# Oracle® Enterprise Manager

Exadata Management Getting Started Guide

Release 12.1 (12.1.0.1, 12.1.0.2, and 12.1.0.3)

**E27442-05**

December 2012

ORACLE®

Oracle Enterprise Manager Exadata Management Getting Started Guide, Release 12.1 (12.1.0.1, 12.1.0.2, and 12.1.0.3)

E27442-05

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

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

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

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

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

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

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

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

# Contents

**Preface** ..... v

Audience ..... v
Documentation Accessibility ..... v
Conventions ..... v

**1 Deployment Overview**

1.1 Oracle Exadata Database Machine Supported Hardware and Software ..... 1-1
1.1.1 Supported Component Versions ..... 1-2
1.1.2 Supported Operating Systems ..... 1-2
1.1.3 Oracle Exadata Database Machine Hardware Not Supported ..... 1-2
1.2 Oracle Exadata Plug-in Deployment Prerequisites ..... 1-3
1.2.1 Create a Database Server ILOM Service Processor User ..... 1-4
1.2.2 Verify Software Versions ..... 1-5
1.2.3 Verify Names Resolution ..... 1-6
1.2.4 Verify Firewall Configuration ..... 1-6
1.3 User Roles ..... 1-8
1.4 Install Enterprise Manager Agent ..... 1-8
1.4.1 Agent Installation Prerequisite - Solaris 11 Only ..... 1-8
1.4.2 Install Oracle Database and Oracle Exadata Plug-ins Using the Automated Kit ..... 1-9
1.4.3 Install Enterprise Manager Agent Using the Push Method ..... 1-9
1.4.3.1 Installing Oracle Management Agent in Silent Mode Option ..... 1-10
1.4.4 Manually Deploy Exadata Plug-in ..... 1-11

**2 Exadata Database Machine Discovery**

2.1 Prerequisites for Guided Discovery ..... 2-1
2.1.1 Secure Storage for Target Monitoring Credentials ..... 2-1
2.1.2 Discovery Precheck Script ..... 2-1
2.1.3 Manual Verification ..... 2-3
2.2 Automatic Discovery Process ..... 2-4

**3 Post-Discovery Configuration and Verification**

3.1 Set Up Compute Node Agent to Receive SNMP Notification ..... 3-1
3.2 Configure Storage Cell SNMP for Enterprise Manager Monitoring ..... 3-2
3.2.1 Check Current SNMP Configuration ..... 3-3
3.2.2 Configure SNMP Values Using `cellcli` ..... 3-4

3.2.3 Configure SNMP Values Using `dcli` (optional) ... 3-4
3.2.4 Verify SSH Connectivity ... 3-4
3.2.5 Remove a Subscription ... 3-5
3.3 Configure and Verify SNMP for InfiniBand Switch Targets ... 3-5
3.3.1 Set Up SNMP for InfiniBand Switch Targets Using Enterprise Manager ... 3-6
3.4 Configure the Compute Node ILOM SNMP for Enterprise Manager Monitoring ... 3-7
3.5 Verify Configuration for Oracle ILOM Server ... 3-8
3.6 Set Up SNMP for Cisco Ethernet Switch Targets ... 3-9
3.6.1 Verify the Cisco Ethernet Switch SNMP Configuration ... 3-10
3.7 Set Up SNMP for Power Distribution Unit (PDU) Targets ... 3-10
3.7.1 Verify the PDU SNMP Configuration ... 3-11
3.8 Set Up SNMP for KVM Targets ... 3-11
3.8.1 Verify the KVM SNMP Configuration (Base SNMP Configuration) ... 3-11
3.8.2 Verify the KVM SNMP Configuration (SNMP Forwarding to Agent) ... 3-12
3.9 Oracle Exadata Database Machine Dashboard Creation ... 3-12

## 4 Oracle Exadata Database Machine Administration

4.1 Creating Roles to Manage the Plug-in ... 4-1
4.2 View Exadata Database Machine Topology ... 4-2
4.2.1 Drilling Down to Individual Targets ... 4-3
4.2.2 Viewing Critical Hardware Information for the Database Machine ... 4-3
4.2.3 Viewing DB Machine Alerts ... 4-3
4.2.4 Remove Database Machine Target ... 4-4
4.3 Exadata Cell Management ... 4-4
4.3.1 Cell Administration ... 4-4
4.3.2 Access Exadata Cell Metrics/Alert Settings ... 4-6
4.3.3 Delete an Exadata Cell ... 4-6
4.4 InfiniBand Network Management ... 4-7
4.4.1 InfiniBand Metrics ... 4-7
4.4.2 Setting Up Alerts ... 4-7

## 5 Troubleshooting

5.1 Establish SSH Connectivity ... 5-1
5.2 Discovery Troubleshooting ... 5-2
5.2.1 Compute Node Error Message ... 5-2
5.2.2 Cell is not Discovered ... 5-2
5.2.3 Compute Node or InfiniBand Switch is not Discovered ... 5-3
5.2.4 InfiniBand Network Performance Page Shows No Data ... 5-3
5.2.5 ILOM, PDU, KVM, or Cisco Switch is not Discovered ... 5-3
5.2.6 Target Does not Appear in Selected Targets Page ... 5-3
5.2.7 Target is Down or Metric Collection Error After Discovery ... 5-4
5.2.8 Troubleshooting the Exadata Database Machine Schematic File ... 5-5
5.3 Exadata Database Machine Management Troubleshooting ... 5-6
5.4 Exadata Derived Association Rules ... 5-6

# 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 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. |

| Convention | Meaning |
| --- | --- |
| `monospace` | Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter. |

# 1

# Deployment Overview

This document describes the Enterprise Manager Cloud Control 12*c* supported configurations of Oracle Exadata Database Machine and the steps to deploy the Exadata plug-in.

