com',port=[port],communi-
  ty='[community string]'), (host='host1.example.com',port=[port],communi-
  ty='[community]',type=ASR))
  ```

  For example, for SNMP V3:

  ```
  ALTER CELL snmpSubscriber=(((host='host1.example.com',port=[port],communi-
  ty='[community string]'),(host='host1.example.com',port=[port], snmpUs-
  er='[v3user]', type=V3ASR))
  ```

> **✎ Note:**
>
> Take special care not to overwrite existing settings for `snmpSubsriber`. If there are existing subscribers, then append the agent subscriptions. For example, if the `cellcli -e list cell attributes snmpSubscriber` command returned:
>
> ```
> # cellcli -e list cell attributes snmpSubscriber
>  ((host=ilm-asr1.example.com,port=162,community=public,type=asr))
> ```
>
> Then you must append the Agent subscriptions:
>
> ```
> #cellcli -e "alter cell snmpSubscriber=((host='ilm-asr1.exam-
> ple.com',port=162,
> community=public,type=asr),(host='[host name]',port=[port]),
> (host='[host name]',port=[port]))"
> ```

2. For SNMP V3, update the following in Enterprise Manager:

- Ensure that the V3 monitoring credentials are set up on the cell target in Enterprise Manager which match the v3 user on the cell:

  – Log in to Enterprise Manager.

  – From the **Setup** menu, select **Security**, then select **Monitoring Credentials**.

  – Select the **Exadata Storage Server** type and click **Manage Monitoring Credentials**.

  – Select the cell and set the V3 credentials.

- Ensure that the `snmpengineid` property is set up on the target in Enterprise Manager:
  - Log in to Enterprise Manager.
  - Go to the Exadata Storage Server home page.
  - From the Exadata Storge Server menu, select **Monitoring Configuration**.
  - If the `snmpengineid` property is not set, then set it manually in Enterprise Manager. You can obtain it from the cell with the following command

    ```
    list cell attributes snmpengineidhex
    ```

    All of the above steps are automatically taken care of it SNMP V3 sub-scription along with ASR option are selected during Exadata Database Machine discovery.

3. Set the `notificationMethod` value:

   ```
   # cellcli -e "alter cell notificationMethod='snmp,mail'"
   ```

4. Set the `notificationPolicy` value:

   ```
   # cellcli -e "alter cell notificationPolicy='Critical,Warning,Clear'"
   ```

Configure SNMP Values Using `dcli` (optional)

The SNMP configuration commands can be run using `dcli` to perform the configuration in batch on all storage cells:

1. Set the `snmpSubscriber` value:

   ```
   $ dcli -g cell_group -l root "cellcli -e \"alter cell snmpSubscrib-
   er=((host='[host name]',port=[port]),(host='[host name]',port=[port]))\""
   ```

   Where `[host name]` and `[port]` values are Agents monitoring your cell targets.

2. Set the `notificationMethod` value:

   ```
   $ dcli -g cell_group -l root "cellcli -e \"alter cell notificationMe-
   thod='snmp,mail'\""
   ```

3. Set the `notificationPolicy` value:

   ```
   $ dcli -g cell_group -l root "cellcli -e \"alter cell notificationPolicy='Criti-
   cal,Warning,Clear'\""
   ```

Verify SSH Connectivity

Open a new terminal and verify whether the SSH connectivity was successfully established:

```
$ ssh -l cellmonitor <cell_ipaddress> cellcli -e 'list cell detail'
```

- If you are not prompted for any password, then you can assume that the connectivity is established.
- If you are asked to confirm whether you want to continue connecting, specify **Yes**.

Remove a Subscription

To remove the subscription, use the `ALTER CELL` command again by excluding the host name that you want to remove from the `snmpsubscriber` list.

> **Note:**
>
> The SNMP receivelet listens on a single address and port for all monitored targets. The port is the UDP port with the same number as the TCP port used in the `EMD_URL`.
>
> By default, the SNMP receivelet listens on all addresses; if the property `SnmpRecvletListenNIC` is set in the `emd.properties` file, the receivelet will attempt to resolve the value as either a name or IP address, and listen on only that address.
>
> This parameter is independent of `AgentListenOnAllNICs` and `EMD_URL` because in some installations, the Agent may need to communicate with the OMS and with managed targets on different networks.

Configure and Verify SNMP for InfiniBand Switch Targets

The SNMP configuration for Enterprise Manager monitoring of InfiniBand Switches is done automatically as part of the Enterprise Manager guided discovery process. It is good practice, however, to verify that SNMP configuration has been successful.

> **Note:**
>
> - For Enterprise Manager Cloud Control 12*c* Bundle Pack 1 (BP1):
>
>   The SNMP Trap setup for Infiniband Switches is done automatically after finishing the guided discovery process.
>
> - For Exadata plug-in Release 12.1.0.2.0 and later:
>
>   During the discovery process, you can optionally provide the necessary `root` credentials to set up SNMP trap for the InfiniBand Switch. If you have done so, then you can skip the remaining steps of this section and proceed with Configure the Compute Node ILOM SNMP for Enterprise Manager Monitoring.

To configure (if necessary) and verify the SNMP configuration for an InfiniBand Switch:

1. Log in to the InfiniBand Switch ILOM web interface using the URL `https://<ib_switch_hostname>` as root.

> **Note:**
>
> Try using Internet Explorer if the console does not display all fields/
> values in your browser of choice.

2. Click **Configuration**, then **System Management Access**, and finally **SNMP**.

3. Ensure the following values are set:

```
State=Enabled
Port=161
Protocols=v1,v2c,v3
```

   If you need to make changes, make sure you click **Save**.

4. Click **Configuration**, then **System Management Access**, then **SNMP**, and finally the **Communities** link. The page scrolls to the SNMP Communities table. In the SNMP Communities table, click **Add**.

   A new window opens.

5. Type the community name into the **Community Name** field. Select the permissions from the Permission drop-down menu. Click **Save**.

   The community is created, and the window closes.

6. Click **Alert Management**.

7. If not already listed, for each Agent that monitors the InfiniBand Switch target, select an empty alert (one that has the Destination Summary `0.0.0.0, snmp v1, community 'public'`) and click **Edit**. Provide the following values:

```
Level = Minor
Type = SNMP Trap
Address = [agent compute node hostname]
Destination Port = [agent port]
SNMP Version = v1
Community Name = public
```

   Click **Save**.

8. Verify the InfiniBand Switch SNMP configuration for Enterprise Manager monitoring:

```
snmpget -v 1 -c <community_string> <hostname_of_IB_switch>
1.3.6.1.4.1.42.2.70.101.1.1.9.1.1.5
```

   For example:

```
$ snmpget -v 1 -c public my_IB_switch.my_company.com
1.3.6.1.4.1.42.2.70.101.1.1.9.1.1.5
SNMPv2-SMI::enterprises.42.2.70.101.1.1.9.1.1.5 = INTEGER: 1
```

> **Note:**
>
> If the Timeout message is displayed as a output for the above command,
> then it means that the InfiniBand Switch is not yet configured for SNMP.

> **Note:**
>
> To remove the subscription, follow steps 1 to 5 above (step 3 is not
> needed). In step 5, set the Agent compute node host name to **0.0.0.0**
> and the port to **0**.

Set Up SNMP for InfiniBand Switch Targets Using Enterprise Manager

You can set up SNMP for InfiniBand Switch targets using the Enterprise Manager
Cloud Control console:

1. Navigate to the IB Network target (not the individual switches) and select Adminis-
   tration.

2. Select the **IB Switch** target type, then one of the IB Switch targets.

3. Select the **Setup SNMP Subscription** command, then select the management
   agent URL that monitors the InfiniBand switch target from the Agent URL list. Click
   Next.

4. Provide credentials for the InfiniBand switch. Click **Next**.

5. Review the details you provided. If there are no further changes, then click **Sub-
   mit**.

Perform steps 1-5 for both the Monitoring Agent and Backup Monitoring Agent of the
InfiniBand switch target.

Configure the Compute Node ILOM SNMP for Enterprise Manager Monitoring

> **Note:**
>
> These instructions apply only for the Exadata Database Machine and are not
> applicable to the Oracle SuperCluster.

The compute node ILOM targets are responsible for displaying a number of disk failure
alerts for their respective compute node that are received as SNMP traps. For Enter-
prise Manager to receive those traps, the `/opt/oracle.cellos/compmon/exada-
ta_mon_hw_asr.pl` script must be run to configure SNMP subscriptions for the agents
(both primary and backup agents) that have been configured to monitor the compute
node ILOM targets. This step is applicable to Exadata plug-in Release 12.1.0.2.0 and
later.

The `exadata_mon_hw_asr.pl` script is run as the root user with the `-set_snmp_sub-
scribers` parameter to add SNMP subscribers. For example:

```
# /opt/oracle.cellos/compmon/exadata_mon_hw_asr.pl -set_snmp_subscribers "(host=host-
name1.mycompany.com,port=3872,community=public,type=asr,fromip=11.222.33.444),
(host=hostname2.mycompany.com,port=3872,community=public,type=asr,fro-
mip=12.345.67.890)"
```

```
Try to add ASR destination Host - hostname1.mycompany.com IP - 11.222.33.44 Port -
3872 Community - public From IP - 22.333.44.555
Try to add ASR destination Host - hostname2.com IP - 11.111.11.111 Port - 3872 Com-
munity - public From IP - 22.333.44.555
```

The script needs to be run on each compute node:

- The `host` values should be the hostnames of the agents configured to monitor the compute node ILOM target associated with the compute node.

- The `fromip` values should be the IP address of the compute node that the compute node ILOM target is associated with.

For example, if you have an X2-2 machine with compute node targets `edbm01db01` through `edbm01db08` and associated compute node ILOM targets `edbm01db01-c` through `edbm01db08-c`, then you would need to run the script once on each compute node - therefore, the script would be run eight times in total.

- On compute node `edbm01db01`, the `host` and `port` values would be the hostnames and ports of the agents monitoring compute node ILOM target `edbm01db01-c` and the `fromip` value would be the IP address of the compute node itself, `edbm01db01`.

- On compute node `edbm01db02`, the `host` and `port` values would be the hostnames and ports of the agents monitoring compute node ILOM target `edbm01db02-c` and the 'fromip' value would be the IP address of the compute node itself, edbm01db02, ... and so on.

This is a good example of where Manual selection of Management Agents for targets is useful. If the first two compute nodes are always the Monitoring Agent and Backup Monitoring Agent, then it is easy to work out the values needed for -`set_snmp_subscribers` parameters, the `host` and `port` values would be the same for all compute nodes.

> **Note:**
>
> The `exadata_mon_hw_asr.pl` script, overwrites any existing SNMP subscriptions. While setting the SNMP subscribers, make sure that current subscribers are included in the new list of subscribers.
>
> It is possible to use the `exadata_mon_hw_asr.pl` script to get the current set of subscribers using the `-get_snmp_subscribers` parameter.
>
> For example:
>
> ```
> # /opt/oracle.cellos/compmon/exadata_mon_hw_asr.pl -get_snmp_subscribers -
> type=asr
> ```
>
> Suppose the current list is:
>
> ```
> (host=hostname1.mycompany.com,port=162,community=public,type=asr,fro-
> mip=11.222.33.444),
> (host=hostname2.mycompany.com,port=162,community=public,type=asr,fro-
> mip=11.222.33.444)
> ```
>
> Then new subscriptions can be added using the following command:
>
> ```
> # /opt/oracle.cellos/compmon/exadata_mon_hw_asr.pl -set_snmp_subscribers
>  "(host=asrhostname1.mycompany.com,port=162,community=public,type=asr,fro-
> mip=11.222.33.444),
> (host=asrhostname2.mycompany.com,port=162,community=public,type=asr,fro-
> mip=11.222.33.444),
> (host=hostname1.mycompany.com,port=3872,community=public,type=asr,fro-
> mip=11.222.33.444),
> (host=hostname2.mycompany.com,port=3872,community=public,type=asr,fro-
> mip=11.222.33.444)"
> ```

After adding the new subscribers, run the command `exadata_mon_hw_asr.pl` script with the `-get_snmp_subscribers` parameter to get the list of SNMP subscribers and verify the new SNMP subscriptions were added successfully. For example:

```
# /opt/oracle.cellos/compmon/exadata_mon_hw_asr.pl -get_snmp_subscribers -type=asr
(host=asrhostname1.mycompany.com,port=162,community=public,type=asr,fro-
mip=10.10.10.226),
(host=asrhostname2.mycompany.com,port=162,community=public,type=asr,fro-
mip=10.10.10.226),
(host=hostname1.mycompany.com,port=3872,community=public,type=asr,fro-
mip=10.10.10.226),
(host=hostname2.mycompany.com,port=3872,community=public,type=asr,fro-
mip=10.10.10.226)
```

Configure the Compute Node ILOM SNMP for Compute Nodes Running Management Server

For compute nodes running Management Server, the call to the `exadata_mon_hw_asr.pl` script is replaced with `dbmCLI` commands, which are similar to `cellCLI` commands on the Storage Cells.

Oracle Exadata Database Machine X5-2 (up to X6) runs the Management Server on compute nodes.

Configure SNMP Values Using dbmcli

1. Set the `snmpSubscriber` value:

    ```
    # dbmcli -e "ALTER DBSERVER snmpSubscriber=((host=[agent1_host-
    name],port=[agent1_port],community=public,type=asr),(host='agent2_hostna-
    me',port=<agent's port>,type=asr))"
    ```

    Where `[host name]` maps to the Enterprise Manager agents monitoring your com-
    pute node target.

2. Set the `notificationMethod` value:

    ```
    # dbmcli -e "ALTER DBSERVER notificationMethod="mail,snmp", notificationPoli-
    cy="critical,warning,clear", smtpFrom="admin", smtpFromAddr=[sender email ad-
    dress], smtpPort=[port], smtpServer=[smtp server], smtpToAddr=[recipient email
    address], smtpUseSSL=TRUE
    ```

3. Verify the updates by executing:

    ```
    # dbmcli -e "LIST DBSERVER attributes snmpSubscriber"
    ```

    For Virtualized Exadata, these commands need to be executed in `Dom0`.

Configure SNMP for Oracle SuperCluster

1. Log in to the Oracle SuperCluster ILOM web interface, which is accessible via a
    browser using the url `http://<ilom_hostname>` and the `root` credentials.

2. Select **Configuration**, then **Alert Management**.

3. Add a row for each agent.

4. Select an empty slot and click **Edit**.

5. Specify the following information:

    *   Level: **Minor**

    *   Type: **SNMP Trap**

    *   Address: IP Address of the Agent

    *   Destination Port: Uncheck **Autoselect**, then specify Agent port manually

    *   SNMP Version: **v1**

    *   Community Name: {your chosen community name}

6. Click **Save**.

Verify Configuration for Oracle ILOM Server

To verify that Alerts can be successfully raised and cleared for the Oracle ILOM Server
targets, perform the following steps:

1. Log in to the Enterprise Manager Cloud Control console as an administrator.

2. Click **Targets** and select **Exadata**. Select one of the Oracle ILOM Server targets
    using the Target Navigation pane.

    The ILOM target page will be displayed, showing the current status of that target
    as well as any incidents that have been raised for it.

3. Raise an alert manually from the ILOM Server being validated. Run following command as `root` on the first database server in the cluster:

```
# ipmitool -I lan -H sclczdb01-c -U oemuser -P oempasswd -L OPERATOR event PS0/
VINOK deassert
```

The output will be similar to:

```
Finding sensor PS0/VINOK... ok
0 | Pre-Init Time-stamp | Power Supply #0x65 | State Deasserted
```

After running the above command, wait a few minutes then refresh the ILOM target page. An incident should appear in the Incidents section.

4. Clear the alert raised in step 3. Run the following command as `root` on the first database server in the cluster:

```
# ipmitool -I lan -H sclczdb01-c -U oemuser -P oempasswd -L OPERATOR event PS0/
VINOK assert
```

The output will be similar to:

```
Finding sensor PS0/VINOK... ok
0 | Pre-Init Time-stamp | Power Supply #0x65 | State Asserted
```

After running the above command, wait a few minutes then refresh the ILOM target page. The incident that was raised in step 3 should show as cleared in the Incidents section.

> **Note:**
>
> Do not forget to clear the alert raised in step 3, as it was raised for testing only and did not reflect a true fault condition!

5. Repeat for the remaining configured ILOM service processors in your Oracle Database Machine.

Set Up SNMP for Cisco Ethernet Switch Targets

The Cisco Ethernet Switch must be configured to allow the Agents that monitor it to be able to both poll the switch and to receive SNMP alerts from the switch. To allow this, perform the following steps (swapping the example switch name `dm01sw-ip` with the name of the Cisco Ethernet Switch target being configured):

1. Log in to the Cisco switch and enter Configure mode:

```
# ssh cisco-switch-host -l <admin user>
User Access Verification Password:
dm01sw-ip> enable
Password:
dm01sw-ip# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
dm01sw-ip(config)#
```

2. Enable access to allow the Agents monitoring Cisco Switch target to poll the switch.

In the command, `[EMagentIPaddr]` is the IP address of the server where the Enterprise Manager Agent is running. The SNMP community specified must match the value provided when configuring the Cisco Switch target:

```
dm01sw-ip(config)# access-list 1 permit [EMagentIPaddr]
dm01sw-ip(config)# snmp-server community <community_string> ro 1
```

3. Set the monitoring Agent as the location where SNMP traps are delivered. The SNMP community specified must match the value provided during Enterprise Manager Cisco Switch Management Plug-In setup:

```
dm01sw-ip(config)# snmp-server host <EMagentIPaddr> version 1 <community string>
udp-port [EMagentRecvltListenPort]
```

Where `[EMagentRecvltListenPort]` is the `EMD_URL` port of the `emagent` or `SnmpRecvletListenNIC` property value if it is enabled.

4. Configure the Cisco Switch to send only environmental monitor SNMP traps:

```
dm01sw-ip(config)# snmp-server enable traps envmon
```

5. Verify settings and save the configuration:

```
dm01sw-ip(config)# end
dm01sw-ip# show running-config
dm01sw-ip# copy running-config startup-config
```

Verify the Cisco Ethernet Switch SNMP Configuration

Run the `snmpwalk` command line utility or equivalent tool to verify the Cisco Switch configuration.

Run the following commands to fetch and display the data from the Cisco switch:

```
$ snmpget -v 1 -c <community_string> <hostname_of_cisco_switch>
1.3.6.1.4.1.9.2.1.56.0
$ snmpget -v 2c -c <community_string> <hostname_of_cisco_switch>
1.3.6.1.4.1.9.2.1.56.0
```

> **Note:**
>
> If a timeout message is displayed as an output for the above command, then it means that the Cisco Switch is not yet configured correctly.

Set Up SNMP for Power Distribution Unit (PDU) Targets

To enable Enterprise Manager to collect metric data and raise events for the PDU target, you must configure the PDU to accept SNMP queries from the Agents that monitor the PDU target. Also, appropriate threshold values for different phase values needs to be set on the PDU.

This section assumes that this is a first time configuration of the PDU. SNMP must be enabled and the trap section completed. Granting SNMP access to a different monitoring Agent IP address is an example where only the "Trap Host Setup" section needs to be changed.

1. Log in to the PDU network interface through a browser at `http://<pdu-name>`, for example: `http://edbm01-pdu1.example.com`

2. Click **Net Configuration**, then log in again.

3. Scroll down until you reach the SNMP section of the frame.

> **Note:**
>
> The network interface for the PDU is a frame within a window. In order to scroll down on this page, you must see the scroll bar for the PDU frame as well as the outside scroll bar for the browser in which you accessed the PDU.

4. If your PDU is not SNMP-enabled, select the **SNMP Enable** check box, then click **Submit**.

5. Scroll to the NMS region of the frame.

6. Enter the following in Row 1 under NMS:

   • IP: Enter the **IP address** of the first monitoring Agent

   • Community: Enter **"public"**

7. Click **Submit**.

For details on configuring the PDU thresholds settings, see the "Configuring Oracle Exadata Database Machine" chapter in your *Exadata Database Machine Owner's Guide*. This guide is pre-loaded along with other Exadata user documentation onto your Oracle Exadata Database Machine.

Verify the PDU SNMP Configuration

Use the `snmpwalk` command line utility or equivalent tool to verify the PDU configuration.

Run the following command to fetch and display the data from PDU:

```
snmpget -v 1 -c <community_string> <hostname_of_pdu> 1.3.6.1.4.1.2769.1.2.3.1.1.1.0
```

> **Note:**
>
> If a timeout message is displayed as an output for the above command, then it means that the PDU is not yet configured correctly.

Set Up SNMP for KVM Targets

The KVM needs to be configured to send SMNP traps to the Agents that monitor it. See the following sections to set up SNMP for KVM targets:

• Set Up SNMP in KVM Management Console

• Verify the KVM SNMP Configuration (Base SNMP Configuration) - Linux

- Verify the KVM SNMP Configuration (Base SNMP Configuration) - Solaris
- Verify the KVM SNMP Configuration (SNMP Forwarding to Agent)

> **Note:**
>
> The SNMP forwarder setup described in Set Up SNMP Trap Forwarding on Compute Node is required on the compute node agent that monitors the KVM target. If the SNMP forwarder is not set up, the agent will not receive traps from the KVM device.

Set Up SNMP in KVM Management Console

Configure the KVM to send traps to the monitoring agent host:

1. Log in to the KVM management console through a browser at:

   ```
   https://<kvm-name>
   ```

   For example:

   ```
   https://edbm01sw-kvm.example.com
   ```

2. Click **SNMP** under Target Devices in the left-hand navigation bar.

3. Select the **Enable SNMP** check box and enter the appropriate community name in the Read, Write, and Trap fields (for example, enter **"public"**).

4. Click **Save**.

5. Click **Destinations** under SNMP in the left-hand navigation bar.

6. Enter the IP address of the Agent monitoring the KVM target.

7. Click **Save**.

The traps from the KVM device will be sent to UDP port 162 on the monitoring agent host. Refer to Set Up SNMP Trap Forwarding on Compute Node for details to set up the trap forwarder to forward traps received on port 162 to the Enterprise Manager agent receivelet port.

Verify the KVM SNMP Configuration (Base SNMP Configuration) - Linux

Run the `snmptrapd` command line utility to verify the KVM configuration. Make sure that the steps outlined in Set Up SNMP Trap Forwarding on Compute Node has been performed.

Follow the steps below on the monitoring agent host for the KVM target:

1. Log in as `root`.

2. Run the following command:

   ```
   # service snmptrapd stop
   # /usr/sbin/snmptrapd -d -Lsd -p /var/run/snmptrapd.pid
   ```

3. Reboot the KVM to generate SNMP traps. To reboot the KVM:

    a. Log in to the KVM.

    b. Click **Overview** on the left side of the screen under Unit View, Appliance.

    c. Click **Reboot**.

    d. In the confirmation window, click **OK** to confirm KVM reboot.

4. Check that `snmptrapd` logs messages in the `/var/log/messages` file from the IP address of the KVM. The following example shows the messages for the KVM's IP address (10.1.1.240):

```
Jul 30 14:51:05 dbm1db02 snmptrapd[65800]:  Received 72 bytes from UDP:
[10.1.1.240]:32768
.
Jul 30 14:51:05 dbm1db02 snmptrapd[65800]: 0000: 30 82 00 44  02 01 00 04  06 70
75 62  6C 69 63 A4    0..D.....public.
.
Jul 30 14:51:05 dbm1db02 snmptrapd[65800]: 0016: 82 00 35 06  09 2B 06 01  04 01
D1 32  12 01 40 04    ..5..+.....2..@.
.
Jul 30 14:51:05 dbm1db02 snmptrapd[65800]: 0032: 0A F5 13 F0  02 01 06 02  01 02
43 03  6D 19 4C 30    ..........C.m.L0
.
Jul 30 14:51:05 dbm1db02 snmptrapd[65800]: 0048: 82 00 15 30  13 06 0B 2B  06 01
04 01  D1 32 12 02    ...0...+.....2..
.
Jul 30 14:51:05 dbm1db02 snmptrapd[65800]: 0064: 06 01 04 04  72 6F 6F
74                            ....root
.
Jul 30 14:51:05 dbm1db02 snmptrapd[65800]:
```

5. If step 4 is confirmed, the KVM has been configured correctly. Run the following commands:

```
# service snmptrapd stop
# service snmptrapd start
```

Verify the KVM SNMP Configuration (Base SNMP Configuration) - Solaris

Run the `snmptrapd` command line utility to verify the KVM configuration. Make sure that the steps outlined in Set Up Compute Node Agent - Solaris have been performed.

Follow the steps below on the monitoring agent host for the KVM target:

1. Log in as `root` and run the following command:

```
# svcadm disable snmptrapd
# /usr/sbin/snmptrapd -d -Lsd -p /var/run/snmptrapd.pid
```

2. Reboot the KVM to generate SNMP traps. To reboot the KVM:

    a. Log in to the KVM.

    b. Click **Overview** on the left side of the screen under Unit View, Appliance.

    c. Click **Reboot**.

    d. In the confirmation window, click **OK** to confirm KVM reboot.

ORACLE

3. Check that the `snmptrapd` daemon logs messages in the `/var/log/messages` file from the IP address of the KVM. The following example shows the messages for the KVM's IP address (10.1.1.240):

```
Jul 30 14:51:05 dbm1db02 snmptrapd[65800]: Received 72 bytes from UDP:
[10.1.1.240]:32768

Jul 30 14:51:05 dbm1db02 snmptrapd[65800]: 0000: 30 82 00 44  02 01 00 04 06 70
75 62  6C 69 63 A4    0..D.....public.

Jul 30 14:51:05 dbm1db02 snmptrapd[65800]: 0016: 82 00 35 06  09 2B 06 01 04 01
D1 32  12 01 40 04    ..5..+.....2..@.

Jul 30 14:51:05 dbm1db02 snmptrapd[65800]: 0032: 0A F5 13 F0  02 01 06 02 01 02
43 03  6D 19 4C 30    ..........C.m.L0

Jul 30 14:51:05 dbm1db02 snmptrapd[65800]: 0048: 82 00 15 30  13 06 0B 2B 06 01
04 01  D1 32 12 02    ...0...+.....2..

Jul 30 14:51:05 dbm1db02 snmptrapd[65800]: 0064: 06 01 04 04 72 6F 6F
74    ....root

Jul 30 14:51:05 dbm1db02 snmptrapd[65800]:
```

4. If step 3 is confirmed, the KVM has been configured correctly. Stop the `snmptrapd` process currently running:

```
# ps -ef | grep snmptrapd
# kill -9 <snmptrapd process ID>
```

5. Start the `snmptrapd` daemon:

```
# svcadm enable snmptrapd
```

Verify the KVM SNMP Configuration (SNMP Forwarding to Agent)

After performing the steps in Verify the KVM SNMP Configuration (Base SNMP Configuration) - Linux or Verify the KVM SNMP Configuration (Base SNMP Configuration) - Solaris, follow the steps below to validate that the monitoring Agent can receive the SNMP traps generated by the KVM and convert the received traps to Enterprise Manager events.

1. In the Enterprise Manager Cloud Control console, go to the KVM target page.

2. In the Targets menu, select **Monitoring**, then **Alert History**.

   You should see an entry for *Reboot Started Status* in the Alert History table.

3. In the Alert History table, click **Reboot Started Status**. You should see the following warning alert with the message:

```
The appliance is rebooting. Command issued by user root.
```

Accessing Oracle Support Workbench for Exadata Storage Server

You can access the Oracle Support Workbench for the current Exadata Storage Server to access diagnostic data for problems and incidents related to the cell.

To access the Support Workbench for a single Exadata cell, follow these steps:

1. From the **Target** menu of the Exadata Storage Server for which you want to ac-
   cess the Oracle Support Workbench, select **Diagnostics**, then select **Support
   Workbench** as shown in Figure 4-1:

   Figure 4-1   Support Workbench Menu
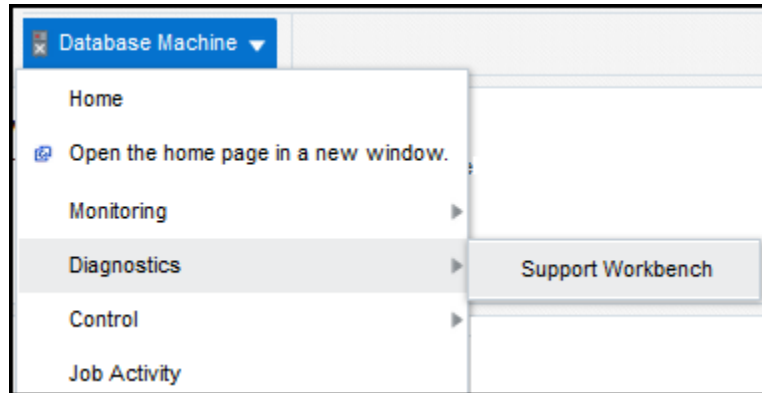
2. If you are logging in to the Support Workbench for the first time, you must first initi-
   alize the Support Workbench properties. For first-time log in, the Initialize Support
   Workbench Properties window will be displayed as shown in Figure 4-2:

   Figure 4-2   Initialize Support Workbench Properties
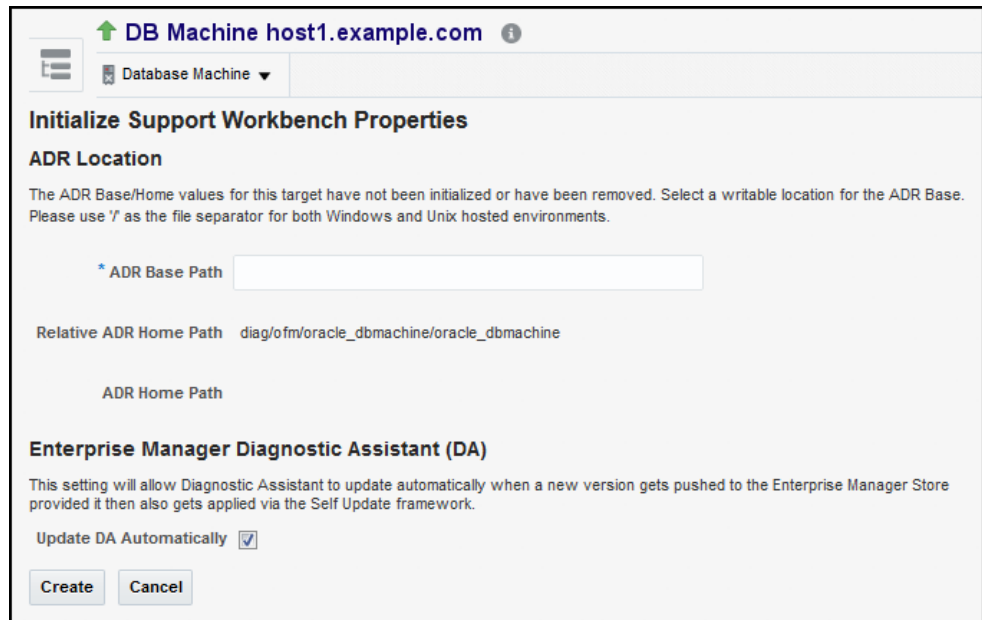
   Enter the Automatic Diagnostic Repository (ADR) Base Path. A typical looks like
   this (Figure 4-3):

Figure 4-3   ADR Base Path

The ADR Home Path is a target-specific, writable path on the agent where the generated package is to be stored. During initializing, it is not editable as it is generated automatically once the ADR base path is specified.

Click **Create**.

3. Once the Support Workbench properties have been initialized, the Support Workbench page displays showing a list of any problems for the Database Machine (Figure 4-4):

Figure 4-4   Support Workbench Page

Oracle Exadata Database Machine Dashboard Creation

You can create a Database Machine dashboard to monitor the performance and usage metrics of the Database Machine system, its sub-components, as well as all the database system components residing on the Database Machine.

• Dashboard Creation for Exadata Database Machine Plug-in Release 12.1.0.3.0 and Later

• How to Make the Report "Public"

• Find All Database Machine Reports

Dashboard Creation for Exadata Database Machine Plug-in Release 12.1.0.3.0 and Later

For Exadata Database Machine plug-in Release 12.1.0.3.0 and later, create the Database Machine Dashboard:

1. Log in to Enterprise Manager.

2. From the Enterprise Manager home page, click the **Enterprise** menu. Select the **Job** submenu, then **Activity**.

3. Select **Database Machine Services Dashboard** from the drop-down menu next to the Create Job option.

4. Click **Go**.

5. Enter a name of the job (for example, `CREATE_DBM_JOB_1`).

6. Click **Add** and select the **DBMachine** target. After adding, make sure the target is selected by clicking on the check box next to it.

7. Click the **Parameters** tab.

   Three options are provided through the drop-down:

   • Select **Create** if it is a new report.

   • Select **Update** for updating an existing report with new components.

   • Select **Cleanup** to remove services created by the Create job executed earlier.

8. Finally, click **Submit** to perform the operation.

   A message `CREATE_DBM_JOB_1 submitted successfully` should display.

   You can monitor the job by clicking on the link corresponding to the job.

How to Make the Report "Public"

The generated report is accessible only by the Enterprise Manager user who creates it. To make the report public:

1. Select the dashboard report from the list of reports shown after following the steps mentioned above.

2. Click **Edit**.

3. Select the **Run report using target privileges of the report owner** option under Privileges section in General tab.

4. Click the **Access** tab.

5. Select the **Allow viewing without logging in to Enterprise Manager** option.

6. Click **OK**.

Find All Database Machine Reports

To find all Database Machine reports:

1. Log in to Enterprise Manager.

2. From the Enterprise Manager home page, click the **Enterprise** menu. Select **Reports**, then **Information Publisher Reports**.

3. Search for the report name. Dashboard report names, one for each Database Machine, are displayed in the following format:

   `[DBMachine Name]_DASHBOARD_REPORT`

4. Click on the report to view the dashboard report.

5

Oracle Exadata Database Machine Administration

This chapter provides the information needed to administer your Oracle Exadata Database Machine through Oracle Enterprise Manager Cloud Control 13*c*. The following topics are discussed:

- Creating Roles to Manage the Plug-in
- View Exadata Database Machine Topology
- Exadata Cell Metrics and Alert Settings
- Exadata Storage Server Management
- Managing the InfiniBand Network
- Flash Cache Resource Monitoring
- Exadata Database Machine Fault Monitoring
- Monitoring Exadata Database Machine Components
- Using the Conversion Wizard to Convert 12*c* Targets to 13*c* Targets

> **Note:**
>
> View a video of how to manage and monitor your Oracle Exadata Database Machine using Oracle Enterprise Manager Cloud Control 13*c*:
>
> https://youtu.be/5S0mlx6cegE

Creating Roles to Manage the Plug-in

To manage the plug-in, you need to create roles and administrators, and then assign roles to administrators. This restricts the privileges that each user has, for example in deleting the plug-in or accessing reports.

> **Note:**
>
> For security reasons, Oracle recommends that the `SYSMAN` account be used only as a template to create other accounts, and not used directly.

To create roles to provide management rights to users:

1. Log in to the Enterprise Manager Cloud Control as the super administrator user.
2. Click **Setup**, then **Security**.

3. Select **Roles**.

   On the Security page, a list of predefined roles is provided. These roles can serve as basis to define custom roles to suite specific site level requirements.

   > **Note:**
   >
   > The predefined roles provided cannot be edited or deleted.

4. Select a role that closely matches the role you wish to create. Click **Create Like**.

5. On the Properties page, enter a name for the role you wish to create. You can optionally add a description.

   Click **Next**.

6. On the Roles page, select the roles from the list of Available Roles. Click **Move** to add the role to Selected Roles.

   Click **Next**.

7. On the Target Privileges page, select the privilege you want to grant to the new role.

   Click **Next**.

8. On the Resource Privileges page, you can edit specific privileges to be explicitly granted. Click the **Manage Privilege Grant** edit icon to make the changes.

   Click **Next**.

9. On the Administrators page, select the administrators from the list of Available Administrators that you want to grant the new role to. Click **Move** to add the administrator to Selected Administrators.

   Click **Next**.

10. On the Review page, a complete summary of the new role you have created is displayed. Click **Back** to go to previous screens to make changes. Click **Finish** to complete the role creation.

When the newly created administrator logs in, unlike `SYSMAN`, the administrator is restricted by the privileges set.

> **Note:**
>
> See *Working with Systems Infrastructure Targets* in *Oracle® Enterprise Manager Cloud Control Administrator's Guide*.

View Exadata Database Machine Topology

Database Machine management simplifies monitoring and managing tasks by integrating all hardware and software components into one entity. You do not need to monitor each target individually, but instead you can view the whole Exadata Database Machine as a single target. You can view all critical issues in the system, monitor per-

formance, and drill down to individual targets from the Database Machine target home page.

The following topology topics are presented in this section:

- Drilling Down to Individual Targets
- Viewing Critical Hardware Information for the Database Machine
- Viewing DB Machine Alerts
- Viewing Metrics
- Adding Exadata Components Manually
- Removing an Exadata Database Machine Target
- Deleting a Component of a Database Machine Target
- Updating the Exadata Database Machine Schematic Diagram

Use the Topology page of Database Machine to view the topology of the system by Cluster or by Database. Clusters are a complete software system starting with a RAC database, the underlying ASM, and CRS. Clusters define one logical entity that is interconnected. The Database Machine could include several clusters, one cluster, or could just be a number of individual databases. While cabinets define the hardware topology of the Database Machine, clusters define the logical or system topology of the Database Machine.

You can view the Topology by Cluster or Database. Click an element in the Topology and view alert data associated with the element.

You can monitor all components of the Database Machine. Database Machine monitors all subcomponent targets, whether hardware or software. This includes the database, ASM, CRS, hosts, Exadata and the InfiniBand network.

To view the topology of an existing Database Machine target:

1. From the **Targets** menu, select **Exadata**.

   Enterprise Manager displays the Oracle Exadata Database Machines page showing all the available Database Machine targets. From this page, you can add hardware components (such as Oracle Exadata Storage Servers, InfiniBand switches, Ethernet Switches, KVM switches, PDU, and compute node ILOM) in the Oracle Database Machine as managed targets.

2. From the Oracle Exadata Database Machines page, select the Oracle Database Machine target whose topology you want to view.

3. From the Oracle Database Machine Home page, click the **Database Machine** menu, then select **Members Topology** from the drop-down menu.

   Enterprise Manager Cloud Control displays the Configuration Topology page.

Drilling Down to Individual Targets

You can drill down immediately to a subcomponent target of the Database Machine (such as RAC, a database instance, or an Exadata cell).

To drill down to individual targets:

1. From the **Targets** menu, select **Exadata**.

Enterprise Manager displays the Oracle Exadata Database Machines page showing all the available Database Machine targets.

2. From the Oracle Exadata Database Machines page, select the Oracle Database Machine target whose components you want to view.

Enterprise Manager displays the Oracle Database Machine Home page showing an Overview, Schematic, and Incident section for the selected Database Machine.

3. From the Oracle Database Machine Home page, use the left navigation panel to expand the list of available targets that comprise the Database Machine.

4. Click the target to which you want to drill down.

Viewing Critical Hardware Information for the Database Machine

You can view critical metrics for all the hardware subcomponents of the Database Machine such as DB hosts, Exadata Storage Servers, InfiniBand switches and so on. These metrics vary for different component targets. For example, database server nodes and Exadata servers include the CPU, I/O, and storage metrics.

To view critical hardware-centric information for the entire Database machine:

1. From the **Targets** menu, select **Exadata**.

Enterprise Manager displays the Oracle Exadata Database Machines page showing all the available DB Machine targets.

2. From the Oracle Exadata Database Machines page, select the Oracle Database Machine target whose hardware information you want to view.

3. From the Oracle Database Machine Home page, view the hardware schematic of the Database Machine.

Viewing DB Machine Alerts

You can view alerts on the Database Machine and drill down to details about each alert. These alerts may be performance/configuration metrics or hardware faults.

To view Database Machine alerts:

1. From the **Targets** menu, select **Exadata**.

Enterprise Manager displays the Oracle Exadata Database Machines page showing all the available DB Machine targets.

2. From the Oracle Exadata Database Machines page, select the Oracle Database Machine target whose machine configuration information you want to view.

Enterprise Manager displays the Oracle Database Machine home page on which you can see all alerts associated with the current DB Machine.

Viewing Metrics

To view the Exadata metrics:

1. Navigate to the Exadata Cell home page by choosing the Exadata target from the All Targets page of Enterprise Manager.

Enterprise Manager displays the Exadata Cell Home page for the target you selected.

2. From the Exadata Storage Server drop-down menu, choose **Monitoring** and then **All Metrics**.

   The All Metrics page appears where you can a wide variety of Exadata metrics. For a complete description of the Exadata metrics available, see the "Oracle Exadata" chapter of the *Oracle® Enterprise Manager Oracle Database and Database-Related Metric Reference Manual*:

   http://docs.oracle.com/cd/E24628_01/em.121/e25160/oracle_exadata.htm

Adding Exadata Components Manually

You can add Exadata components manually using the following steps:

1. From the **Setup** menu, select **Add Target**, then select **Add Targets Manually**.

   Enterprise Manager displays the Add Targets Manually page where you can choose the type of target you want to add.

2. From the Add Targets Manually section, choose **Add Non-Host Targets by Specifying Target Monitoring Properties**.

3. In the **Target Type** combo box, choose the appropriate target type, for example, KVM for kvm, PDU for pdu, Cisco switch for Cisco, and Oracle ILOM Server for ilom plug-in).

4. Choose the monitoring agent using the search option.

5. Click **Add Manually** and provide the required properties

Removing an Exadata Database Machine Target

To delete and Exadata Database Machine target, you have the choice to:

- Remove all members of the Oracle Exadata Database Machine. If the member target is shared with another Database Machine target, then the member target will not be deleted and will continue to be monitored. In other words, the member targets will be deleted if they are associated with only this Database Machine target.

- Remove only system members of the Oracle Exadata Database Machine. The other member targets will not be deleted and will continue to be monitored. They can be associated to another Oracle Exadata Database Machine, if required.

To remove an Exadata Database Machine target:

1. From the Database Machine target menu, select **Target Setup**, then select **Remove Target**.

2. On the Remove page, select whether to remove all members or to remove only the system members.

   If you choose to remove all members, then you also have an additional option to unsubscribe SNMP subscriptions for member Exadata Storage Servers and Infiniband Switches. Specify the appropriate user credentials to unsubscribe the SNMP subscriptions.

3. Click **Yes** to initiate the remove job.

> **Note:**
>
> Host targets for the compute nodes and any targets that are also member targets of another Oracle Exadata Database Machine target will not be removed. System and non-system targets include:
>
> **System Targets**:
>
> - Oracle Exadata Database Machine
> - Oracle Infiniband Network (*Enterprise Manager 12c target*)
> - Oracle Exadata Storage Server Grid
>
> **Non-System Targets**:
>
> - Oracle Exadata Storage Server
> - Oracle Exadata KVM
> - Systems Infrastructure Switch
> - Systems Infrastructure PDU
> - Systems Infrastructure Rack
> - Oracle Infiniband Switch (*Enterprise Manager 12c target*)
> - Oracle Engineered System Cisco Switch (*Enterprise Manager 12c target*)
> - Oracle Engineered System PDU (*Enterprise Manager 12c target*)
> - Oracle Engineered System ILOM Server (*Enterprise Manager 12c target*)

Deleting a Component of a Database Machine Target

If you need to remove a component of an Exadata Database Machine target, you can perform this task within Enterprise Manager Cloud Control 13*c*:

1. From the DB Machine home page's Target Navigation pane, right-click on the target item you wish to remove. You may need to expand the Exadata Grid item to view all of the available cells.

2. Select **Target Setup**, then **Remove Target**.

3. A warning page will display to confirm the target deletion. Click **Yes** to continue.

Updating the Exadata Database Machine Schematic Diagram

In some cases, the Exadata Database Machine schematic diagram is not displaying the components correctly. For example:

- You may have successfully discovered the Exadata Database Machine, but some components are not displaying correctly in the Exadata schematic diagram. Instead, an empty slot is shown in place of the component.

- The Exadata Database Machine schematic diagram shows shows the status of the component as "red/down" where as individual components would really show that they are up and running fine.

- You want to re-locate or rearrange the order of the components in the slots of Exadata Database Machine schematic diagram.

To accomplish these tasks, you will need to drop a component from the schematic diagram and add the correct one:

- Drop a Component from the Exadata Database Machine Schematic Diagram

- Add Components to the Exadata Database Machine Schematic Diagram

Drop a Component from the Exadata Database Machine Schematic Diagram

To drop a component from the Exadata Database Machine schematic diagram:

1. From the Targets menu, select **Exadata**.

2. On the Exadata Database Machine schematic diagram, click **Edit** as shown in Figure 5-1:

Figure 5-1   Schematic Diagram Edit Button

3. Right-click on the component you want to drop. In the pop-up window, select **Delete Component** as shown in Figure 5-2:

Figure 5-2   Delete Component

4. Ensure you have selected the correct component in pop-up shown and click OK as shown in Figure 5-3:

Figure 5-3   Confirm Delete
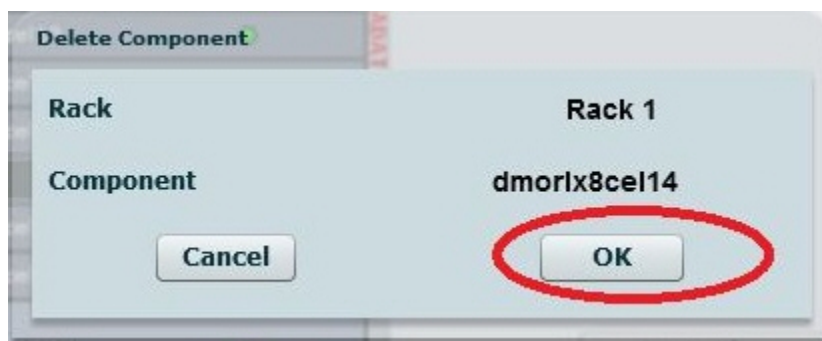
5. The Exadata Database Machine schematic diagram will refresh to show the empty slot, as shown in Figure 5-4:

Figure 5-4   Refreshed Schematic Diagram with Empty Slot

6. Once you see the component deleted in the slot you specify, click **Done** on the Exadata Database Machine schematic diagram.

Add Components to the Exadata Database Machine Schematic Diagram

To add a component from the Exadata Database Machine schematic diagram:

1. From the Targets menu, select **Exadata**.

2. On the Exadata Database Machine schematic diagram, click **Edit**.

3. Right-click on the empty slot for the component you want to add. In the pop-up window, select **Add Component** as shown in Figure 5-5:

Figure 5-5   Add Component
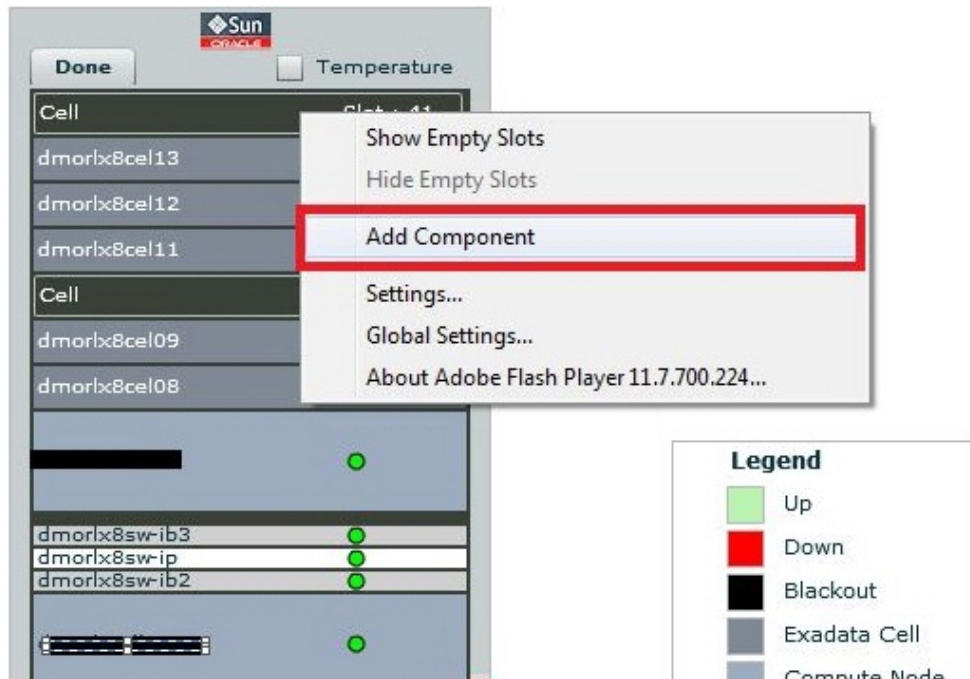
4. If there are multiple components to be added to schematic diagram, select the correct component from the **Component** drop-down menu, as shown in Figure 5-6:

Figure 5-6   Add Multiple Components

Also select the correct slot number in **Available Location (Unum)** drop-down menu, as shown in Figure 5-7:

Figure 5-7   Available Location
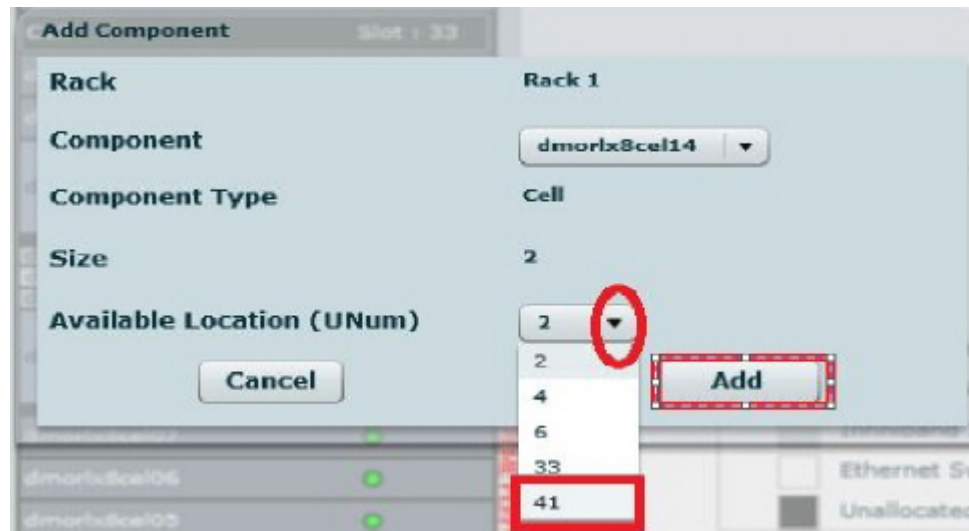
Click **Add**.

5. Once you see the component added in the slot you specify, click **Done** on the Exadata Database Machine schematic diagram.

Exadata Cell Metrics and Alert Settings

To access the settings for Exadata Cell metrics/alert:

1. From the Enterprise Manager home page, select **Targets**, then **Exadata**. Select an Exadata Storage Server from the list.

2. From the Exadata Storage Server menu, click **Monitoring**, then **All Metrics** to display all editable metric alert setting.

3. To change a setting, click **Monitoring**, then **Metric and Collection Settings** from the Exadata Storage Server menu. The default View option "Metrics with thresholds" is displayed. You can modify the following parameters:

   • Warning Threshold

   • Collection Schedule - click the link to set a collection schedule.

   • Click the Edit icon [icon] for advanced settings.

4. Click **OK** to save any changes.

Exadata Storage Server Management

This section provides introductory instructions for managing Exadata Storage Servers. The following topics are presented:

   • About Exadata Storage Server

   • Using Exadata As a Cloud Control Target

   • Viewing an Exadata Storage Server Configuration

- Performing Administration Tasks on Exadata Storage Servers
- Managing the IO Resource
- Diagnosing Exadata Cell Alerts
- Accessing Oracle Support Workbench for Exadata Storage Server
- Deleting a Component of a Database Machine Target

About Exadata Storage Server

An Exadata Storage Server is a network-accessible storage array with Exadata soft-ware installed on it. Use the Exadata Home page to manage and monitor the Oracle Exadata Storage Server (also known as Exadata cell) by managing it as an Enterprise Manager Cloud Control target. You can discover and consolidate management, moni-toring and administration of a single or a group of Oracle Exadata Storage Servers in a datacenter using Enterprise Manager.

Exadata Storage Servers can be discovered automatically or manually. Once discov-ered, you can add them as Enterprise Manager targets. The individual Exadata Stor-age Server is monitored and managed as an Enterprise Manager target and provides the exception, configuration and performance information.

Grouping of Exadata Storage Servers is used for easy management and monitoring of the set of Storage Servers. You can group them both manually and automatically. The grouping function provides an aggregation of exceptions, configuration and perform-ance information of the group of cells.

You can view performance analysis by linking Exadata performance both at a cell level and group level to ASM and database performance. You can drill down to Exadata configuration and performance issues from both the database and ASM targets.

Storage Grid (for example, multiple database/ASM instances sharing the same Exada-ta Storage Server) is supported to the same extent as dedicated storage.

Using Exadata As a Cloud Control Target

Use Oracle Exadata to manage and monitor the Oracle Exadata Storage Server (also known as Exadata cell) by managing the Exadata cells as Enterprise Manager Cloud Control targets. You can discover and consolidate management, monitoring and ad-ministration of a single or a group of Oracle Exadata Storage Servers in a datacenter using Enterprise Manager.

Exadata cells can be discovered automatically or manually. Once discovered, you can add the Exadata cells as Enterprise Manager targets.

The individual Exadata cell is monitored and managed as an Enterprise Manager tar-get and provides the exception, configuration and performance information.

Grouping of Exadata cells is used for easy management and monitoring of the set of Exadata cells. You can group Exadata cells both manually and automatically. The grouping function provides an aggregation of exceptions, configuration and perform-ance information of the group of cells.

You can view performance analysis by linking Exadata performance both at a cell level and group level to ASM and database performance. You can drill down to Exadata configuration and performance issues from both the database and ASM targets.

Viewing an Exadata Storage Server Configuration

You can view the configuration of an Oracle Exadata Storage Server target by following the steps below:

1. Navigate to the Exadata Storage Server home page by choosing the Exadata target for which you want to view the IORM Performance page from the All Targets page.

   Enterprise Manager displays the Exadata Storage Server Home page for the target you selected.

2. From the Target menu, choose **Configuration** and then **Topology**.

   Enterprise Manager displays the Configuration Topology page for the selected Exadata Storage Server. The topology page provides a visual layout of a the target's relationships with other targets. From this page you can:

   • Do a target search filtered by target status/events/target type)

   • Select from a set of relationships to represent in the graph

   • Select annotations to display in the graph, such as alerts and link labels

   • Select from a set of options: view navigator, expand or collapse all, toggle graph layout, reload topology

   • Print

   • Zoom via the slide control

   • Pan via the navigator control

   • Toggle the presentation from graph to table

   When you hover over a node or group member, a popup displays detailed information about the entity. A link can appear in the popup to more detailed information such as customer documentation.

Performing Administration Tasks on Exadata Storage Servers

To perform an administration operation on an Exadata Storage Server, such as executing a cell command, follow these steps:

1. Navigate to the Exadata Storage Server home page by choosing the Exadata target for which you want to perform an administrative task from the All Targets page.

   Enterprise Manager displays the Exadata Storage Server Home page for the target you selected.

2. Click **Target**, then select **Administration**.

   From this menu you can choose either **Execute Cell Command, Support Workbench,** or **Manage IO Resource**.

3. Click **Execute Cell Command**.

   The Command page of the Exadata Storage Server Administration wizard appears. Enter a CELLCLI command as the administrative command to be executed on the cell. You must read the Command Instructions before you enter a command. Only a single CELLCLI command is allowed to execute. You must enter the command without the `cellcli -e` prefix, which is automatically appended when

you submit the command. Finally, you cannot use the following characters: ; / ' < > / |.

4. Click **Next** to continue.

   Enterprise Manager displays the Admin Credentials page. Select or enter the Administration credentials to execute the command. The credentials you enter are used when submitting the operation. You can choose between Preferred Credentials, Named Credentials, and New Credentials. You can also click **More Details** to view information about Credential Type, Last modified, Credential Name, Credential Owner, Last Modified Date, Last Modified By, and Preferred Credentials Set At.

5. Click **Next**.

   Enterprise Manager displays the Schedule page. Use the Schedule page to schedule the administration task. Enter the Job Name and the Job Description, then provide the job information in the Schedule the Administration Job section. You can choose to begin the job immediately or enter the time you want the job to begin.

6. Click **Next** to continue.

   The Summary page displays. Use the Summary page to ensure you have entered the correct values and then submit the command. The Summary page lists the Job Name, Description, Command to Execute, when the job is Scheduled, and the Selected Cell.

7. Click **Submit Command** to submit the job.

   The Job Status page displays. Use the Job Status page to link to the Job Detail page of the administration task.

Managing the IO Resource

Oracle Exadata Database Machine Cells are added as targets during the database machine discovery workflow (see Exadata Database Machine Discovery) and are grouped automatically under the group **Exadata Storage Server Grid**.

To access the IORM Performance page:

1. Select an Exadata Storage Server cell. One way to select the cell:

   a. From the Targets menu, select **Exadata**.

   b. Select a DB Machine from the list of Target Names.

   c. In the Target Navigation pane, expand the Exadata Grid item and click one of the cells.

2. Once you have selected an Exadata Storage Server cell, click the **Exadata Storage Server** menu, select **Administration**, then **Manage IO Resource**.

Once you have accessed the IORM page, you can make the following modifications:

• Add/Update IORM Configuration

• The Inter-Database Plan

The IORM Monitoring section of the page provides a view of the performance statistics of Disk IO (Wait, IOPS, MBPS, Utilization, Latency, and Objective charts). These statistics help to identify which databases and consumer groups are using the available

resources. They also help to adjust the IORM configuration (using IORM Settings section on the same page) as needed.

For further details on managing I/O resources, refer to the *Managing I/O Resources* chapter in the *Oracle® Exadata Storage Server Software User's Guide*.

Add/Update IORM Configuration

To update the I/O Resource Manager (IORM) settings (for Exadata Storage Server software release 12.1.2.1.0 and later):

1. Navigate to the IORM Performance page as described above. Figure 5-8 shows the I/O Resource Manager (IORM) Settings pane.

Figure 5-8   I/O Resource Manager (IORM) Settings

> **✎ Note:**
>
> You can also update a single cell. Expand the Exadata Grid group to view all cells associated with the group. Click the cell you want to update.
>
> The steps to update the IORM settings is the same for a single cell or group of cells.

2. From the Database Name column, select a database from the drop-down menu.

3. Enter a value for the Hard Disk I/O Utilization Limit column.

4. Enter a value for the Database I/O Share column.

5. Enter minimum and maximum values (in MB) for the Flash Cache column.

6. In the Disk I/O Objective drop-down menu, select an objective from the list (**Auto** is the default):

    • **Low Latency** - Use this setting for critical OLTP workloads that require extremely good disk latency. This setting provides the lowest possible latency by significantly limiting disk utilization.

- **Balanced** - Use this setting for critical OLTP and DSS workloads. This setting balances low disk latency and high throughput. This setting limits disk utilization of large I/Os to a lesser extent than Low Latency to achieve a balance between good latency and good throughput.

- **High Throughput** - Use this setting for critical DSS workloads that require high throughput.

- **Auto** - Use this setting to have IORM determine the optimization objective. IORM continuously and dynamically determines the optimization objective, based on the workloads observed, and resource plans enabled.

- **Basic** - Use this setting to disable I/O prioritization and limit the maximum small I/O latency.

Click **Update**. The Exadata Cell Administration Wizard will appear prompting you for the information necessary to complete the Disk I/O Objective configuration:

a. On the Command page, the Cell Control Command-Line Interface (CellCLI) value should be:

```
# alter iormplan objective = 'auto'
```

Click **Next**.

b. On the Admin Credentials page, enter the username and password for the selected cells.

Click **Next**.

c. On the Schedule page, enter a job name (required) and job description (optional). Select an option to start **Immediately** or **Later**. If you select the Later option, enter the time you want the job to run.

Click **Next**.

d. On the Review page, verify the settings are correct. If there are no changes, click **Submit Command**.

e. Once the job is successfully submitted, the Job Status page will display.

Click **Return** to return to the I/O Resource Manager (IORM) Settings pane.

7. Click **Get Latest** to refresh the page, which will include your Disk I/O Objective selection.

8. Confirm the IORM objective settings. From the command line, run the following command:

```
# dcli -g cell_group cellcli -e "list iormplan attributes objective"
```

Output should show a value of **auto**:

```
cell01: auto
cell02: auto
cell03: auto
.
.
.
cell14: auto
```

The Inter-Database Plan

An inter-database plan specifies how resources are allocated by *percentage* or *share* among multiple databases for each cell. The directives in an inter-database plan specify allocations to databases, rather than consumer groups. The inter-database plan is configured and enabled with the CellCLI utility at each cell.

The inter-database plan is similar to a database resource plan, in that each directive consists of an allocation amount and a level from 1 to 8. For a given plan, the total allocations at any level must be less than or equal to 100 percent. An inter-database plan differs from a database resource plan in that it cannot contain subplans and only contains I/O resource directives. Only one inter-database plan can be active on a cell at any given time.

You can view the current configured inter-database plan and update an existing Percentage/Share based inter-database plan and a new Percentage/Share based plan can be configured using the Add/Remove options.

You can also view Share, Percentage Radio buttons and a drop down with Basic, Advance options.

> **✎ Note:**
>
> If the Exadata plug-in version is 12.1.0.3.0 and earlier or if the Exadata Storage Server version is 11.2.3.1.0 or earlier, the Share, Percentage based inter-database plan radio buttons are not available. You can view only Percentage-based options (that is, the drop-down only displays the Basic, Advance options).

When considering an inter-database plan:

- If Oracle Exadata Storage Server is only hosting one database, then an inter-database plan is not needed.

- If an inter-database plan is not specified, then all databases receive an equal allocation.

For further details on the inter-database plan, refer to the *About Interdatabase Resource Management* section in the *Oracle® Exadata Storage Server Software User's Guide*.

Diagnosing Exadata Cell Alerts

Enterprise Manager listens for Exadata Cell alerts sent from the Exadata Cell Management Server; so, any hardware failure or cell error will be reported in Enterprise Manager. For detailed cell error code and its interpretation, refer to the *Hardware Alert Messages* section in Appendix B, "Alerts and Error Messages" of the *Oracle® Exadata Storage Server Software User's Guide*.

Managing the InfiniBand Network

All InfiniBand Switches are discovered automatically during the database machine discovery workflow (see Exadata Database Machine Discovery) and are grouped automatically under the group **IB Network**.

1. From the Enterprise Manager home page, select **Targets**, then **Oracle Exadata Database Machine**.

2. In the Target Navigation pane, select **IB Network** from the list.

3. In the IB Network pane, you can view an overview and activity summary for all InfiniBand Switches.

4. Click **Refresh** for an On Demand refresh of the InfiniBand schematic. Updates reflect the real-time data.

The following topics address managing your InfiniBand network:

- InfiniBand Metrics
- Performing Administration Tasks on Infiniband Networks
- Setting Up Alerts

InfiniBand Metrics

The following metrics are available for your InfiniBand Network:

- Aggregate Sensor
- Response
- Switch Configuration

Aggregate Sensor

The Aggregate Sensor takes input from multiple sensors and aggregates the data to identify problems with the switch that require attention. Whenever the sensor trips into an "Asserted" state (indicating a problem) or "Deasserted" (indicating that the problem is cleared) for a component on the switch, associated Enterprise Manager events will be generated.

Response

This is the main metric indicating availability of the InfiniBand switch. It is collected every 60 seconds by default through the management interface of the switch.

Switch Configuration

This metric captures the switch configuration. The information collected is valuable only to Oracle Support, which will use it to assist in debugging situations.

Performing Administration Tasks on Infiniband Networks

To perform an administration operation on an Infiniband Network, follow these steps:

1. Navigate to the DB Machine home page of the Infiniband Network by choosing the DB Machine for which you want to perform an administrative task from the All Targets page.

   Enterprise Manager displays the DB Machine Home page for the target you selected.

2. Select the IB Network for which you want to perform an administrative task.

3. From the Target menu item, choose **Administration**.

   The Target & Command page of the Infiniband Network Administration wizard appears.

4. Choose the **Target Type** and then select the target on which you want to perform the administrative task from the Target drop-down list. Enter the administrative command you want to execute. The available operations from which you can select are dependent on the target type and target you selected. Once you choose the operation, you may need to select a value that will appear after choosing the operation.

5. Click **Next** to continue.

   Enterprise Manager displays the Credentials & Schedule page. Select or enter the credentials to execute the command. The credentials you enter are used when submitting the operation. You can choose between Preferred Credentials, Named Credentials, and New Credentials. Schedule the administration task. Provide the job information in the **Administration Job Schedule** section. You can choose to begin the job immediately or enter the time you want the job to begin

6. Click **Next** to continue.

   The Review page appears. Use the Review page to ensure you have entered the correct values and then submit the command. The Review page lists the Job Name, Description, Command to Execute, when the job is Scheduled, the Target Type, and the Selected Target.

7. Click **Submit Command** to submit the job.

   When you click Submit Command, a popup is shown if the job is successful. You can go to the Job Detail Page or back to the page from where this wizard was launched.

Setting Up Alerts

After configuring the InfiniBand Switch targets to send SNMP alerts, set up alerts in Enterprise Manager Cloud Control.

1. Log in to Enterprise Manager Cloud Control.

2. Click **Targets**, then **All Targets**. All discovered targets will display.

3. In the *All Targets* page, click **Oracle Exadata InfiniBand Switch**.

4. Click the target you are interested in. The target home page appears.

5. In the drop-down menu for the Oracle Exadata InfiniBand Switch, select **Metric and Collection Settings**.

6. In the *Metric and Collection Settings* page, you can modify metric threshold values, edit monitoring settings for specific metrics, change metric collection schedules, and disable collection of a metric.

You can modify the thresholds directly in the table or click the edit icon (pencil icon) to access the Edit Advanced Settings page. For more information on the fields displayed in this page and how the thresholds can be modified, click **Help** from the top-right corner of this page.

Flash Cache Resource Monitoring

The Oracle Exadata plug-in release 13.1.0.1.0 and later provides flash cache resource monitoring for Oracle Exadata Storage Servers. From the Storage Server home page or from the IO Distribution Detail page, Cloud Control provides a high-level overview of flash cache resources (Figure 5-9). Details include:

- I/O Utilization (as a percentage).
- Hard Drive I/O Time Breakdown (in milliseconds per request).
- Flash I/O Time Breakdown (in milliseconds per request).

Figure 5-9   I/O Distribution by Databases
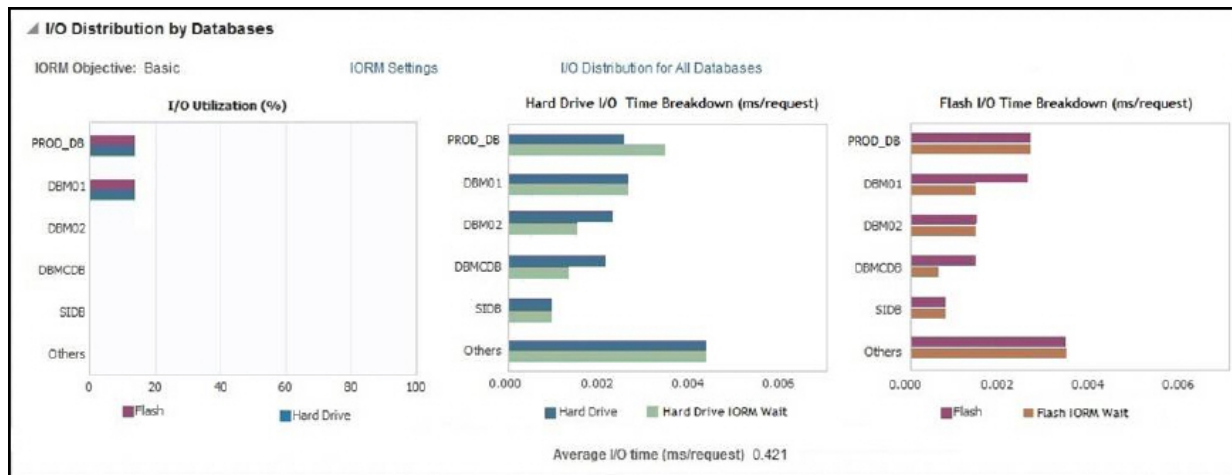
From the IO Distribution Details page, which provides a view of all available databases statistics, select **Table View** (the default is Graph View) to view the data as a table (Figure 5-10):

Figure 5-10   I/O Distribution by Databases - Table View

I/O Distribution for All Databases
Average I/O time (ms/request): 0.514   IORM Objective: Basic   Last Collected at Feb 27, 2015 2:15:00 PM GMT

Graphic View   Table View

Database	I/O Utilization (%)		Hard Drive I/O Time Breakdown (ms/request)		Flash I/O Time Breakdown (ms/request)	
	Hard Drive	Flash	Latency	IORM Wait Time	Latency	IORM Wait Time
ASM	0	0	0.001	0.003	0	0
DBM01	0	0	0.001	0.008	0.001	0
DBM03	0	0	0.001	0.003	0.001	0
DBMCDB	0	0	0.001	0.004	0.001	0
Others	0	0	0.001	0.007	0.001	0.006

The IORM Performance Page (Figure 5-11) provides detailed metrics, such as Average Throttle Time for Disk I/Os for both hard drives and flash drives. Select Flash Cache Space Usage (Figure 5-12) for detailed performance about flash cache space.

Figure 5-11   IORM Performance Page

Figure 5-12   IORM Performance - Flash Cache Space Usage
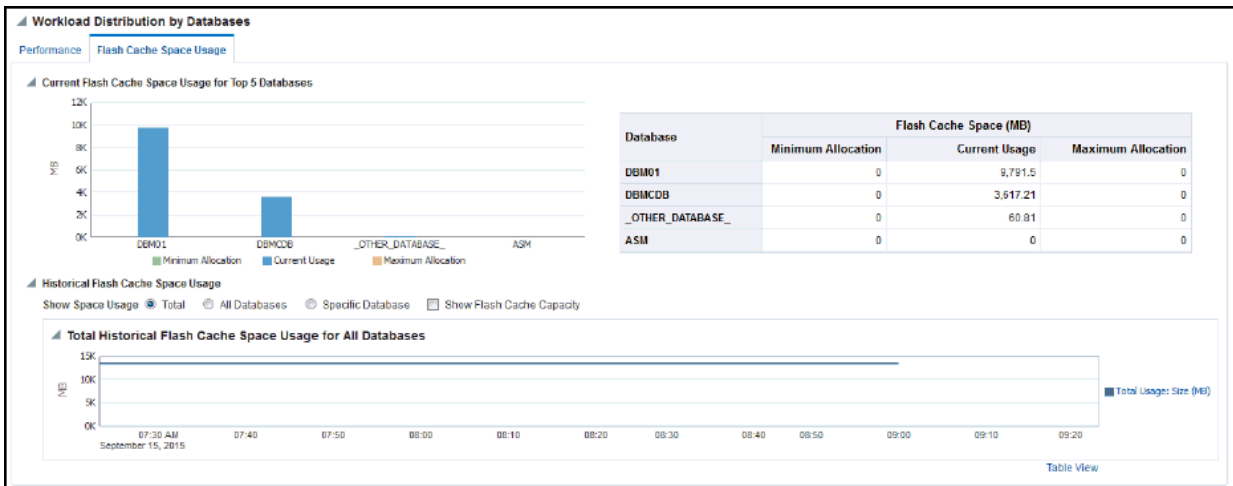
Exadata Database Machine Fault Monitoring

Oracle Enterprise Manager Cloud Control provides hardware fault monitoring for Oracle Exadata Database Machine. Table 5-1 shows the fault monitoring for the Exadata Storage Server. Table 5-2 shows the fault monitoring for the compute nodes.

> **Note:**
>
> The fault monitoring information in the following tables, while comprehensive, may not always be complete. As new fault monitoring functionality is added, these tables will be updated accordingly.

Table 5-1   Exadata Storage Server Fault Monitoring

Area	Fault Monitoring
Access	Cell cannot be accessed (e.g. ping failure).
Memory	Memory Controller Error
	Memory DIMM Error
	Memory Channel Error
	Memory DIMM Temperature Sensor Error
	Memory Correctable ECC Error
CPU	Internal Processor Error
	Intel 5500 Chipset Core Error
	Data Cache Error
	Cache Error
	Instruction Cache Error
ESM	ESM Battery Charge Error
	ESM Battery Life Error
Hard Disk	SCSI Error for Media, Device
	Disk Temperature Threshold Excess
	Physical Disk Not Present
	Block Corruption
Flash Disk	Flash Disk Failure
	Flash Disk Predictive Failure
	Flash Disk not Present
Miscellaneous	Chassis or Power Supply Fan Error
	PCI-E Internal Error
	Power Supply Voltage Excess Error
	Temperature Excess Error
	Network Port Disconnection and Fault

Table 5-2   Compute Node Fault Monitoring

Area	Fault Monitoring
Memory	Memory Controller Error
	Memory DIMM Error
	Memory Channel Error
	Memory DIMM Temperature Sensor Error
	Memory Correctable ECC Error
CPU	Internal Processor Error
	Intel 5500 Chipset Core Error
	Data Cache Error
	Cache Error
	Instruction Cache Error
Disk	SCSI Error for Media, Device
	Disk Temperature Threshold Excess
	Block Corruption
Miscellaneous	Chassis or Power Supply Fan Error
	Non-fatal PCI-E Internal Error
	Power Supply Voltage Excess Error
	Temperature Excess Error
	Network Port Disconnection and Fault

Monitoring Exadata Database Machine Components

Enterprise Manager collects details for the following components:

- Storage Cells
- InfiniBand Switches
- Cisco Switch
- ILOM Targets
- Power Distribution Units (PDUs)
- KVM Switch

Storage Cells

An Enterprise Manager Agent runs the `cellcli` command via `ssh` to collect Storage Cell metrics. SNMP traps are sent to the Enterprise Manager Agent for subscribed alert conditions.

Monitoring requires the `cellmonitor ssh eq` setup with an Agent user.

ASM targets and disk groups are associated.

On the home page, rich storage data is collected, including:

- Aggregate storage metrics.
- Cell alerts via SNMP (PUSH).

- Capacities.

- IORM consumer and Database-level metrics.

InfiniBand Switches

An Enterprise Manager Agent runs remote `ssh` calls to the InfiniBand switch to collect metrics. The InfiniBand Switch sends SNMP traps (PUSH) for all alerts.

Monitoring requires `ssh eq.` for the `nm2user` for metric collections such as:

- Response

- Various sensor status

  - Fan

  - Voltage

  - Temperature

- Port performance data

- Port administration

Cisco Switch

An Enterprise Manager Agent runs a remote SNMP `get` call to collect metric data for the Cisco switch, including details on:

- Status / Availability

- Port status

- Vital signs: CPU, Memory, Power, Temperature

- Network interface various data

  - Incoming traffic errors, traffic kb/s and %

  - Outgoing traffic errors, traffic kb/s and %

  - Administration and Operational bandwidth Mb/s

ILOM Targets

An Enterprise Manager Agent runs remote `ipmitool` calls to each Compute Node ILOM target. Monitoring requires the `nm2user` user credentials to run `ipmitool`.

The following details are collected:

- Response – availability

- Sensor alerts

  - Temperature

  - Voltage

  - Fan speeds

  - Configuration Data: Firmware version, serial number, and so forth.

Power Distribution Units (PDUs)

An Enterprise Manager Agent runs remote SNMP `get` calls and receives SNMP traps (PUSH) from each PDU. Collected details include:

- Response and `ping` status.
- Phase values.

KVM Switch

An Enterprise Manager Agent runs remote SNMP `get` calls and receives SNMP traps (PUSH) from the KVM switch. Collected details include:

- Status and response.
- Reboot events.
- Temperature.
- Fan status.
- Power state.
- Factory settings.

Using the Conversion Wizard to Convert 12*c* Targets to 13*c* Targets

To convert an Exadata Database Machine discovered by Enterprise Manager 12*c* to be monitored by Enterprise Manager 13*c*:

1. From the Database Machine menu, select **Convert 12c Member Targets** ():

Figure 5-13   Convert 12c Member Target Menu
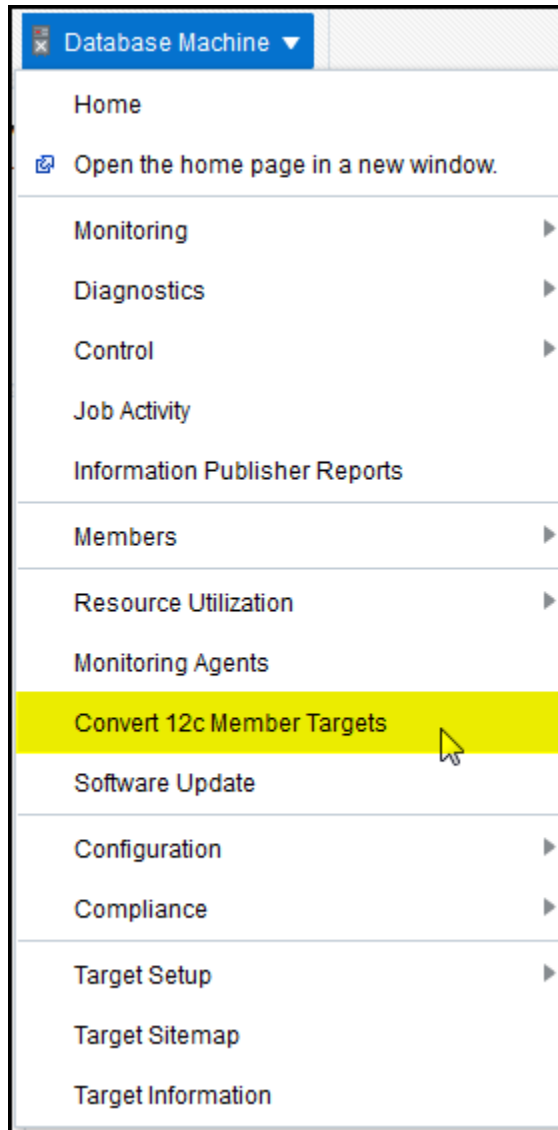
2. Select a **Conversion Option** (Figure 5-14):

   - (Default) Delete 12*c* targets and their historical data. This option halts all monitoring of legacy targets and deletes the historical data. This options allows for a clean start for all Enterprise Manager 13*c* target monitoring.

   - Retain 12*c* targets and their historical data. This option preserves the historical data for legacy targets.

Figure 5-14   Database Machine Conversion: Conversion Option

Once you have selected a conversion option, click **Next**.

3. Set the **Credentials** (Figure 5-15). For the conversion, you must set the credentials for the Exadata Database Machine components to be converted.

Figure 5-15   Database Machine Conversion: Credentials

From the **Set Credential** menu, you can set the credentials for a single component or for the entire component types:

• InfiniBand Switch (Figure 5-16)

Enter the username and password for the InfiniBand Switch's ILOM administration.

In the SNMP Credentials section:

If you select **SNMP V1** from the Credential type drop-down, then enter **public** for the Community String.

If you select **SNMP V3** credentials for the Credential Type, then enter a username and authorization password, select an authorization protocol, and enter a privacy password, as shown in Figure 5-17:

Figure 5-16   InfiniBand Switch Credentials
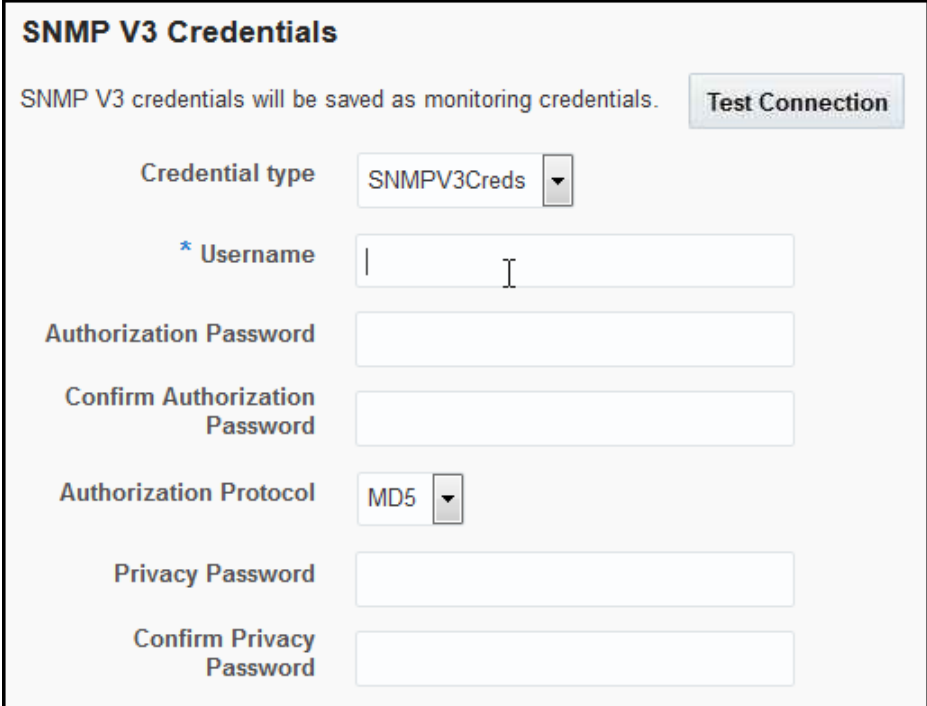
Figure 5-17   InfiniBand Switch SNMP V3 Credentials

Click **Test Connection** for any credential to verify the connection. Click **OK**.

*   Compute Node Server ILOM

    To set the Compute Node Server ILOM, select **New** and enter a username and password, as shown in Figure 5-18:

Figure 5-18   Compute Node Server ILOM Credentials

Click **Test Connection** for any credential to verify the connection. Click **OK**.

- Ethernet Switch (Figure 5-19)

  To set the Ethernet Switch credentials, enter the Cisco IOS username, pass-word, and privileged EXEC password. For the SNMP V3 credentials, enter a username and authorization password, select an authorization protocol, and enter a privacy password.

Figure 5-19   Ethernet Switch Credentials

Click **Test Connection** for any credential to verify the connection. Click **OK**.

- PDU

  To set the HTTP monitoring credentials, select **New** and enter a username and password. For the SNMP V3 credentials, enter a username and authoriza-tion password, select an authorization protocol, and enter a privacy password.

Figure 5-20   PDU Credentials

Click **Test Connection** for any credential to verify the connection. Click **OK**.

Once you have set the credentials, the Credentials page will update to show the credentials set for all components to be converted. Click **Next**.

4. **Review** the components to be converted in the following three sections (Figure 5-21):

   • **Summary**: This section summarizes the number of targets to be converted and if any targets will have additional monitoring information available to you after the conversion.

   • **Targets to be Converted**: This table shows all Enterprise Manager 12*c* targets to be converted for monitoring by Enterprise Manager 13*c* and provides the new target name information.

   • **Targets Not Impacted by Conversion**: All components of the Exadata Database Machine do not need to be converted to be monitored by Enterprise Manager 13*c*. This list identifies those components that to not need to be converted. These components are already monitored by Enterprise Manager 13*c*.