In this chapter, you will find the information needed to get started with the installation and configuration for your device.

## 1.1 Oracle Exadata Database Machine Supported Hardware and Software

Enterprise Manager Cloud Control 12*c* is supported on the following Exadata Database Machine configurations:

- V2
- X2-2: Full rack, half rack, and quarter rack
- X2-8: Full rack
- X3-2: Full rack, half rack, quarter rack, and eighth rack
- X3-8: Full rack
- 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 12*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 Exadata plug-in Release 12.1.0.2:
    * 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.

- For Exadata plug-in Release 12.1.0.3:
  - 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.
- For all Exadata plug-in releases: User can confirm and select individual components for each Database Machine.

### 1.1.1 Supported Component Versions

The following component versions are supported for Enterprise Manager Cloud Control 12*c*:

- Exadata Storage Server Software 11g Release 2 (11.2.2.3.0 through 11.2.3.2)
- InfiniBand Switch Release 1.1.3.0.0 to 1.3.3.2.0.
- Integrated Lights Out Manager (ILOM) Release 3.0.9.27.a r58740
  - ILOM ipmitool Release 1.8.10.3 (for Oracle Linux) or Release 1.8.10.4 (for Oracle Solaris)
- Avocent MergePoint Unity KVM Switch Release 1.2.8
- Power Distribution Unit Release 1.04
- Cisco - Cisco IOS Software, Catalyst 4500 L3 Switch Software (cat4500-IPBASE-M), Version 12.2(46)SG, RELEASE SOFTWARE (fc1)

### 1.1.2 Supported Operating Systems

The following operating systems (where OMS and agent is installed on) are supported:

- Management Server Plug-in: (all Enterprise Manager Cloud Control 12*c*-certified platforms) specifically, as of now Linux x86, Linux x86-64, 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)

### 1.1.3 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 12.1 (12.1.0.1, 12.1.0.2, and 12.1.0.3):

- V1 hardware
- Super Clusters

  Starting with SPARC SuperCluster 1.1 and later, you can monitor all Exadata-related software and hardware components in the cluster using Oracle Enterprise Manager Exadata 12.1.0.3 plug-in only in the supported configuration described in the note below.

**Note:** Only Oracle SuperCluster with software Version 1.1 with DB Domain on Control LDOM-only environments are supported. Earlier versions of SPARC 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/compmon@0.5.11,5.11-0
.1.0.11:20120726T024158Z
```

Known issues:

- The pre-requisite check script `exadataDiscoveryPreCheck.pl` that is bundled in Exadata plug-in 12.1.0.3 does not support the `catalog.xml` file. Please download the latest `exadataDiscoveryPreCheck.pl` file from My Oracle Support as described in Discovery Precheck Script.
- 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. However, 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 have no Exadata Storage server members because they are already monitored.
- If the `perfquery` command installed in the Oracle SuperCluster has version 1.5.8 or later, you will encounter a bug (ID 15919339) 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 will not be reported in Enterprise Manager.

  To check your version, run the following command:

  ```
  perfquery -V
  ```

- Expansion rack
- Multi-Rack Exadata Database Machine

**Note:** Although Multi-Rack Exadata Database Machine display in schematic is not supported or monitored as a single entity. However, each individual Rack can be monitored and managed separately.

- Use of client network hostnames for compute nodes as Enterprise Manager target names is not supported with the Exadata plug-in Release 12.1.0.1 and 12.1.0.2. This support is added in 12.1.0.3.

## 1.2 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

### 1.2.1 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. Create a text file that contains one line with the password for the ILOM service processor root user ID in the `/tmp` directory called `changeme`. The `/tmp/changeme` file is used in the ILOM CLI command examples.

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='aucro'
Set 'role' to 'aucro'
```

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

```
ipmitool -I lan -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.

## 1.2.2 Verify Software Versions

### Exadata Storage Server Software

The supported version is Exadata Storage Server Software 11*g* Release 2 (11.2.2.3.0 through 11.2.3.2). To verify the cell software version on the Exadata cell, `ssh` to the Exadata cell as the `root`, `celladmin`, or `cellmonitor` 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&doctype=REFERENCE&id=88882

#### PDU Firmware

The PDU firmware version must be 1.02 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.

Software updates for KVM are available at:

http://www.avocent.com/Support_Firmware/MergePoint_Unity/MergePoint_Unity_Switch.aspx

### 1.2.3 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 12*c*, it is necessary for your local machine to be able to resolve the host name of Cloud Control 12*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.

### 1.2.4 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 12*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 12*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 under `<AGENT_HOME>/agent_inst/sysman/config`

5. Open SSH Ports

   The Enterprise Manager Cloud Control 12*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)

   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, KVM, and PDUs and the Agent.

## 1.3 User Roles

To manage the Exadata Storage Server plug-in, 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 Chapter 4, "Oracle Exadata Database Machine Administration."

## 1.4 Install Enterprise Manager Agent

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

- Agent Installation Prerequisite - Solaris 11 Only
- Install Oracle Database and Oracle Exadata Plug-ins Using the Automated Kit
- Install Enterprise Manager Agent Using the Push Method
- Manually Deploy Exadata Plug-in

**Notes:**

- 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.

### 1.4.1 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.

### 1.4.2 Install Oracle Database and Oracle Exadata Plug-ins Using the Automated Kit

The Oracle Enterprise Manager Cloud Control 12*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, see Doc ID 1440951.1 in My Oracle Support:

https://support.oracle.com

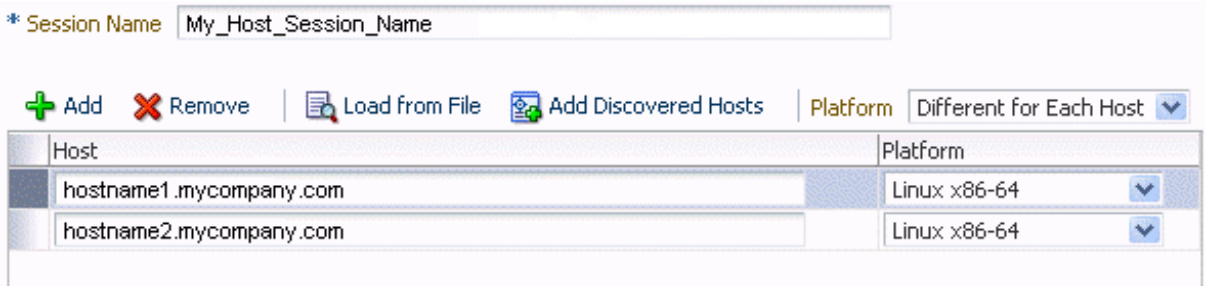
### 1.4.3 Install Enterprise Manager Agent Using the Push Method

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 12*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. Figure 1–1 shows how the selection should look.

***Figure 1–1 Add Host Targets***




3. Click **Next** to add the details for the host.

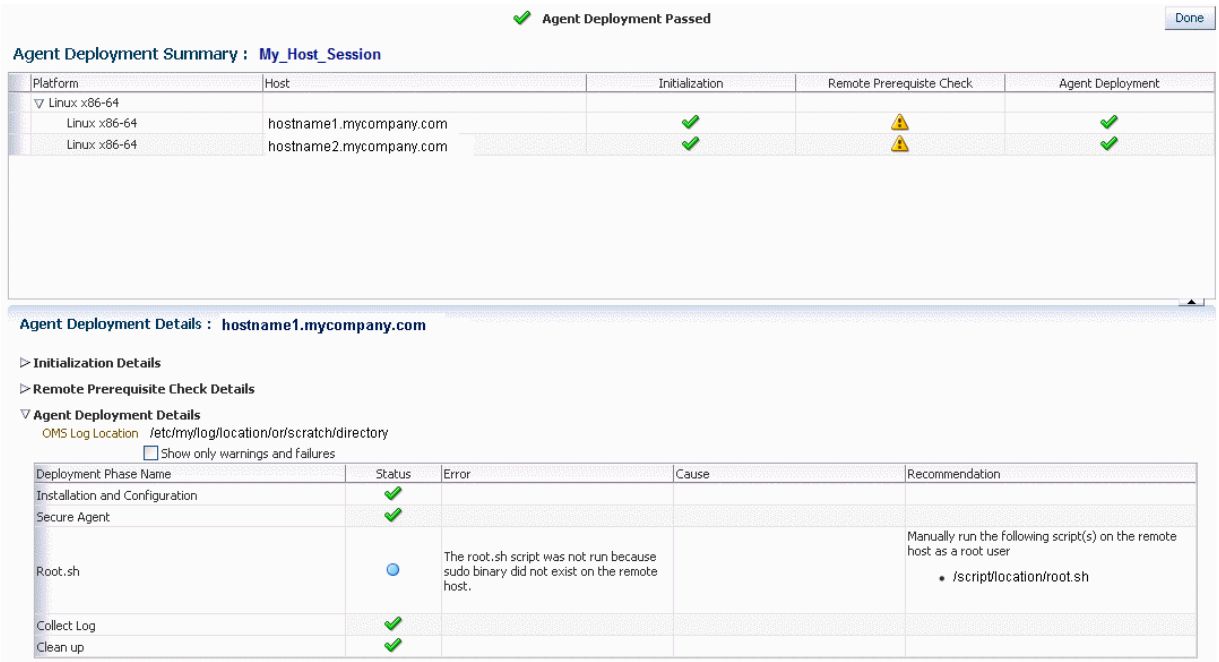
4. On the *Installation Details* screen, provide the following information:

   - 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 1–2 shows an example of a successful agent deployment.

***Figure 1–2 Agent Deployment Summary***




---

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

---

### 1.4.3.1 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 the *Installing Oracle Management Agent in Silent Mode* chapter in the *Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide* for more information:

`http://docs.oracle.com/cd/E24628_01/install.121/e24089/install_agent_usng_rsp.htm#CEGGACJE`

### 1.4.4 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, 12.1.0.2, or 12.1.0.3. 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 agent has deployed to all the 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.

# 2

# Exadata Database Machine Discovery

This chapter provides instructions for discovery of the Oracle Exadata Database Machine through Enterprise Manager Cloud Control 12*c*.

## 2.1 Prerequisites for Guided Discovery

Before you begin the 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. You should perform the steps outlined in the following sections before proceeding with Automatic Discovery Process.

1. Discovery Precheck Script
2. Manual Verification

### 2.1.1 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 afterward. 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.

### 2.1.2 Discovery Precheck Script

Some Exadata discoveries in Oracle Enterprise Manager 12*c* may run into issues because of various configuration mismatches in software setup. A discovery precheck script has been developed to resolve the most common configuration problems. Run the script before all Database Machine discovery and examine the output thoroughly before proceeding with Automatic Discovery Process.

### Download the Script

You can obtain the script in one of the following ways

- 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

- Access the script as part of the Oracle Enterprise Manager Cloud Control 12*c* Setup Automation kit (Exakit) 12.1.0.1.3. See Doc ID 1440951.1 in My Oracle Support for more information on the kit:

  https://support.oracle.com

- Access the script as part of Exadata plug-in 12.1.0.3 after the plug-in is deployed to the agent:

  ```
  <agent installation directory>/plugins/oracle.sysman.xa.discovery.plugin_
  12.1.0.3.0/discover/dbmPreReqCheck/exadataDiscoveryPreCheck.pl
  ```

### Run the Discovery Precheck Script

To run the script:

```
cd $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.

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 detail'
  ```

- 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
    * 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 and earlier, 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.

---

**Notes:**

- If you are using Exadata Release 11.2.3.2 and later, see Manual Verification for the file requirements.
- 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.

---

### 2.1.3 Manual Verification

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

- Use the 11.2 (or later) Database Oracle home directory when prompted for in Automatic Discovery Process.
- Pre-requirements for platform and Database Machine version.
- 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 or 12.1.0.2, 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, the target name of the compute node host target can be the host name in the management network or the client network.
- 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.
- Verify the Database Machine schematic file requirements for Exadata Release 11.2.3.2 and later:
  - Verify that the schematic file exists on the agent host selected for discovering the Exadata Database Machine at:

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

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

– Verify 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, but not in Releases 12.1.0.1 and 12.1.0.2.

---

**Notes:**

- If you are using Exadata Storage Server Software Release 11.2.3.1 and earlier, see Discovery Precheck Script for the Database Machine schematic file requirements.
- 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.

---

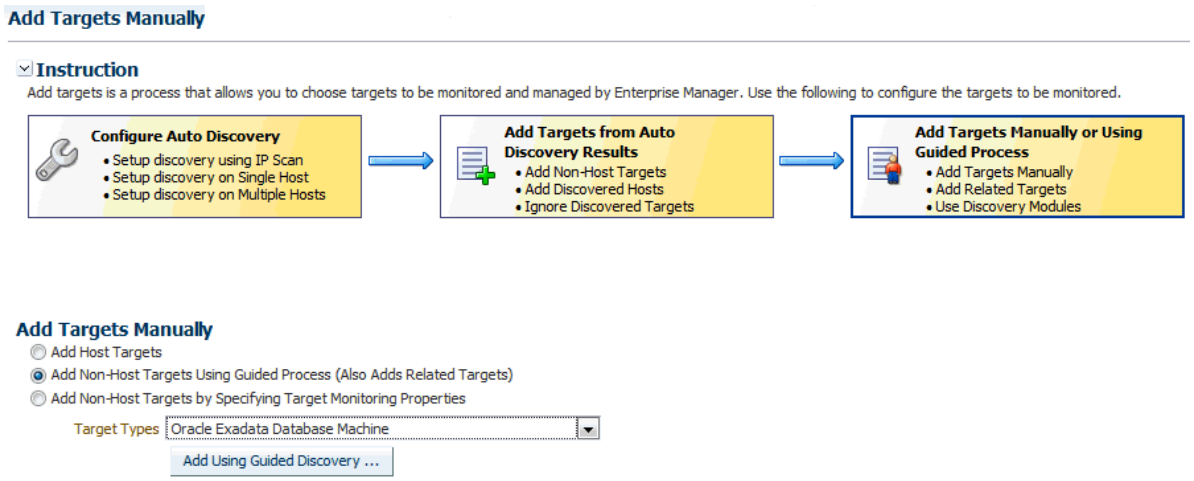
- For users of Oracle Enterprise Manager Cloud Control 12*c* Release 12.1.0.1.0 or if the installed version has been upgraded to Release 12.1.0.2.0 from 12.1.0.1.0 of the plug-in, you must manually push the Exadata plug-in to the agent.

## 2.2 Automatic Discovery Process

To automatically discover a Database Machine target, follow these steps:

1. From the Enterprise Manager home page, select the **Setup** menu (upper right corner), **Add Targets**, and then **Add Targets Manually**. Figure 2–1 shows the Add Targets Manually page.

***Figure 2–1 Add Target Manually***




2. Select the **Add Non-Host Targets Using Guided Process (Also Adds Related Targets)** option. From the Target Types drop-down, select **Oracle Exadata Database Machine**. Click **Add Using Guided Discovery**.

Enterprise Manager displays the Oracle Exadata Database Machine Discovery page. From here you can add the hardware components such as Exadata Storage Servers and InfiniBand Switches in the Oracle Exadata Database Machine as managed targets. You can choose to discover a new Database Machine and its hardware components as targets or instead discover newly added hardware components in an existing Database Machine as targets.

3. On the *Oracle Exadata Database Machine Discovery* page, select the **Discover a new Database Machine and its hardware components as targets** option. Click **Discover Targets**.

   Enterprise Manger displays the Database Machine Discovery wizard that steps you through the process of discovering the Database Machine. The first page of the wizard, the Discovery Inputs page, appears.