Figure 5-21   Database Machine Conversion: Review

Click **Submit** to begin the conversion.

5. A **Processing** pop-up window will appear (Figure 5-22), which shows you the status of the conversion and a summary of the success or failure of the components to be converted.

    Do not close this window until the processing is complete!

Figure 5-22   Processing Targets

You can select the option to close the window after the processing is complete, or click **Done**.

6. Once processing is complete, a **Conversion Results** page (Figure 5-23) provides a summary of the components converted and details of each component that succeeded or failed to be converted:

Figure 5-23   Database Machine Conversion: Conversion Result

From this page, click **Convert Remaining 12c Targets** to repeat the conversion process for those components that failed to be converted. Click **Launch New Database Machine Home Page** to view the updated home page with all converted components monitored by Enterprise Manager 13*c*.

6
Virtualized Exadata Database Machine

This chapter describes how to manage and monitor a virtualized Oracle Exadata Database Machine with DB clusters using Oracle Virtual Machine (OVM) for x86 and Oracle Exadata Storage Servers in Exadata plug-in 12.1.0.6 and later.

The Exadata plug-in discovers, manages, and monitors virtualized Exadata Database Machine in conjunction with the Virtualization Infrastructure plug-in. For details about this plug-in, see Direct Monitoring of Xen Based Systems in *Oracle® Enterprise Manager Cloud Administration Guide*:

`http://docs.oracle.com/cd/E24628_01/doc.121/e28814/direct_monitor_cs.htm#EMCLO531`

The following sections describe how to discover a virtualized Exadata Database Machine and other supported targets:

- Integration with Virtualization Infrastructure Plug-in
- Discovering Virtualized Exadata Database Machine
- Post-Discovery Configuration
- Exadata Virtualized Provisioning
- Viewing Virtualized Exadata Database Machine
- Resource Utilization Graphs

Once you have completed the discovery of a virtualized Exadata Database Machine, continue with the configuration steps outlined in Post-Discovery Configuration and Verification.

Integration with Virtualization Infrastructure Plug-in

The physical server (physical Oracle Server target), `Dom0` (Virtual Platform target), and `DomU` (virtual Oracle Server target) are discovered and monitored by the Virtualization Infrastructure (VI) plug-in.

The Exadata discovery can work with the VI plug-in by the physical server, `Dom0`, and `DomU` are discovered using the VI plug-in before Exadata Database Machine discovery. During Exadata discovery, the discovery code looks up the existing Virtual Platform target that corresponds to the `Dom0` of the compute node.

The Exadata discovery flow with VI plug-in integration includes the following checks:

1. Check whether the Exadata Database Machine is virtualized based on the configuration metric of the host target of the discovery agent.

2. Check whether the VI plug-in is deployed. If not, you will be prompted to deploy it as described in Direct Monitoring of Xen Based Systems in *Oracle® Enterprise Manager Cloud Administration Guide*:

   `http://docs.oracle.com/cd/E24628_01/doc.121/e28814/direct_monitor_cs.htm#EMCLO531`

Discovering Virtualized Exadata Database Machine

With virtualized Exadata, one Exadata Database Machine target will be created for each physical Database Machine instead of one DB Machine target for each DB cluster deployed through OEDA. Compute nodes, Exadata Storage Servers, InfiniBand switches, compute node ILOM, PDU, KVM, and Cisco switches targets are discovered by the Exadata plug-in.

With only the compute nodes virtualized, the physical servers, `Dom0` and `DomU`, are monitored by the Virtualization Infrastructure (VI) plug-in. The Exadata plug-in is integrates with the VI plug-in for discovery and target management as discussed below.

The hardware targets in virtualized Exadata are discovered in almost the same way as physical Exadata (see Discovering an Exadata Database Machine) except as noted below:

- The `Dom0` of the compute nodes are discovered using `ibnetdiscover`. Compute node ILOM to compute node mapping and VM hierarchy are obtained from the VI plug-in.

- Exadata Storage Servers are discovered using `ibnetdiscover` instead of `kfod`. Therefore, there is no need to specify the Database Oracle Home during discovery.

- InfiniBand switches are discovered using `ibnetdiscover`.

- Compute node ILOM, PDU, and Cisco switch are discovered based on the `databasemachine.xml` schematic file.

- Cluster and Database Target Discovery

  – The cluster and database target discovery is similar to the physical Exadata case (see Discovering Grid Infrastructure and RAC). The only difference is that the Enterprise Manager agents needed to be deployed on the `DomU` of the Database cluster before the cluster, ASM, and database targets can be discovered using the DB plug-in.

- Agent Placement

  – The primary and backup Enterprise Manager agents monitoring the Exadata hardware targets should be deployed in two dedicated `DomU` that will not be suspended or shut down, and are ideally on different physical servers to ensure high availability.

  – For static virtual machine configurations, the Enterprise Manager agents that are used to monitor the Database clusters can be used to monitor the Exadata hardware.

To discover a virtualized Exadata Database Machine:

1. From the Setup menu, select **Add Target** then **Add Targets Manually**.

2. On the Add Targets Manually page, select **Add Using Guided Process** (Figure 6-1):

Figure 6-1   Add Targets Manually
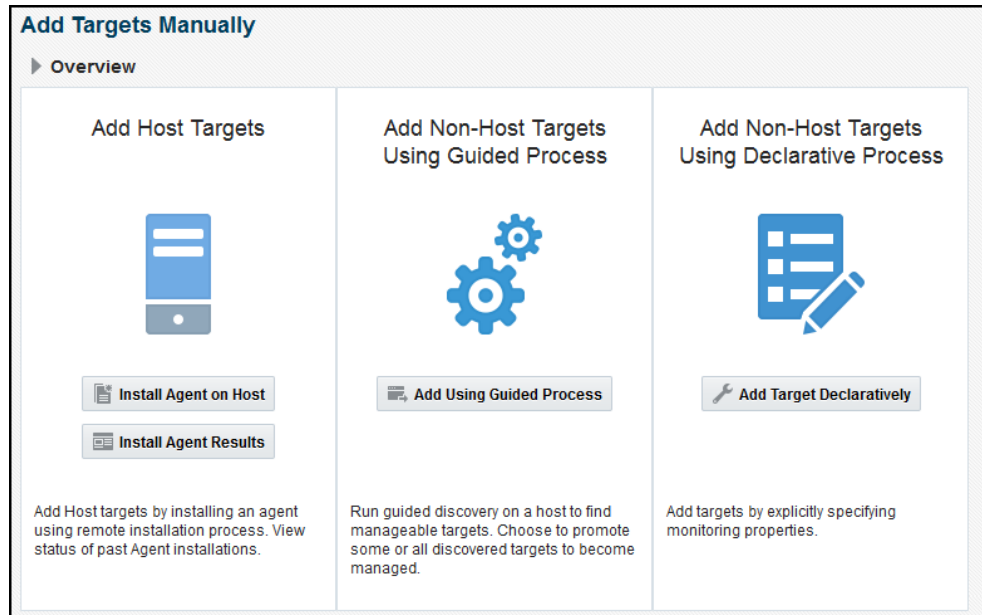
3. In the Add Using Guided Process pop-up window, select **Oracle Virtual Platform** and click **Add** (Figure 6-2):

Figure 6-2   Add Oracle Virtual Platform
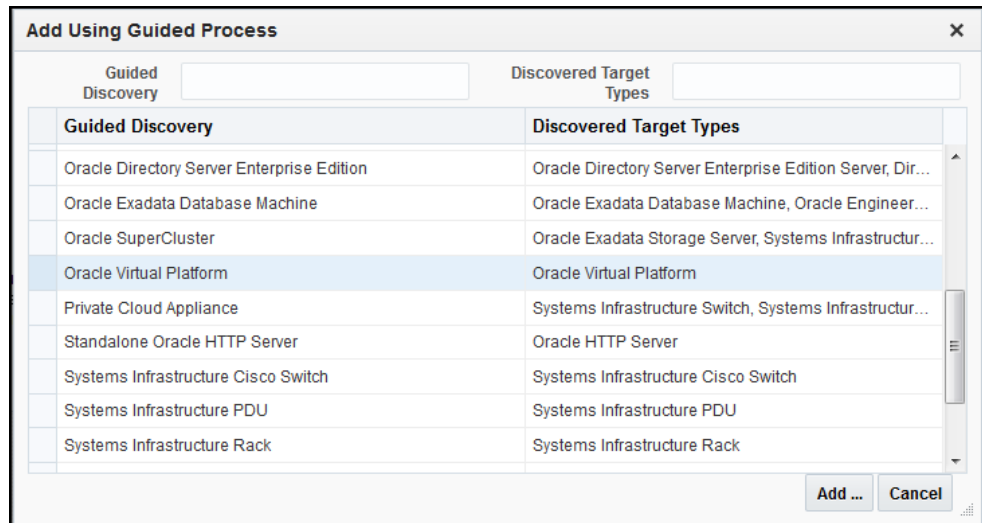
> **Note:**
>
> This option will be available only if the Virtualization Infrastructure (VI) plug-in has been deployed.
>
> If the plug-in is not deployed, then the Oracle Virtual Platform option will not appear. Deploy the VI plug-in as described in Direct Monitoring of Xen Based Systems in *Oracle® Enterprise Manager Cloud Administration Guide*.

4. On the Discover Oracle Virtual Platforms page, register Oracle Virtual Platforms with Enterprise Manager. Target credentials and/or monitoring agent can be specified for each target. If set, these override the defaults for that target.

   • Set the Default Monitoring Agent and Credentials (Figure 6-3). Click the magnifying glass icon 🔍 to search for the monitoring agent location. For the Credential Properties, enter `root` for the Username and provide the host's root password.

   > **Note:**
   >
   > A non-root user with `sudo` privilege can also be used. Refer to the VI plug-in documentation for the necessary setup steps.

   Figure 6-3   Default Monitoring Agent and Credentials

   • Add a Host Name or IP address. Click **Add** and enter the fully qualified domain name (FQDM) or IP address for the host in the pop-up window (Figure 6-4). If you have more than one, each entry **must** appear on a separate line.

Figure 6-4   Discover Virtual Serves: Add Host/IP Address
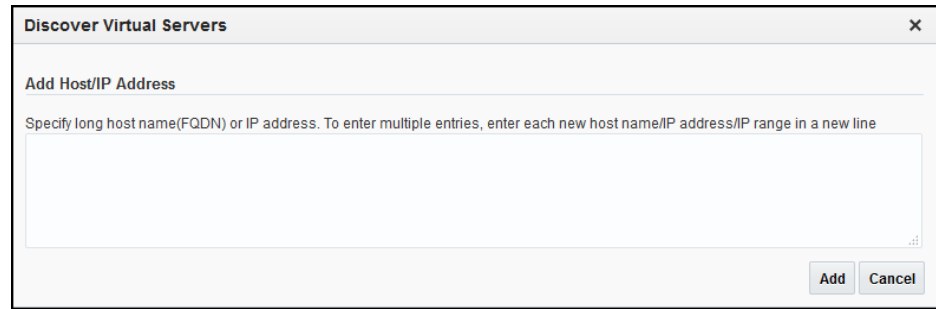
Click **Add** to close the pop-up window.

Once added, the Hostname and IP address fields will update as shown in Figure 6-5:

Figure 6-5   Enter Hostname or IP Address
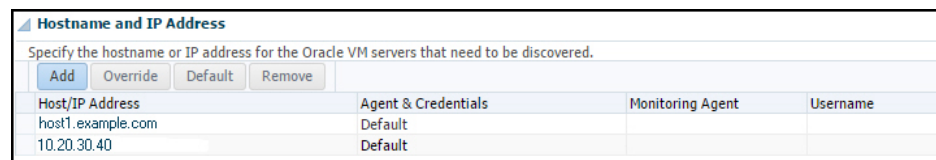
- Click **Submit**. A job is submitted to register the Oracle Virtual Platform, which creates the virtual targets. Approximately five (5) minutes is required to complete the job. Click **Job Details** to check the status, or click **Close** to close the window (Figure 6-6):

Figure 6-6   Submit Oracle Virtual Platform Registration Job
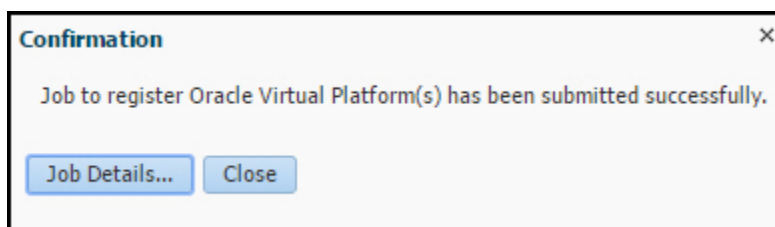
5. Once the job completes, then discover the Exadata Database Machine. From the Setup menu, select **Add Target** then **Add Targets Manually**.

6. On the Add Targets Manually page, select **Add Using Guided Process** (Figure 6-7):

Figure 6-7   Add Targets Manually
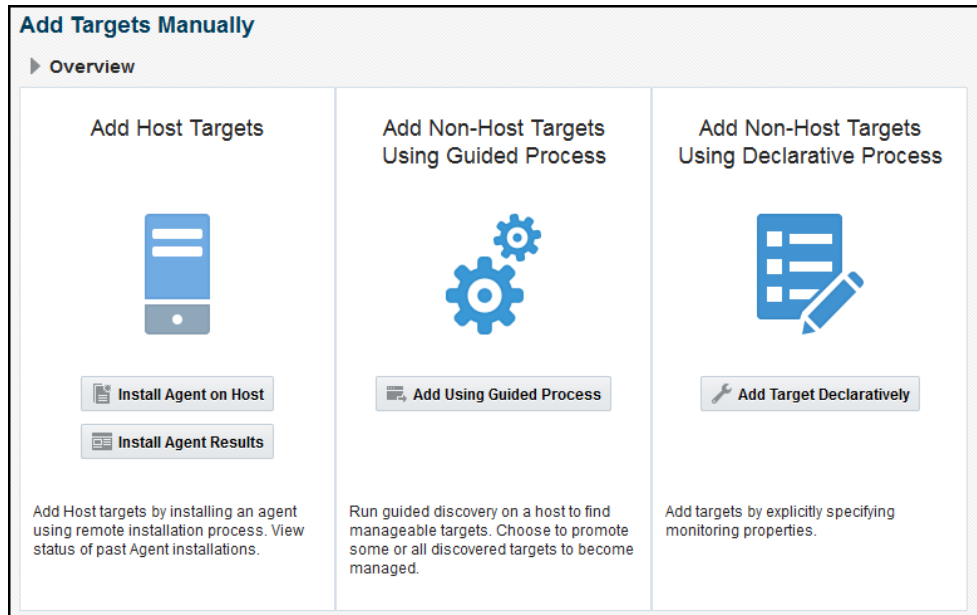
7. For the Target Types drop-down menu, select **Oracle Exadata Database Machine** (Figure 6-8):

Figure 6-8   Add Using Guided Process: Add Oracle Exadata Database Machine
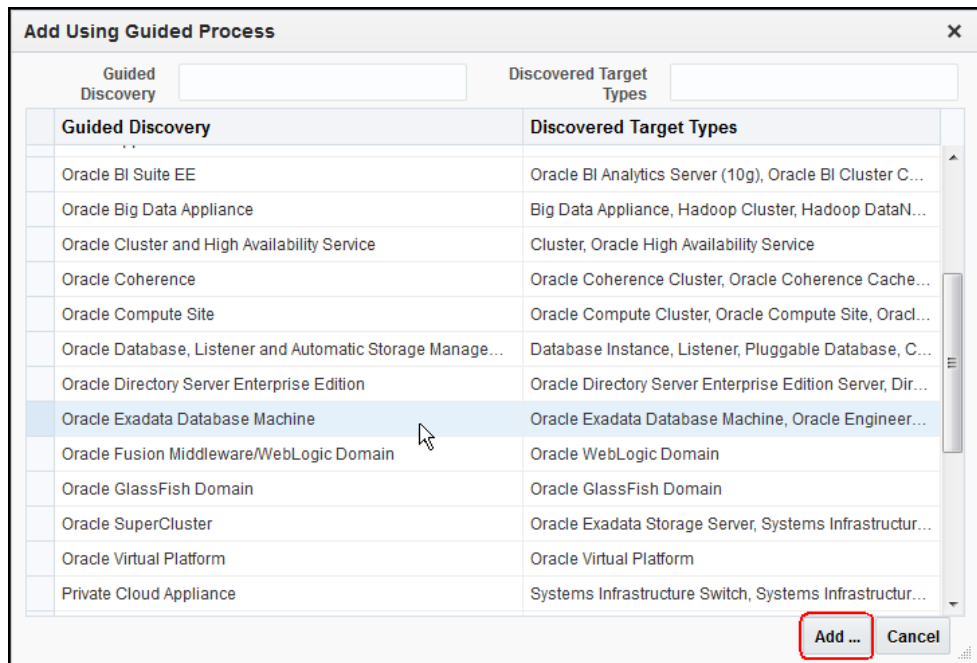
8. On the Oracle Exadata Database Machine Discovery page, select the **Discover a new Database Machine and its hardware components as targets** option and click **Discover Targets**.

9. On the Discovery Inputs page, click the magnifying glass icon 🔍 to search for an agent in a `DomU` that resides in the DB Machine to be discovered. Do not search for

a virtual platform (`Dom0`) because you cannot install an Enterprise Manager Agent in `Dom0`. Just like the physical Exadata case, you are specifying a host on which the schematic file can be read. Usually, it will be the same host as the discovery agent. It will not be the `Dom0`

In the Schematic Files section, select a host on which the schematic file can be read, and set the host credential that can read the schematic file. Click **Set Credential** to set the log in and password (Figure 6-9) for the host you registered in the previous steps. Click **OK**.

Figure 6-9   Set Credential
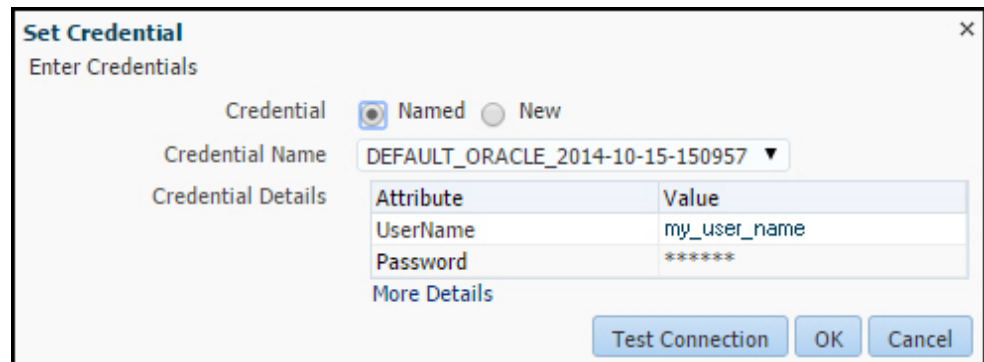
Click **Next**.

10. On the InfiniBand Discovery page, set the `nm2user` credential. Select the New option and enter **nm2user** for the Username field and provide a password as shown in Figure 6-10:

Figure 6-10   Set InfiniBand Credentials
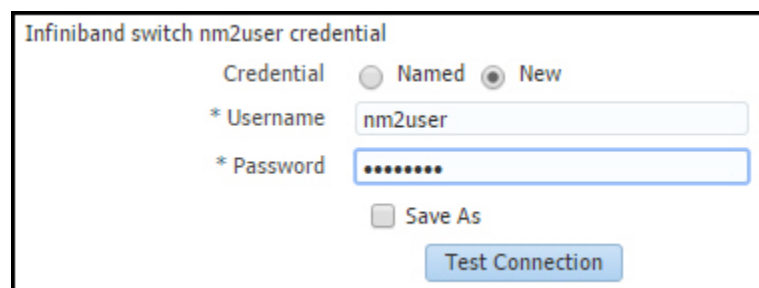
Click **Next**.

> ✏️ **Note:**
>
> A known issue about missing CLIENTNAME and CLIENTIP information will cause an Error pop-up message. Click **OK** to dismiss the pop-up and to continue with the guided discovery.

11. On the Prerequisite Check page, verify the Status is successful, then click **Next**.

12. On the Components page, review the Exadata components that were discovered, then click **Next**.

13. On the Monitoring Agents page, review the names, locations, and backup locations of the Monitoring Agents. Click **Next**.

14. On the Agent Credential page, if the credentials are the same for all agents, then you can enter a new username and password or accept the default. Click **Next**.

    If the credentials are different for all agents, then select the **Different for all agents** option and enter usernames and passwords for all hosts. Click **Next**.

15. On the Monitoring Credentials page, verify or enter the credentials for the following components:

    • Oracle Exadata Storage Server

    • InfiniBand Switch

    • ILOM

    Click **Test Connection** for each component to verify the connection. If the credentials are different for each component, then provide the appropriate username and password.

    Click **Next**.

16. On the SNMP Subscription page, enter the SNMP Community String (default is **public**) value for both Oracle Exadata Storage Server and InfiniBand Switch areas. For the InfiniBand Switch, provide the root credentials (Figure 6-11). Click **Next**.

    Figure 6-11   Enter InfiniBand Switch Root Credential

17. On the Component Properties page, enter **public** for both Ethernet and PDU components (Figure 6-12). Click **Next**.

Figure 6-12   Enter 'public' for Ethernet Switch and PDUs

18. On the Review page, review the details of the following components:

    • System Target

    • Compute Node

    • Oracle Exadata Storage Server

    • InfiniBand Switch

    • Ethernet Switch

    • Compute Node ILOM

    • KVM

    • PDU

    Click **Submit** to promote all targets. Allow for approximately five (5) minutes to process. Once complete, all targets will now be monitored by Oracle Enterprise Manager Cloud Control.

> **Note:**
>
> The VI plug-in regularly checks whether a VM is added or deleted. The Oracle VM instance targets are auto-promoted once they are detected by the VI plug-in. If you want to monitor the OS, ASM, and DB in the VM, you need to push the Enterprise Manager agent to the VM.

Post-Discovery Configuration

Since agents run inside `DomU` nodes and remotely monitor cells, ILOMs, switches, and PDUs, ensure that Primary and Backup agents are on physically different `DomU` hosts. In case of a `Dom0` outage, Enterprise Manager can continue to monitor such targets us-

ing an agent that is running on an active `DomU` hosted by a different `Dom0` that is still running. This will achieve continuous monitoring in case of a complete `Dom0` outage.

For details on how agents monitor Exadata targets remotely, refer to Post-Discovery Configuration and Verification, for details.

Exadata Virtualized Provisioning

Provisioning involves repeatable, reliable, automated, unattended, and scheduled mass deployment of a RAC Cluster including virtual machines (VMs), Oracle Database (DB), Grid Infrastructure, and ASM on Virtualized Exadata.

With the Exadata plug-in's virtualization provisioning functionality, you can:

- Creating a Database Cluster
- Scaling Up a Database Cluster
- Deleting a Database Cluster

Creating a Database Cluster

To create a database cluster:

1. From the Database Machine target menu, select **Provisioning**, then select **Create Cluster** (Figure 6-13):

    Figure 6-13   Provisioning Menu
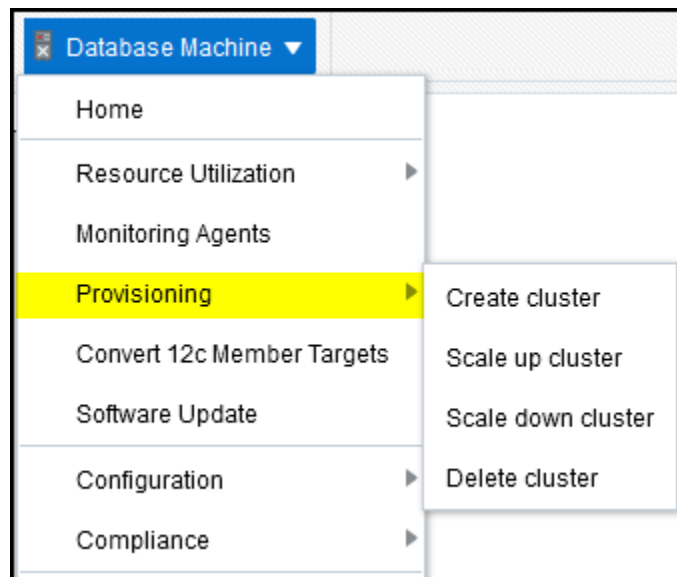
    The Exadata Provisioning Wizard will display.

2. On the Exadata Provisioning: Cluster page, provide the information for:
    - **Cluster Definition**: Create a cluster name. Click **Show existing clusters** to display a list of database clusters already provisioned.

- **Virtual Machine Location**: Select the servers on which you want to create the virtual machines. Select one or more from the **Available Servers** pane, then click the move button to move the selected server to the **Selected Servers** pane (Figure 6-14):

Figure 6-14   Select Virtual Machine Location
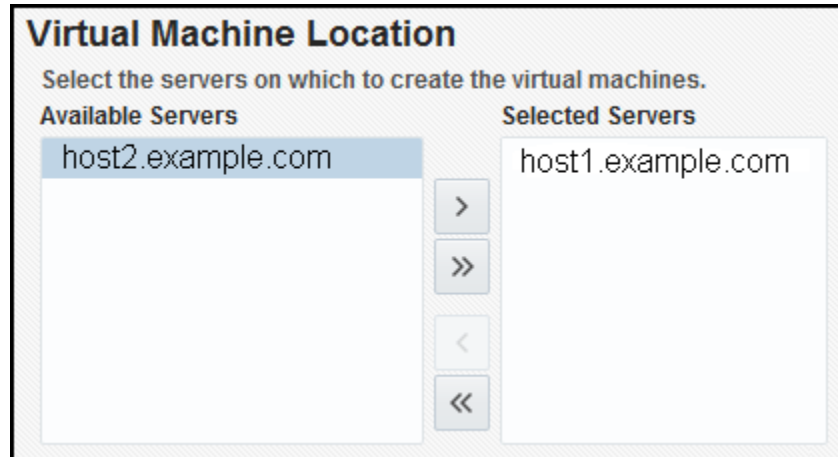
- **Storage Definition**: Select the Exadata Storage Servers to be used by the virtual machines. Select one or more from the **Available Storage Servers** pane, then click the move button to move the selected server to the **Selected Storage Servers** pane:

Figure 6-15   Select Exadata Storage Servers
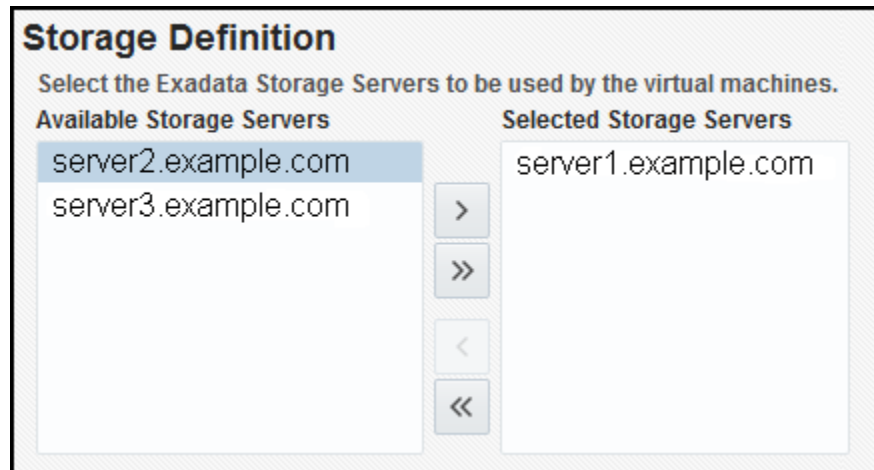
Click **Next**.

3. On the Credentials page, set the credentials for:

- **Compute Server**: Set the credentials for the `root` user. From the Set Credentials drop-down, select **All** to apply the settings to all servers, or select one or more servers from the list and select **Selected** to apply the settings to only the selected servers.

  In the Set Server Credential pop-up window, select an existing named credential or select **New** to create a new one.

Click **Test Connection** to verify that the credentials are properly set. If successful, the Test Credential Status will update to show Succeeded (Figure 6-16):

Figure 6-16   Set Compute Server Credentials

- **Exadata Storage Server**: Set the credentials for the cell administrator.

  In the Set Server Credential pop-up window, select an existing named credential or select **New** to create a new one.

  Click **Test Connection** to verify that the credentials are properly set. If successful, the Test Credential Status will update to show Succeeded (Figure 6-17):

Figure 6-17   Set Exadata Storage Server Credentials

Click **Next** to define the Virtual Machines.

4. On the Virtual Machines (VMs) page, provide the following information:

> ✎ **Note:**
>
> When available, the Exadata Provisioning Wizard will pre-populate the fields with the appropriate defaults. You can change this information to suit your environment.

- **Virtual Machine Definition**: In this region (Figure 6-18), provide the details to define the VM:

- Virtual Machine Size: Select Small, Medium, or Large. Click Customize to adjust the number of CPU cores and available memory.
- Root password: Create a password in the two password fields.
- Verify the Prefix, DNS, and NTP fields.
- Time Zone: select the appropriate time zone from the drop-down list.

Figure 6-18   Exadata Provisioning: Virtual Machine Definition

- **Software Locations**: When available, the Exadata Provisioning Wizard will pre-populate the fields (Figure 6-19); otherwise, provide the following information:
  - Inventory Location
  - Grid Infrastructure Home
  - Database Home Location
  - Agent Installation Base Directory
  - Agent Port (optional)
  - Software Language (optional)

Figure 6-19   Exadata Provisioning: Software Locations