4. Select an agent on one of the compute nodes that has the schematic file.

   Click the search icon . In the Search and Select pop-up, enter the name of a target you have deployed (see "Install Enterprise Manager Agent Using the Push Method" on page 1-9) and click **Search**. Select a Target Name from the results list and click **Select**.

   > **Note:** If this is a partitioned Exadata Machine, be sure to pick one of the compute nodes that is part of the partition you wanted to be represented by this Database Machine target.

5. On the *Discovery Agent* section of the Discovery Inputs page, enter the following information:

   - **Agent URL:** The Agent deployed on compute node
   - **Database Oracle Home:** The Database Oracle home directory on compute node

   > **Note:** The Agent user needs execute privileges on the `$ORACLE_HOME/bin/kfod` binary of the Oracle home specified. (Oracle Database should be Release 11.2 or later.)

   Click **Next**.

6. On the *InfiniBand Discovery* page, enter the following information:

   - **IB Switch Host Name:** The InfiniBand switch host name (such as, `exa01sw-ib2.mycompany.com`)
   - **Nm2user Password:** The password for the InfiniBand switch

7. On the *Prerequisite* page, Enterprise Manager automatically performs the following checks:

   - Whether KFOD can be executed by the agent.
   - Whether the schematic file is present.
   - Whether the schematic file is readable by the agent.

8. On the *Components* page, the components below are pre-selected. You can deselect any unwanted component.

- **Compute Node:** select the hosts that are compute nodes in the Oracle Exadata Database Machine.
- **Oracle Exadata Storage Server**
- **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. Theses Integrated Lights Out Managers 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).

---

Click **Next** to display the Monitoring Agents page.

9. On the *Monitoring Agents* page, select an agent from the drop-down selection box or click Reset to reassign. Click **Next** to display the Agent Credential page

---

**Note:** The best practice is to use the **Manually select the agents** option on the *Monitoring Agents* page (instead of the **Automatically select the agents** option) and to use the Agent on compute node 1 for the **Monitoring Agent** and the Agent on compute node 2 for the **Backup Monitoring Agent** for all targets.

This configuration is to ensure that you know which Agents to use when configuring SNMP for Exadata Storage Cell and InfiniBand switch targets (see Configure Storage Cell SNMP for Enterprise Manager Monitoring and Configure and Verify SNMP for InfiniBand Switch Targets).

---

10. On the *Agent Credential* page, specify whether the agent host users and passwords are the same for all agents. The agent users and passwords are required to set up password-less SSH between the agents and the cells monitored by the agents.

    If the users and passwords are the same, choose **Same for all agents** and enter the user and password combination. If they are not the same for each agent, choose **Different for all agents** and enter each combination for each agent.

    Click **Next** to display the Monitoring Credential page.

11. On the *Monitoring Credential* page, configure the credentials for:

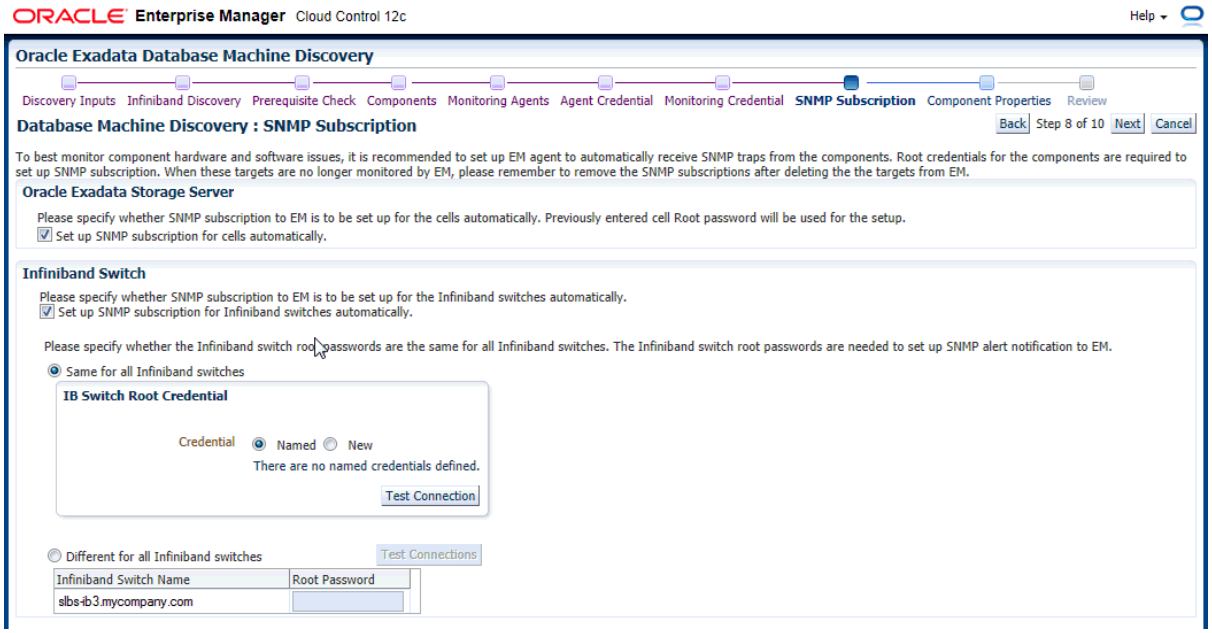
    - **Oracle Exadata Storage Server:** select the **Same for all cells** option. Enter the **Cell Root Password**.
    - **Infiniband Switch:** select the **Same for all Infiniband switches** option. Enter the **Infiniband Switch Nm2user Password**.
    - **ILOM:** select the **Same for all ILOM** option. Enter the **ILOM password**.

> **Note:** In all cases you can choose to enter the same user/password combinations for all components or you can enter the credentials separately for each occurrence.

Click **Next** to display the SNMP Subscription page.

12. On the *SNMP Subscription* page, automatically set up an SNMP subscription on the cell and InfiniBand Switch targets. Figure 2–2 shows an example of the SNMP subscription options.

***Figure 2–2 SNMP Subscription***



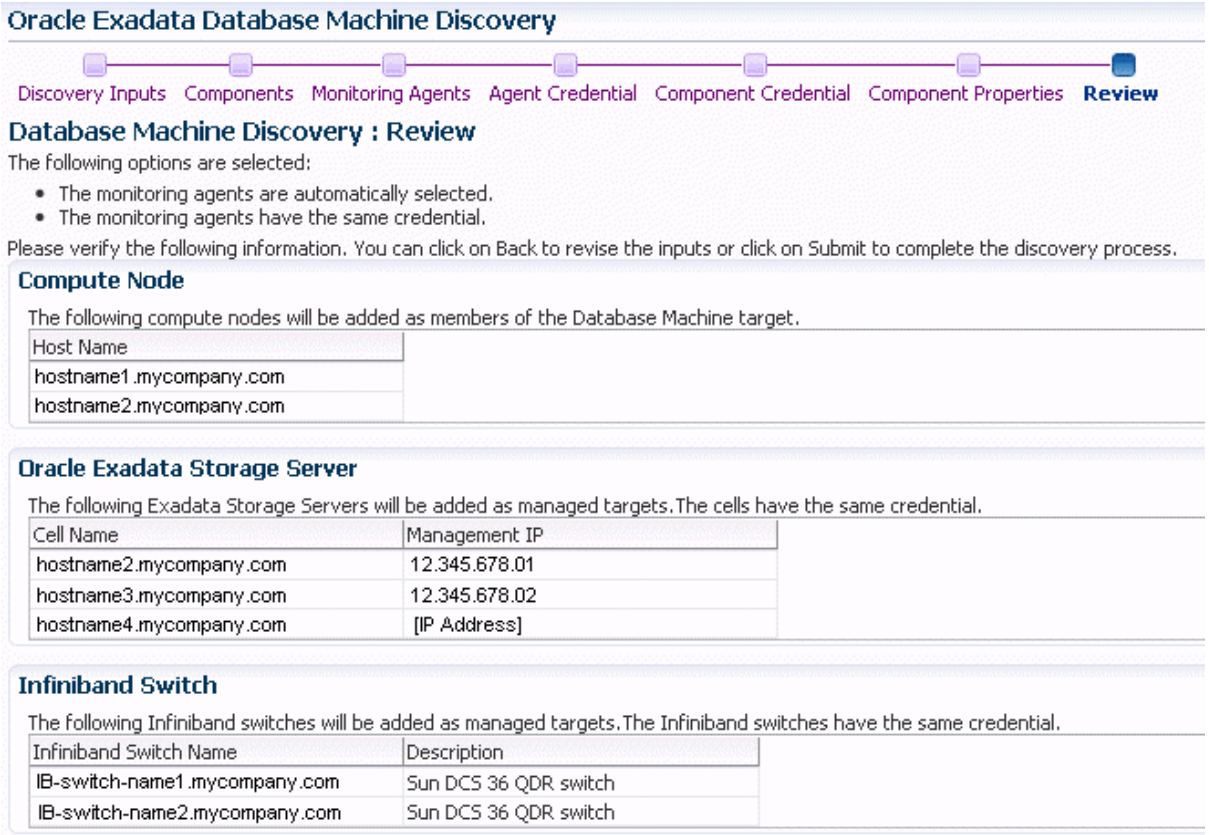

Click **Next** to display the Component Properties page.

13. On the *Component Properties* page, specify the target properties of the different components. For each component, enter the required information.

    Click **Next** to display the Review page.

14. On the *Review* page, verify each section is correct. Figure 2–3 shows an example of an accurate review.

***Figure 2–3 Database Machine Discovery Review Page***




15. If the information is correct, click **Submit**.
16. On the *Target Creation Summary* page, click **OK**.

Enterprise Manager displays the Target Promotion Summary page that displays the targets that are now managed targets.

The discovery of the Oracle Exadata Database Machine is complete.

# 3

# Post-Discovery Configuration and Verification

Once the Oracle Exadata Database Machine has been discovered through Enterprise Manager Cloud Control 12*c*, you must complete post-discovery configuration on the following targets:

- Set Up Compute Node Agent to Receive SNMP Notification
- 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
- Oracle Exadata Database Machine Dashboard Creation

**Remember:** 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, 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.

## 3.1 Set Up Compute Node Agent to Receive SNMP Notification

You must configure SNMP forwarding on each of the compute nodes being used as monitoring agents for other targets.

For the Enterprise Manager Agent to receive traps, an SNMP trap forwarder must be set up on the host where the Enterprise Manager Agent is running so that the forwarder utility can receive traps using port 162 and forward the same to the agent receivelet's listening port.

**Note:** The Enterprise Manager Agent receivelet listening port is specified as the value of the `EMD_URL` property in the `<AGENT_INST>/sysman/config/emd.properties` file, where `<AGENT_INST>` is the location of the Agent's `agent_inst` directory.

Follow the steps below on the compute nodes being used to monitor other targets. 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 other targets.

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 forwarder utility:

   ```
   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
   ```

5. Run the following command:

   ```
   chkconfig snmptrapd on
   ```

6. Run the following command to start the forwarder utility:

   ```
   service snmptrapd start
   ```

## 3.2 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.

**Notes:**

- For Enterprise Manager Cloud Control 12*c* Bundle Pack 1 (BP1):

  The SNMP trap setup for Exadata Storage Cells is done automatically after finishing the guided discovery process.
- For Exadata plug-in Release 12.1.0.2 and later:

  During the discovery process, you can optionally provide the necessary `root` credentials to set up SNMP trap for 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.

#### 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.

### 3.2.1 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 Master and non-Master 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
   ```