- **Operating System Users and Groups**: Like the Software Location region, the Exadata Provisioning Wizard will pre-populate the fields except for the password fields (Figure 6-20). Otherwise, provide the following information:

  – User name: including the ID, password, and home directory.

  – DBA group name and ID.

  – OINSTALL group name and ID.

Figure 6-20   Exadata Provisioning: Operating System Users and Groups

Click **Next** to provide the Network details.

5. On the Network page, specify the IP address, name and domain used for the Admin, Client and Private network. Provide the details for the following information:

   - **Gateway and Domain Details**: The domain and subnet mask details should already be supplied by the Exadata Provisioning Wizard. Enter a valid IP address for the Admin and Client gateway (Figure 6-21):

Figure 6-21   Exadata Provisioning: Network Gateway and Domain Details

   - **Virtual Machine 1** (Figure 6-22): For the first virtual machine in the cluster, the Exadata Provisioning Wizard will auto-complete the Prefix and Start ID field. You can enter an optional Suffix. Enter a valid IP address.

Figure 6-22   Exadata Provisioning: Virtual Machine 1

- **Generated Virtual Machine Name and IP** (Figure 6-23): After you have entered the information for the first VM, click **Generate** to create the information for the other VMs in the cluster. You can always enter the details manually.

Figure 6-23   Exadata Provisioning: Generated Virtual Machine Name and IP

Once you have entered all the necessary information, click **Validate IP** at the top of the page to verify the IP addresses. Click **Next** to continue to the enter the details for Grid Infrastructure and to create the Initial Database.

6. On the Grid Infrastructure and Initial Database page, enter the details for:

- **Grid Infrastructure** (Figure 6-24): Enter the details for the Cluster (SCAN name and port) and verify the Disk Group information. The Exadata Provisioning Wizard will pre-populate the details, but you can adjust them as needed.

Figure 6-24   Exadata Provisioning: Grid Infrastructure

- **Initial Database**: Click the check box to create the initial database. Additional information for Database Identification and Administrator Credentials will be required as shown in Figure 6-25:

Figure 6-25   Exadata Provisioning: Initial Database

Click **Advanced** to expand the region for additional details for Memory Parameters, Processes, and Character Sets as shown in Figure 6-26:

Figure 6-26   Exadata Provisioning: Initial Database Advanced Details

Click **Next** to set the schedule.

7. On the Schedule page, the Exadata Provisioning Wizard will create the Deployment Instance value. Select a schedule start and notification options:

   • **Schedule**: Select to initiate the creation immediately or later. If you select later, then you will be prompted to select a date and time.

   • **Notification**: Select the notification statuses for which you will be notified.

   Click **Review** to review the settings and initiate the job.

8. On the Review page, review the selection in the summary displayed. To change any section, return to the previous page and edit the selection.

   Click **Submit** to begin the creation job.

Scaling Up a Database Cluster

To scale up a database cluster:

1. From the Database Machine target menu, select **Provisioning**, then select **Scale Up Cluster**.

   The Exadata Provisioning Wizard will display.

2. On the Cluster page, enter the cluster name or click the Search icon to select a cluster from the list.

Select one or more from the **Available Servers** pane, then click the move button to move the selected server to the **Selected Servers** pane.

Click **Next** to set the credentials.

3. On the Credentials page, set the credentials for:

   • **Compute Server**: Set the credentials for the `root` user. From the Set Credentials drop-down, select **All** to apply the settings to all servers, or select one or more servers from the list and select **Selected** to apply the settings to only the selected servers.

     In the Set Server Credential pop-up window, select an existing named credential or select **New** to create a new one.

     Click **Test Connection** to verify that the credentials are properly set. If successful, the Test Credential Status will update to show Succeeded (Figure 6-27):

Figure 6-27   Set Compute Server Credentials

   • **Virtual Machines** (Figure 6-28): Set the credentials for the DomU Host and Root and for the Cluster ASM and Database.

     You have the option to use preferred credentials or to override the preferred credentials.

     Click **Test Connection** to verify that the credentials are properly set.

Figure 6-28   Scale Up Cluster: Virtual Machines Credentials

Click **Next**.

4. On the Virtual Machines page, click **Next**.

5. On the Network page, specify the IP address, name and domain used for the Admin, Client and Private network. Provide the details for the following information:

   • **Gateway and Domain Details**: The domain and subnet mask details should already be supplied by the Exadata Provisioning Wizard. Enter a valid IP address for the Admin and Client gateway (Figure 6-29):

Figure 6-29   Scale Up: Network Gateway and Domain Details

   • **Virtual Machine 1** (Figure 6-30): For the first virtual machine in the cluster, the Exadata Provisioning Wizard will auto-complete the Prefix and Start ID field. You can enter an optional Suffix. Enter a valid IP address.

Figure 6-30   Scale Up: Virtual Machine 1

   • **Generated Virtual Machine Name and IP** (Figure 6-29): After you have entered the information for the first VM, click **Generate** to create the information for the other VMs in the cluster. You can always enter the details manually.

Figure 6-31   Scale Up: Generated Virtual Machine Name and IP

Once you have entered all the necessary information, click **Validate IP** at the top of the page to verify the IP addresses.

Click **Next** to continue to schedule the scale up.

> **Note:**
>
> The step for Grid Infrastructure and Initial Database are skipped because they do not need to be set up again.

6. On the Schedule page, the Exadata Provisioning Wizard will create the Deployment Instance value. Select a schedule start and notification options:

   • **Schedule**: Select to initiate the scale up immediately or later. If you select later, then you will be prompted to select a date and time.

   • **Notification**: Select the notification statuses for which you will be notified.

   Click **Review** to review the settings and initiate the scale up.

7. On the Review page, review the selection in the summary displayed. To change any section, return to the previous page and edit the selection.

   Click **Submit** to begin the scale up.

Scaling Down a Database Cluster

To scale down a database cluster, the Virtual Machine is removed from the cluster:

1. From the Database Machine target menu, select **Provisioning**, then select **Scale Down Cluster**.

   The Exadata Provisioning Wizard will display.

2. Enter the cluster name you want to scale down or click the Search icon to select an available cluster.

   Once you have selected a cluster, you will be prompted to:

   • Select nodes to delete.

   • Verify or enter new named credentials for DomU (host, root, and Exadata Server) and for the Exadata Storage Server. Click **Test Credentials** to verify the credentials have been selected properly.

   Click **Next** to schedule the scale-down job.

3. On the Schedule page, the Exadata Provisioning Wizard will create the Deployment Instance value. Select a schedule start and notification options:

   • **Schedule**: Select to initiate the scale down immediately or later. If you select later, then you will be prompted to select a date and time.

   • **Notification**: Select the notification statuses for which you will be notified.

   Click **Review** to review the settings and initiate the scale down.

4. On the Review page, review the selection in the summary displayed. To change any section, return to the previous page and edit the selection.

   Click **Submit** to begin the scale down.

Deleting a Database Cluster

To delete an existing cluster:

1. From the Database Machine target menu, select **Provisioning**, then select **Delete Cluster**.

    The Exadata Provisioning Wizard will display.

2. On the Cluster page, enter the cluster name you want to delete or click the Search icon to select an available cluster.

    The page will update to show the nodes to be deleted

    Verify or enter new named credentials for DomU (host, root, and Exadata Server) and for the Exadata Storage Server. Click **Test Credentials** to verify the credentials have been selected properly.

    Click **Next** to schedule the delete job.

3. On the Schedule page, the Exadata Provisioning Wizard will create the Deployment Instance value. Select a schedule start and notification options:

    • **Schedule**: Select to initiate the scale down immediately or later. If you select later, then you will be prompted to select a date and time.

    • **Notification**: Select the notification statuses for which you will be notified.

    Click **Review** to review the settings and initiate the delete job.

4. On the Review page, review the selection in the summary displayed. To change any section, return to the previous page and edit the selection.

    Click **Submit** to begin the delete job.

Viewing Virtualized Exadata Database Machine

Once discovered, the Exadata plug-in shows the virtual machines monitored by Enterprise Manager Cloud Control 12*c*, as shown in Figure 6-32:

Figure 6-32   Virtual Machines Monitored
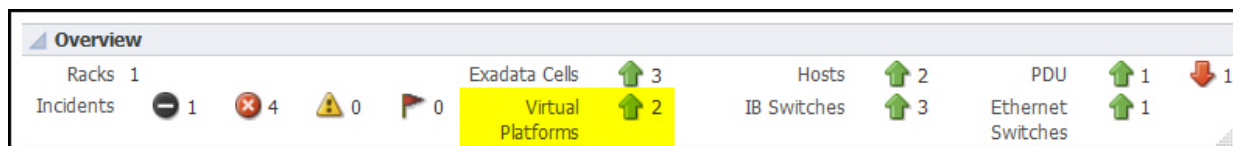
> **✎ Note:**
>
> The schematic diagram in the Database Machine home page is based on the content of the `databasemachine.xml` file found during discovery. The **virtual platforms** (`Dom0`) are displayed as compute nodes in the rack in the schematic diagram.
>
> The Database Machine Software topology diagram will not display the physical Oracle Server, virtual Oracle Server targets (`DomU`), and Virtual Platform target (`Dom0`) targets. However, it will continue to show the host targets which are running in `DomU`.

The Software tab for the Exadata Database Machine target shows all clusters, ASM, and Database targets in the whole physical Database Machine grouped by clusters as described in Figure 6-33:

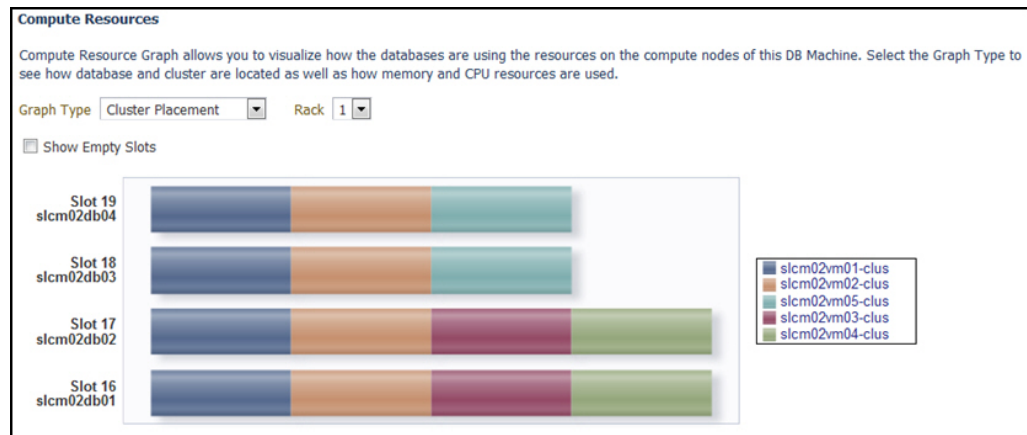**Figure 6-33   Exadata Database Machine Software Tab**

Resource Utilization Graphs

The following compute resource allocation graphs are available in virtualized Exadata. These graphs are dependent on the virtual machine hierarchy and metric data from the VI plug-in:

Cluster Placement

This graph (Figure 6-34) shows the ClusterWare cluster placement on physical servers in a particular Exadata Database Machine rack. Since this is a placement graph, the widths of the data series reflect the number of clusters on the physical server that has the most number of clusters.
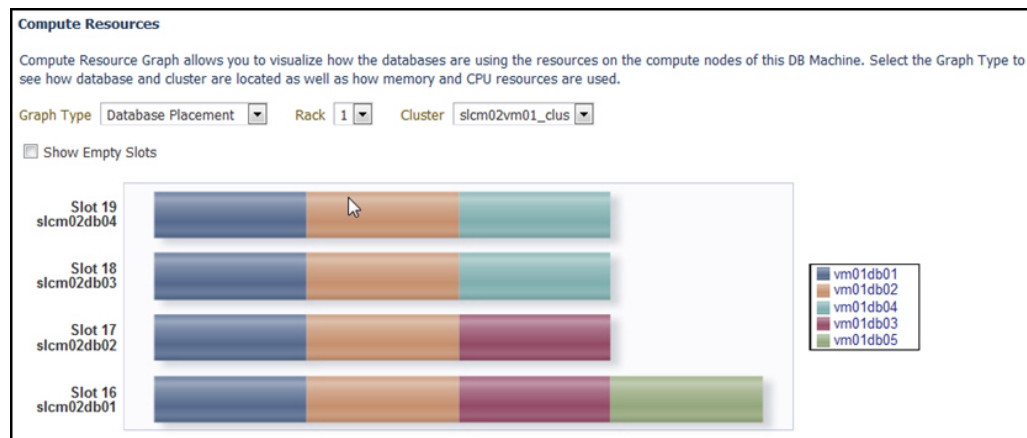
Figure 6-34   Resource Utilization: Cluster Placement

Database Placement

This graph (Figure 6-35) shows the database placement on physical servers in a particular Exadata Database Machine rack for a particular DB cluster. Since this is a placement graph, the widths of the data series reflect the number of DB on the physical server that has the most number of databases for a particular DB cluster.
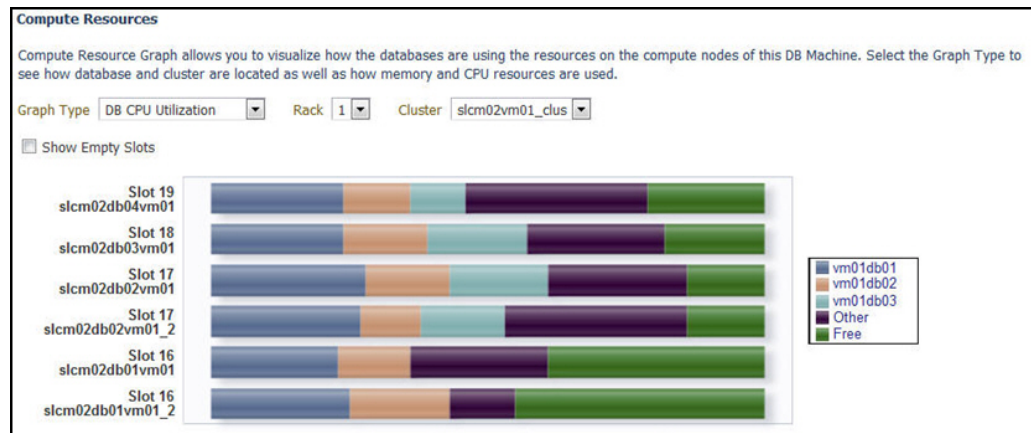
Figure 6-35   Resource Utilization: Database Placement

Database CPU Utilization

This graph (Figure 6-36) shows the database CPU utilization per database per VM host for a particular DB cluster.

Figure 6-36   Resource Utilization: Database CPU Utilization

Database Memory Utilization

This graph (Figure 6-37) shows the database memory utilization per database per VM host for a particular DB cluster.

Figure 6-37   Resource Utilization: Database Memory Utilization
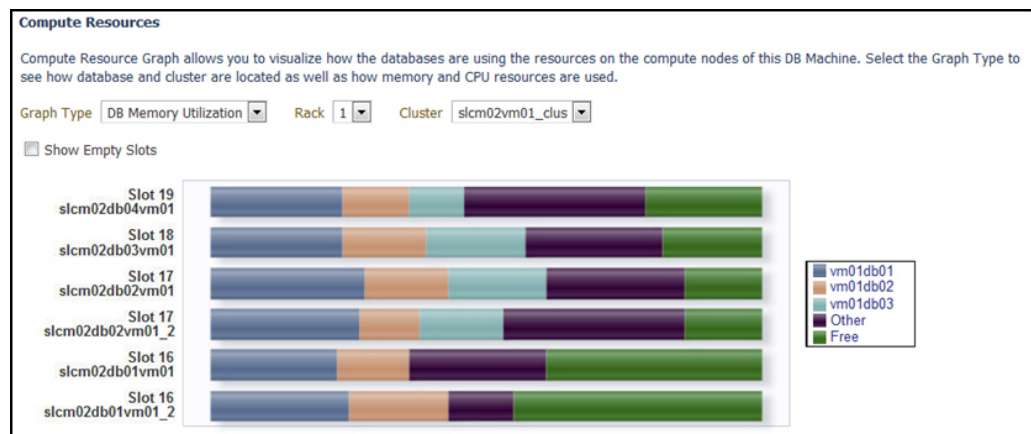
7

Exadata Metrics

This chapter describes how to access the various metrics for the Oracle Exadata Database Machine and provides examples of key metrics including:

- Accessing Exadata Metrics
- Aggregated Exadata FlashDisk and HardDisk Metric Example
- Exadata Cell Metric Example

Accessing Exadata Metrics

For a complete list of metrics available for the Oracle Exadata Database Machine, see *Oracle Exadata* in *Oracle® Enterprise Manager Oracle Database Plug-in Metric Reference Manual*:
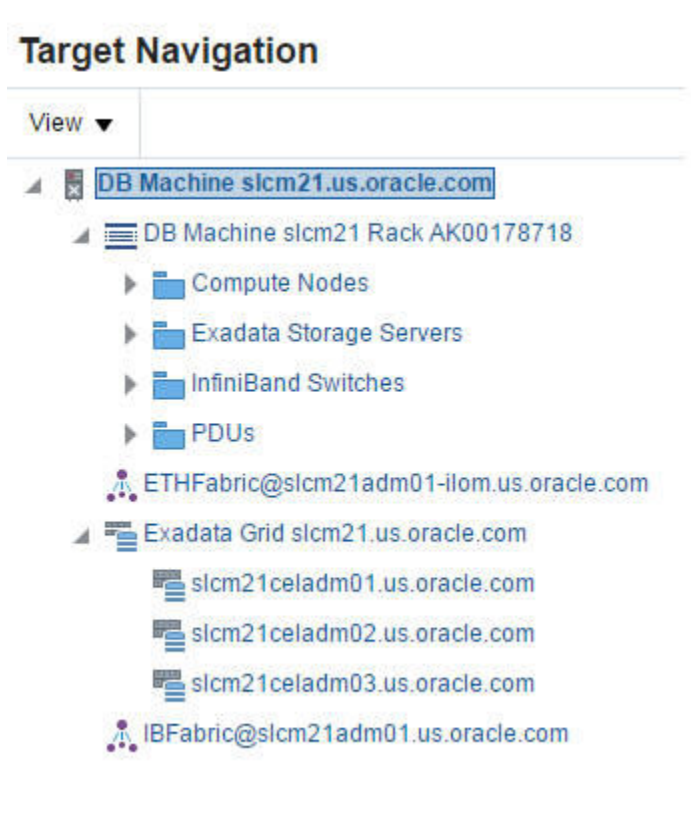
To access the available Exadata Metrics:

1. From the Targets menu, select **Exadata** (Figure 7-1):

   **Figure 7-1 Enterprise Manager Targets Menu**

2. On the Oracle Exadata Database Machines page, select an Exadata Database Machine from the list.

3. From the Target Navigation tree, expand the **Exadata Grid** and select an Exadata Storage Server (Figure 7-2):

Figure 7-2   Expand the Exadata Grid in the Target Navigation Tree

4. On the Storage Server page, select the **Exadata Storage Server** menu and select **Monitoring** then **All Metrics** (Figure 7-3):

Figure 7-3   Exadata Storage Server Monitoring Menu
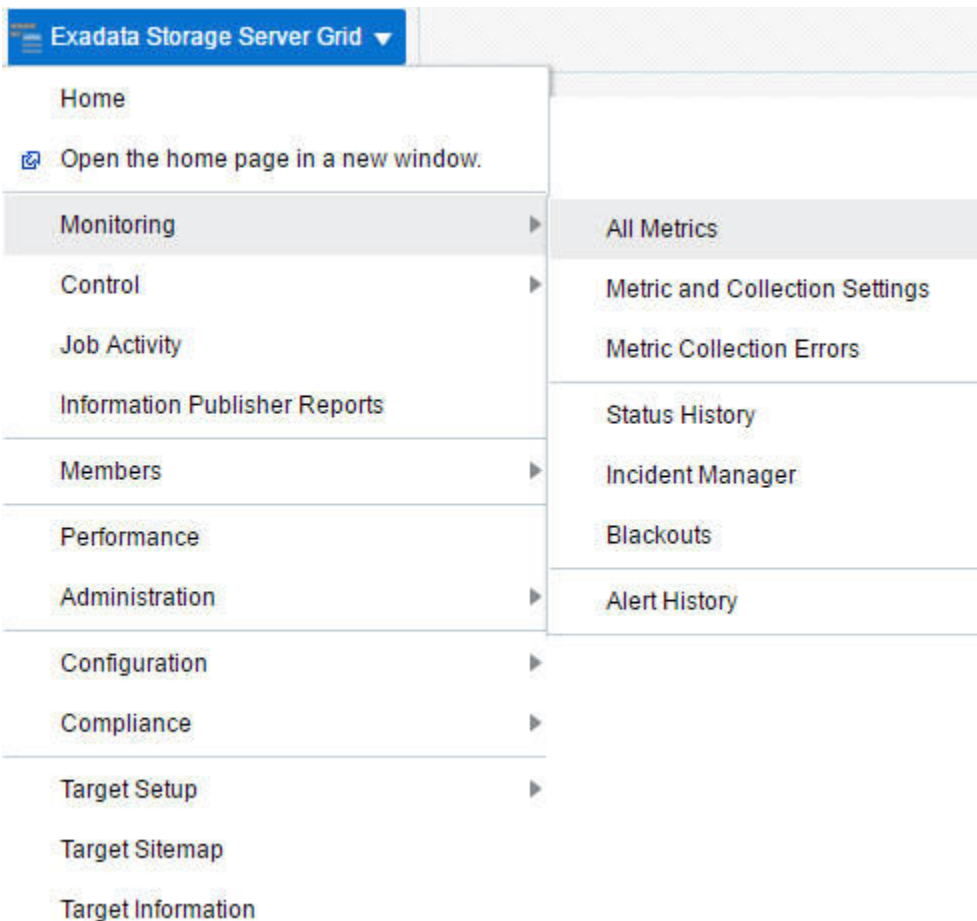
5. On the All Metrics page, a variety of metrics are available. Select a metric or click to expand available metric details.

Aggregated Exadata FlashDisk and HardDisk Metric Example

This metric category contains metrics that are aggregated over either the hard disks or flash disks in a cell. Selecting this metric from the All Metrics page generates a high-level summary, as shown in Figure 7-4:

Figure 7-4   Aggregated Exadata FlashDisk and HardDisk Metric

Expand the **Aggregated Exadata FlashDisk and HardDisk Metric** in the All Metrics page to show a variety of metric details, such as **Average CellDisk Read Throughput** (Figure 7-5), which gives an indication of the average number of bytes read from the cell disk, or **Total CellDisk IO Load** (Figure 7-6), which gives an indication of the total input/output load to the celldisk.

Figure 7-5   Average CellDisk Read Throughput

CellDisk Type	Average Value	Low Value	High Value	Last Known Value	Current Severity	Alert Triggered
FlashDisk	0.09	0.02	0.36	0.06	Not Applicable	-
HardDisk	190.36	92.54	368.79	130.37	Not Applicable	-

Figure 7-6   Total CellDisk IO Load

CellDisk Type	Average Value	Low Value	High Value	Last Known Value	Current Severity	Alert Triggered
FlashDisk	16	16	16	16	Not Applicable	-
HardDisk	51.69	48	93	49	Not Applicable	-

Exadata Cell Metric Example

This metric category contains the performance metrics collected at the cell level for each cell, such as CPU utilization and memory utilization. Selecting this metric from the All Metrics page generates a high-level summary, as shown in Figure 7-7:

Figure 7-7   Exadata Cell Metric

Exadata Cell Metric

Collection Schedule Every 15 Minutes [Modify]
Upload Interval Every Collection
Last Upload Jan 21, 2015 8:23:02 PM GMT

Metric	Thresholds	Real Time Value
Cell Name	Not Applicable	adscx0008
CPU Utilization	Not Set	14.43
Disk I/O Objective	Not Applicable	3
Exadata Temperature Lower Threshold	Not Set	26
Exadata Temperature Reading	Not Applicable	26
Exadata Temperature Upper Threshold	Not Set	26
LED Status	Not Applicable	off
Memory Utilization	Not Set	70
Network Received	Not Applicable	0.04
Network Sent	Not Applicable	0.04

Data shown in above table is collected in real time.

Expand the **Exadata Cell Metric** in the All Metrics page to show a variety of metric details, such as **CPU Utilization** (Figure 7-8), which provides information about the CPU

utilization, or **Disk I/O Objective** (Figure 7-9), which provides the optimization objective which IORM is configured to achieve (for example, "Low Latency" or "Balanced" for OLTP-oriented databases, or "High Throughput" for data warehouses).
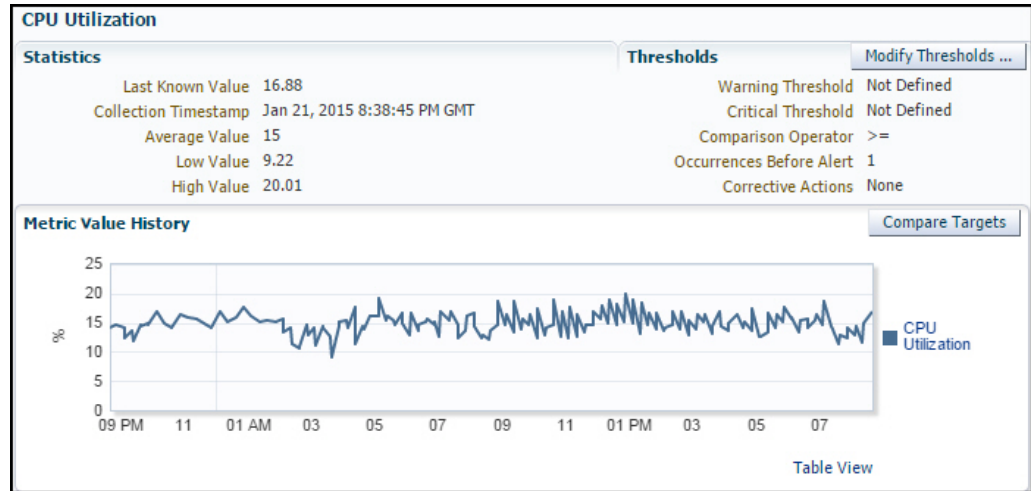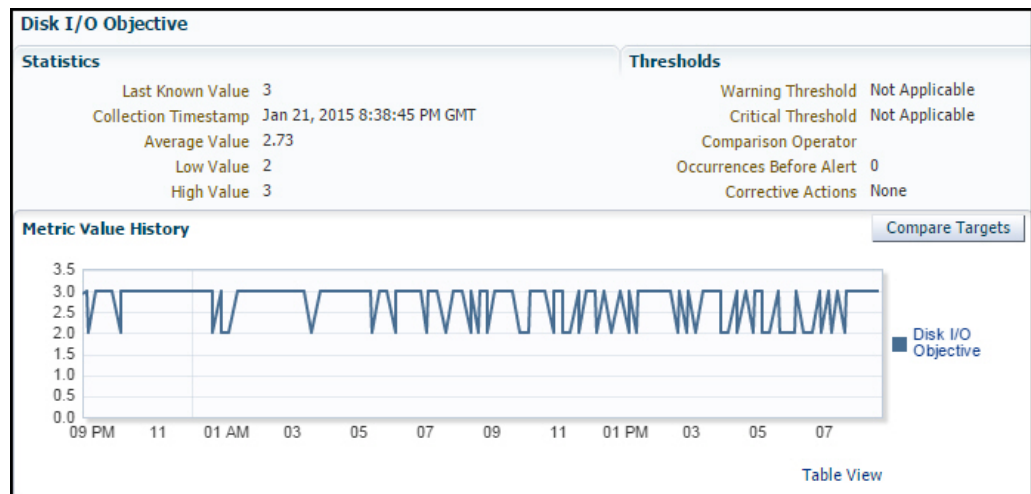
Figure 7-8   CPU Utilization

Figure 7-9   Disk I/O Objective

8

Troubleshooting the Exadata Plug-in

This chapter provides troubleshooting tips and techniques on installing, discovering, and configuring the Exadata plug-in. The following sections are provided:

- Establish SSH Connectivity
- Discovery Troubleshooting
- Troubleshooting the Exadata Database Machine Schematic File
- Exadata Database Machine Management Troubleshooting
- Exadata Derived Association Rules
- InfiniBand Patch Details Missing
- Oracle Auto Service Request (ASR) Issues
- Metric Collection Issues
- Status: Pending Issues
- Enhanced MIB Incompatibility
- Monitoring Agent Not Deployed for IPv6 Environments

Establish SSH Connectivity

For Release 12.1.0.1.0, the SSH key location is `<ORACLE_HOME>/.ssh` where `ORACLE_HOME` is the installation directory of the Enterprise Manager agent. For example:

```
/u01/app/oracle/product/gc12/agent/core/12.1.0.1.0
```

> **✎ Note:**
>
> Some metric collection has a dependency on `~/.ssh/known_hosts`.

For Release 12.1.0.2.0 or later, the SSH key location is `$HOME/.ssh` of the agent user.

To set up SSH connectivity between the computer where Agent is running and the Oracle Exadata Storage Server, as the Agent user:

1. Log in to the computer where the Enterprise Manager Agent is running, open a terminal, and run the following commands as the Agent user to generate a pair of the SSH private/public keys if they are not present:

   - For Release 12.1.0.1.0:

     ```
     $ cd <ORACLE_HOME>/.ssh
     $ ssh-keygen -t dsa -f id_dsa
     ```

     Where `<ORACLE_HOME>` is the installation directory of the Enterprise Manager Agent.

- For Release 12.1.0.2.0:

```
$ cd $HOME/.ssh
$ ssh-keygen -t dsa -f id_dsa
```

Where `$HOME` is the home directory of the Agent user.

2. Copy the public key (`id_dsa.pub`) to the `/tmp` directory on the storage cell:

```
$ scp id_dsa.pub root@<cell_ipaddress>:/tmp
```

3. Add the contents of the `id_dsa.pub` file to the `authorized_keys` file in the `.ssh` directory within the home directory of the cellmonitor user:

```
$ ssh -l root <cell_ipaddress> "cat /tmp/id_dsa.pub >> ~cellmonitor/.ssh/author-
ized_keys"
```

> **✎ Note:**
>
> If the `authorized_keys` file does not exist, then create one by copying the `id_dsa.pub` file to the `.ssh` directory within the home directory of the user cellmonitor:
>
> ```
> $ ssh -l root <cell_ipaddress> "cp /tmp/id_dsa.pub ~cellmonitor/.ssh/
> authorized_keys; chown cellmonitor:cellmonitor ~cellmonitor/.ssh/
> authorized_keys"
> ```

4. Make sure that the `.ssh` directory and `authorized_keys` have the right file permission:

```
# chmod 700 ~cellmonitor/.ssh
# chmod 600 ~cellmonitor/.ssh/authorized_keys
```

Discovery Troubleshooting

Very often, the error message itself will include the cause for the error. Look for error messages in the OMS and agent logs (case insensitive search for `dbmdiscovery`) or in the Discovery window itself.

The following sections are provided:

- Hardware Availability
- Discovery Failure Diagnosis
- Cell is not Discovered
- Compute Node Error Message
- Compute Node or InfiniBand Switch is not Discovered
- Compute Node not Managed by Enterprise Manager
- Extra or Missing Components in the Newly Discovered Exadata Database Machine
- InfiniBand Network Performance Page Shows No Data
- ILOM, PDU, KVM, or Cisco Switch is not Discovered
- Target Does not Appear in Selected Targets Page

- Target is Down or Metric Collection Error After Discovery
- Discovery Process Hangs

Hardware Availability

All the hardware components must be "known" and reachable; otherwise, communication failures will occur. Use the `ping` command for each hardware component of the Exadata rack to make sure all names are resolved.

The MAP targets in Enterprise Manager Cloud Control 13*c* may fail while collecting the correlation identifier. This failure can happen if the credentials are incorrect OR if a target (for example, the ILOM) is too slow in responding.

ILOM can be slow when the number of open sessions on ILOM has exceeded the limit. You can resolve this issue by temporarily closing the sessions on the ILOM.

The rack placement of targets can fail:

- If `examan` did not return valid rack position for the target.
- If there is an existing target in the same location.

Discovery Failure Diagnosis

Should discovery of your Oracle Exadata Database Machine fail, collect the following information for diagnosis:

- Any `examan-*.xml`, `examan-*.html`, `targets-*.xml`, and `examan*.log` files from the `AGENT_ROOT/agent_inst/sysman/emd/state` directory.
- Agent logs: `emagent_perl.trc` and `gcagent.log`
- OMS logs: `emoms.trc` and `emoms.log`
- Any snapshot (screen capture) of errors shown on the target summary page.

Cell is not Discovered

If the cell itself is not discovered, possible causes could be:

- The installation of RDBMS Oracle Home Release 11.2 is incorrect.
- The `/etc/oracle/cell/network-config/cellip.ora` file on the compute node is missing or unreadable by the agent user or cell not listed in that file.
- The cell is not listed in the `/etc/oracle/cell/network-config/cellip.ora` file.
- Management Server (MS) or cellsrv is down.
- Cell management IP is changed improperly. Bouncing both cellsrv and MS may help.
- To check that the cell is discovered with a valid management IP, run the following command on the compute node used for discovery:

  `$ORACLE_HOME/bin/kfod op=cellconfig`

Compute Node Error Message

Problems with the compute node may generate the following error:

```
The selected compute node is not an existing host target managed by Enterprise Manag-
er. Please add the compute node as managed target before you continue.
```

Possible causes for this error include:

- The compute node was not added as an Enterprise Manager host target before the Exadata Database Machine discovery.

- The host target name for compute node is an IP address. This problem can be an `/etc/hosts` or DNS issue.

- The host target name is not fully qualified with domain name (for example, host-name.mycompany.com)

Compute Node or InfiniBand Switch is not Discovered

If there are problems with discovery of the compute node or the InfiniBand switch, pos-sible causes could be:

- The InfiniBand switch host name or `nm2user` password is incorrect.

- The connection from the compute node to the InfiniBand switch through SSH is blocked by a firewall.

- The InfiniBand switch is down or takes too long to respond to SSH.

To resolve problems with the compute node or InfiniBand switch discovery, try:

- If the InfiniBand switch node is not discovered, the InfiniBand switch model or switch firmware may not be supported by EM Exadata. Run the `ibnetdiscover` command. Output should look like:

  ```
  Switch 36 "S-002128469f47a0a0" # "Sun DCS 36 QDR switch switch1.example.com" en-
  hanced port 0 lid 1 lmc 0
  ```

- To verify discovery of the compute node, run the following command on the com-pute node used for discovery:

  ```
  # ssh <IB switch> -l nm2user ibnetdiscover
  ```

- If the compute node is not discovered, run the `ibnetdiscover` command. Output should look like:

  ```
  Ca 2 "H-00212800013e8f4a" # " xdb1db02 S 192.168.229.85 HCA-1"
  ```

  A bug in the 11.2.2.2.2 compute node image shows "S" and the InfiniBand IP as missing. Output would look like:

  ```
  Ca 2 " H-00212800013e8f4a " # "xdb1db02 HCA-1"
  ```

  A workaround for this problem is to run the following command as root on the com-pute nodes:

  ```
  # /opt/oracle.cellos/ib_set_node_desc.sh
  ```

Compute Node not Managed by Enterprise Manager

If you encounter an instance where the compute note is not being managed by Enterprise Manager, then check the following troubleshooting steps:

- If the Agent host name is different than the compute node host name, then run the following command as `root` to match up to agent host name:

  `# ibnetdiscover`

- If the wrong Agent is used for discovery, then select the compute node Agent for discovery.

- If the compute node name has been reset from the client to management or vice-versa, then run the following command:

  `# /usr/sbin/set_nodedesc.sh`

- If a short host name is used for agents, then reinstall the agents using fully-qualified host name `<hostname.domain>`.

Extra or Missing Components in the Newly Discovered Exadata Database Machine

If you are showing extra components or if there are missing components, then check the following troubleshooting steps:

- For extra components, examine them for Exadata Database Machine membership. Deselect any extra components manually from the discovered list.

- Verify which schematic file that was used for discovery. Ensure that Enterprise Manager can read the latest `xml` file (for example, `databasemachine.xml`) on the compute node.

- For missing components, check the schematic file content.

- If you need to generate a new schematic file, then log a service request (SR) with Oracle Support and provide the details.

InfiniBand Network Performance Page Shows No Data

If the InfiniBand network performance page does not show data, double check that the files under the `/opt/oracle.SupportTools/em/` directory on compute nodes should be publicly readable. Se Oracle Bug 13255511 for more information.

ILOM, PDU, KVM, or Cisco Switch is not Discovered

If the ILOM, PDU, KVM, or Cisco switch is not discovered, the most likely cause is that the Exadata Database Machine Schematic file cannot be read or has incorrect data. See Troubleshooting the Exadata Database Machine Schematic File.

Target Does not Appear in Selected Targets Page

Even though no error may appear during the Exadata Database Machine guided discovery, the target does not appear on the Select Components page. Possible causes and solutions include:

- Check the All Targets page to make sure that the target has not been added as an Enterprise Manager target already:

  – Log in to Enterprise Manager.

  – Select **Targets**, then **All Targets**.

  – On the All Targets page, check to see if the Oracle Exadata target appears in the list.

- A target that is added manually may not be connected to the Exadata Database Machine system target through association. To correct this problem:

  – Delete these targets before initiating the Exadata Database Machine guided discovery.

  – Alternatively, use the `emcli` command to add these targets to the appropriate system target as members.

Target is Down or Metric Collection Error After Discovery

After the Exadata Database Machine guided discovery, an error that the target is down or that there is a problem with the metric collection may display. Possible causes and recommended solutions include:

- For the cell or InfiniBand switch, the setup of SSH may not be configured properly. To troubleshoot and resolve this problem:

  – The agent's SSH public key in the `<AGENT_INST>/.ssh/id_dsa.pub` file is not in the `authorized_keys` file of `$HOME/.ssh` for cellmonitor or nm2user.

  – Verify permissions. The permission settings for `.ssh` and `authorized_keys` should be:

    ```
    drwx------ 2 cellmonitor cellmonitor 4096 Oct 13 07:06 .ssh
    -rw-r--r-- 1 cellmonitor cellmonitor 441842 Nov 10 20:03 authorized_keys
    ```

  – Resolve a `PerformOperationException` error. See Troubleshooting the Exadata Database Machine Schematic File for more information.

- If the SSH setup is confirmed to be properly configured, but the target status is still down, then check to make sure there are valid monitoring and backup agents assigned to monitor the target. To confirm, click the **Database Machine** menu and select **Monitoring Agent**. Figure 8-1 shows an example of the monitoring agents:

Figure 8-1   Monitoring Agents Example

- For the ILOM, PDU, KVM, or Cisco switch, possible causes include:

  - The Exadata Database Machine Schematic Diagram file has the wrong IP address.

  - Monitoring Credentials is not set or incorrect. To verify:

    * Log in to Enterprise Manager.

    * Click **Setup**, then **Security**, and finally **Monitoring Credentials**.

    * On the Monitoring Credentials page, click the **Oracle Exadata** target type. Then set the monitoring credentials.

ILOM Credential Validation Fails During 12c Discovery

ILOM Credential Validation Failure Errors

> **Note:**
>
> The following applies to Enterprise Manager Cloud Control Release 2, Plug-in Update 1 and later.

ILOM credential validation may fail while performing a 12*c* discovery. The following errors may occur:

- *Authentication failed*

  Problem: Credentials provided are invalid.

  Resolution: Use valid credentials.

- *Unable to establish IPMI V2 / RMCP+ session.*

Problem: IPMI V2 is not enabled on the ILOM server.

Resolution: If IPMI V2 was disabled on purpose and the ILOM server is configured to use the more secure TLS1.2 protocol, then the IPMI client needs to be upgraded to use TLS1.2 for establishing a session with ILOM server.

- *Unable to establish LAN session.*

    Problem: Occurs when IPMI V1.5 is not enabled on the ILOM server.

    Resolution: Enable IPMI V1.5 on the ILOM server. IPMI V1.5 is used for communication as a third option after TLS1.2 and IPMI V2 have failed.

Discovery Process Hangs

If the discovery process for the Exadata Database Machine hangs, then check the following troubleshooting steps:

- Examine your network to verify:

    - That the host name can be resolved.

    - That the Agent(s) can access the OMS.

    - That a simple job can be executed from the console.

- If the OMS reported any errors, then check the following log file:

    `MW_HOME/gc_inst/sysman/log/emoms.log`

- For Repository issues, check the Repository database's `alert.log` file.

- For Agent issues, check the following log file:

    `$AGENT/agent_inst/sysman/log/gcagent.log`

Troubleshooting the Exadata Database Machine Schematic File

The Exadata Database Machine Schematic file version **503** is required as a prerequisite for guided discovery. As part of any discovery troubleshooting, possible causes and recommended resolution with the schematic file can include:

- The schematic file on the compute node is missing or is not readable by the agent user.

    - For Exadata Release 11.2.3.2 and later, the schematic file is:

        `/opt/oracle.SupportTools/onecommand/catalog.xml`

    - For Exadata Release 11.2.3.1 and earlier, the schematic file is:

        `/opt/oracle.SupportTools/onecommand/databasemachine.xml`

- If a `PerformOperationException` error appears, the agent NMO is not configured for `setuid-root`:

    - From the OMS log:

        ```
        2011-11-08 12:28:12,910 [[ACTIVE] ExecuteThread: '6' for queue: 'weblog-
        ic.kernel.Default (self-tuning)']
        ERROR model.DiscoveredTarget logp.251 -
        ```

```
ERROR: NMO not setuid-root (Unix only) oracle.sysman.emSDK.agent.client.ex-
ception.PerformOperationException:
```

- As root, run:

  ```
  # <AGENT_INST>/root.sh
  ```

- In the `/etc/pam.d` file, `pam_ldap.so` is used instead of `pam_unix.so` on compute nodes.

  - Even though the agent user and password are correct, this errors appears in the agent log:

    ```
    oracle.sysman.emSDK.agent.client.exception.PerformOperationException:
    ERROR: Invalid username and/or password
    ```

- Schematic file has error because of a known Exadata Database Machine configurator bug:

  - Verify that the Exadata Database Machine configurator is version 12.0

  - Verify that the schematic file is version 503

  - Older versions may or may not have the bug depending on the Exadata Database Machine rack type and partitioning.

- If the schematic file is blank, then:

  - Check your browser support and Enterprise Manager Cloud Control 12*c*.

  - Run through discovery again and watch for messages.

  - Check the `emoms.log` file for exceptions at the same time.

- If components are missing, then:

  - Add manually to the schematic page (click **Edit**).

  - Check for component presence in Enterprise Manager. Check to see if it is monitored.

Exadata Database Machine Management Troubleshooting

If data is missing in Resource Utilization graphs, then run a "view object" SQL query to find out what data is missing. Common problems include:

- Schematic file is not loaded correctly.

- Cluster, Database, and ASM are not added as Enterprise Manager targets.

- Database or cell target is down or is returning metric collection errors.

- Metric is collected in the Enterprise Manager repository, but has an `IS_CURRENT !` `= Y` setting.

Exadata Derived Association Rules

Exadata derived association rules depend on Exadata and DB/ASM ECM data. This data may take up to 30 minutes to appear depending on metric collection schedule. To check for data availability:

- From the Enterprise Manager Cloud Control console:

  - Click **Targets**, then **All Targets**.

— On the All Targets page, click the **Oracle Exadata** target from the list.

— Click **Database System**, then **Configuration**, and finally **Last Collected**.

— On the Latest Configuration page, click **Actions**, then **Refresh**.

- From the command line:

```
# emctl control agent runCollection
# target_name:target_type <collectionName>
```

Other troubleshooting tips include:

- Verify that ECM data are collected and present in Enterprise Manager repository.

- Verify that all data and conditions in query are met by running the query in SQL+.

- Verify triggers by enabling debug logging to check for timing issues.

InfiniBand Patch Details Missing

Problem: If you select both InfiniBand switches in an Exadata Database Machine, the Patch Details section is empty. Installation of a patch for both InfiniBand switches are not affected - only the details of the installed patch.

Workaround: Select each InfiniBand switch individually to review the patch details.

Oracle Auto Service Request (ASR) Issues

- Oracle ASR Not Working on Exadata Storage Server
- No Slots Available Error

Oracle ASR Not Working on Exadata Storage Server

Problem: You may encounter a problem where Oracle ASR is not working on the Exadata Storage Server.

Resolution: Ensure that there are two subscriptions on the Exadata Storage Server:

- The type should be `ASR` *or* `V3ASR` for receiving the cell ILOM traps.

- The type should be `default` (no type) *or* `v3` for receiving the MS MIB traps from the cell.

No Slots Available Error

The `asr` type entry on MS MIB adds a subscription to the cell ILOM automatically. If the ILOM SNMP slots are full, then the subscription command on the cell may fail with the following error:

```
CELL-02669: No slots are available for ILOM SNMP subscribers
```

There is a limit of 15 subscribers on the ILOM which might cause this failure. You will need to free up some slots on the ILOM and retry the ASR subscription:

1. Login to the ILOM console (for example: `https://XXXCELL-c.example.com`).

2. Click **ILOM Administration** and then **Notification**.

3. Choose the slot and set the subscriber to **0.0.0.0** to clear it up.

Target Status Issues

If the Target status shows DOWN inaccurately, then:

- For the **Cell**: Check `ssh` equivalence (cellmonitor user) with the followign command:

  ```
  ssh -i /home/oracle/.ssh/id_dsa -l cellmonitor <cell name> -e cellcli list cell
  ```

  Output should be: `<cell name>`

- For the **PDU**: Check to make sure you can access the PDU through your browser to verify that it is connected to your LAN:

  ```
  http://<pdu name>
  ```

- For the **Cisco Switch**: Check for proper SNMP subscriptions. See Set Up SNMP for Cisco Ethernet Switch Targets for details.

Metric Collection Issues

If the Target status shows a Metric Collection Error, then:

- Hover over the icon or navigate to Incident Manager.

- Read the full text of the error.

- Visit the Monitoring Configuration page and examine the settings. From the **Setup** menu, select **Monitoring Configuration**.

- Trigger a new collection: From the **Target** menu, select **Configuration**, then select **Last Collected**, then **Actions**, and finally select **Refresh**.

- Access the monitoring Agent Metric through your browser:

  ```
  https://<agent URL>/emd/browser/main
  ```

  Click **Target >>** and then click **Response** to evaluate the results. You may need to log a service request (SR) with Oracle Support.

Status: Pending Issues

For those issues where components are in a Pending status, see the following troubleshooting steps:

- Cellsys Targets
- Database Machine Target or Any Associated Components

Cellsys Targets

If the Cellsys target seems to be in a Pending status for too long, then:

- Verify that there is an association for the Cluster ASM, Database, and Storage Cell.

- Check and fix the status of the associated target database.

- Check and fix the status of the associated target ASM cluster.
- Ensure an **UP** status for all cell server targets.
- Delete any unassociated cellsys targets.

Database Machine Target or Any Associated Components

If the Exadata Database Machine target or any associated components are in a Pending status for too long, then:

- Check for duplicate or pending delete targets. From the **Setup** menu, select **Manage Cloud Control**, then select **Health Overview**.
- Check the target configuration. From the target's home page menu, select **Target Setup**, then select **Monitoring Configurations**.
- Search for the target name in the agent or OMS logs:

  ```
  $ grep <target name> gcagent.log or emoms.log
  ```

Enhanced MIB Incompatibility

With some shipments of the X4 series of Exadata and all later version of the hardware, the Exadata Database Machine contains an upgraded PDU that is running a newer version of firmware. This firmware ships with an enhanced Management Information Base (MIB) that is not compatible with the Exadata 12.1.x plug-in. In these cases, change the setting in the PDU to using the original MIB as illustrated in Figure 8-2.

1. Select **Original MIB** if you are monitoring the ILOM as an "Oracle Engineered System PDU" in Enterprise Manager.

2. To use the Enhanced MIB instead, you can use the "Oracle System Infrastructure PDU" and then convert Exadata Database Machine components to use Oracle Enterprise Manager Cloud Control 13*c*. For details on converting to this version, see Using the Conversion Wizard to Convert 12*c* Targets to 13*c* Targets.

Figure 8-2   Selecting Original MIB

Monitoring Agent Not Deployed for IPv6 Environments

Problem: For IPv6 environments, the monitoring agent is not deployed.

Cause: If the IPv6 address is not included in the `/etc/hosts` file, then the agent will not be deployed.

Resolution: Edit the `/etc/hosts` of the compute node (or the VM in case of virtual Exadata) to map the OMS host name to an IPv6 address.

Configure IPv6–SNMPv3 Subscription

You can only do SNMPv3 subscriptions on Oracle Exadata Storage Server page.

Prerequisites:

- You need to create an SNMPv3 user on Cell. See **Step 1** for instructions.

- Exadata Storage Server version must be 12.1.2.2 or later to support SNMPv3 subscription.

To configure your IPv6–SNMPv3 subscription:

1. Creating an SNMPv3 user on Exadata Storage Server Target.

   - Suppose you need a user called `"v3user"`. You can check whether this user is already present on the cell using this command:

     ```
     cellcli -e "list cell attributes snmpUser"
     ```

   - If this user is not present on the Exadata Storage Server:

     ```
     ALTER CELL snmpUser=((name='[v3user]', authProtocol='MD5', authPass-
     word='[passwd]', privProtocol='DES', privPassword='[passwd]'))
     ```

   > **Note:**
   >
   > The Enterprise Manager Agent supports DES and MD5/SHA combination.

2. When running the discovery process on 12c and 13c, ensure that the v monitoring credentials on the cell target in EM match the v user on the cell.

   > **Note:**
   >
   > Make sure that an SNMP v3 user has been created before the discovery process is initiated (see **Step 1** for instructions).

3. If you need to edit the SNMP v3 monitoring credentials of the Exadata Storage Server after discovery, you can log in to EM and:

- Select **Configuration**, then **Security**, then **Monitoring Credentials.**

- Select **Exadata Storage Server** type, and click on **Manage Monitoring Credentials** button.

- Select the **Exadata Storage Server** and set the v3 Credentials.

> **Note:**
>
> Ensure that the v3 monitoring credentials are setup on the cell target in EM which match the v3 user on the cell.

Index