### 3.2.2 Configure SNMP Values Using `cellcli`

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

1. Set the `snmpSubscriber` value:

   ```
   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.

   **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.example.com,port=162,
   community=public,type=asr),(host='[host
   name]',port=[port]),(host='[host name]',port=[port]))"
   ```

2. Set the `notificationMethod` value:

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

3. Set the `notificationPolicy` value:

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

### 3.2.3 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
   snmpSubscriber=((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
   notificationMethod='snmp,mail'\""
   ```

3. Set the `notificationPolicy` value:

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

### 3.2.4 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**.

### 3.2.5 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.

---

**Notes:** 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.

---

## 3.3 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.

---

**Notes:**

- For Enterprise Manager Cloud Control 12*c* Bundle Pack 1 (BP1):

  The SNMP trap setup for Exadata Storage Cells is done automatically after finishing the guided discovery process.

- For Exadata plug-in Release 12.1.0.2 and later:

  During the discovery process, you can optionally provide the necessary `root` credentials to set up SNMP trap for Exadata Storage Cells. 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 **Alert Management**.
5. 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**.
6. 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:

   ```
   echo "set /SP/alertmgmt/rules/12 destination='0.0.0.0' destination_
   port=0" | spsh
   ```

### 3.3.1 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 Administration.
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 **Submit**.

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

## 3.4 Configure the Compute Node ILOM SNMP for Enterprise Manager Monitoring

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 Enterprise Manager to receive those traps, the `/opt/oracle.cellos/compmon/exadata_mon_hw_asr.pl` script must be run to configure SNMP subscriptions for the 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 and later.

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

```
# /opt/oracle.cellos/compmon/exadata_mon_hw_asr.pl -set_snmp_subscribers
"(host=hostname1.mycompany.com,port=3872,community=public,type=asr,fromip=11.222.3
3.444),(host=hostname2.mycompany.com,port=3872,community=public,type=asr,fromip=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
Community - 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.

**Important 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,fr
omip=11.222.33.444),
(host=hostname2.mycompany.com,port=162,community=public,type=asr,fr
omip=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=as
r,fromip=11.222.33.444),
(host=asrhostname2.mycompany.com,port=162,community=public,type=asr
,fromip=11.222.33.444),
(host=hostname1.mycompany.com,port=3872,community=public,type=asr,f
romip=11.222.33.444),
(host=hostname2.mycompany.com,port=3872,community=public,type=asr,f
romip=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=host1.mycompany.com,port=162,community=public,type=asr,fromip=10.10.10.226),
(host=host2.mycompany.com,port=162,community=public,type=asr,fromip=10.10.10.226),
(host=host3.mycompany.com,port=3872,community=public,type=asr,fromip=10.10.10.226)
,(host=host4.mycompany.com,port=3872,community=public,type=asr,fromip=10.10.10.226
)
```

## 3.5 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 fail 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. 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 nofail 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. 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.

## 3.6 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. Login to the Cisco switch and enter Configure mode:

   ```
   # telnet dm01sw-ip
   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
   ```

### 3.6.1 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 command 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
```

**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.

## 3.7 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 *PDU Threshold Settings for Oracle Exadata Database Machine* (See Doc ID 1299851.1) in My Oracle Support.

### 3.7.1 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.

## 3.8 Set Up SNMP for KVM Targets

The KVM needs to be configured to send SMNP traps to the Agents that monitor it.

Configure the KVM to send traps to monitoring agent host and receivelet listening port, the port value of `EMD_URL` property from the `$ORACLE_HOME/sysman/config/emd.properties` file (for example, 3872):

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**.

### 3.8.1 Verify the KVM SNMP Configuration (Base SNMP Configuration)

Run the `snmptrapd` command line utility or equivalent tool to verify the KVM configuration.

Follow the steps below on the monitoring Agent host:

1. Log in as root.
2. Run the following command:

```
service snmptrapd stop
```

3. Rename the `/etc/snmp/snmptrapd.conf` file to be `/etc/snmp/snmptrapd.conf_bk` to create a backup.
4. Run the following command:

```
snmptrapd -p 162
```

5. Reboot the KVM (to generate SNMP traps).
6. The terminal where the `snmptrapd` command was run should display the received trap which is generated by the KVM due to the reboot.

If step 6 is confirmed, the KVM has been configured correctly. Rename the backup file and restart the `snmptrapd` service:

1. Use **Ctrl+C** to stop the `snmptrapd` command that was started in step 4 above.
2. Rename the `/etc/snmp/snmptrapd.conf_bk` backup file to be `/etc/snmp/snmptrapd.conf`
3. Run the following command:

```
service snmptrapd start
```

### 3.8.2 Verify the KVM SNMP Configuration (SNMP Forwarding to Agent)

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. Log in to the KVM.
2. Click **Overview** on the left side of the screen under Unit View, Appliance.
3. Click **Reboot**.
4. Click **OK** to confirm KVM reboot in the window that asks if you want to continue.
5. In the Enterprise Manager Cloud Control console, go to the KVM target page. An Incident should be displayed for the KVM reboot event in the Incidents and Problems section of the page.

## 3.9 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 and Later

For Exadata Database Machine plug-in Release 12.1.0.3 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.

### Dashboard Creation for Exadata Database Machine Plug-in Release 12.1.0.2 and Earlier

For Exadata Database Machine plug-in Release 12.1.0.2 and earlier, create the Database Machine Dashboard:

1. Go to the following directory:

   ```
   /opt/oracle.SupportTools/emkit/exadata/dashboard/
   ```

2. Run the following script:

   ```
   perl DashboardOperations.pl
   ```

Running this script will generate one Dashboard report per Database Machine system.

> **Note:** For details of script usage, please see the Dashboard Report Script README.
>
> Creation of the dashboard assumes the use of the OMS `emkit` and can only be run from the OMS server that the kit was deployed on.
>
> If the OMS `emkit` is not installed, please refer to support note 1458346.1 in My Oracle Support for instructions:
>
> https://support.oracle.com

### 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.

# 4

# Oracle Exadata Database Machine Administration

This chapter provides the information needed to administer your Oracle Exadata Database Machine through Oracle Enterprise Manager Cloud Control 12*c*.

## 4.1 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.

## 4.2 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 performance, and drill down to individual targets from the Database Machine target home page.

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 **Target**, then select **Members Topology** from the drop-down menu.

   Enterprise Manager Cloud Control displays the Configuration Topology page.

### 4.2.1 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.

### 4.2.2 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 cells, 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.

### 4.2.3 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.

### 4.2.4 Remove Database Machine Target

In Enterprise Manager Cloud Control 12*c* Bundle Pack 1 (BP1), deleting the Database Machine target will delete the Database Machine system as well as its hardware component targets and associated systems.

In Enterprise Manager Cloud Control 12*c*, deleting the Database Machine target will only delete the Database Machine system itself, without deleting its hardware component targets and associated systems.You must manually delete each of these targets/systems:

- Hardware member targets:
  - Oracle Exadata Storage Server
  - Oracle InfiniBand Switch
  - Cisco Switch
  - PDU
  - KVM
  - Oracle ILOM Server
  - Host
- Associated systems:
  - Oracle Database Machine
  - Oracle Exadata Storage Server Grid
  - Oracle Database Exadata Storage Server System
  - Oracle InfiniBand Network

## 4.3 Exadata Cell Management

This section provides instructions to manage Exadata cells, including how to manage the administration of cell groups and single cells and how to configure SNMP to propagate alerts.

### 4.3.1 Cell Administration

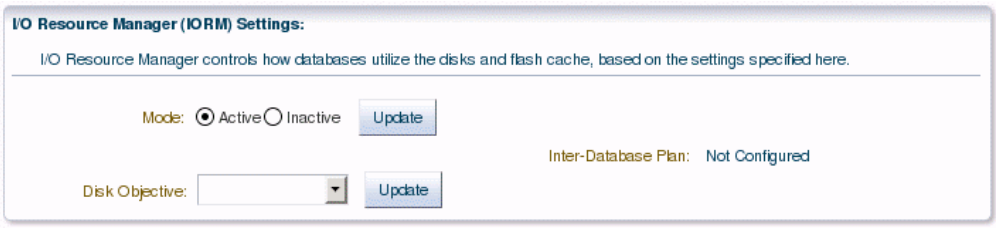
Oracle Exadata Database Machine Cells are added as targets during the database machine discovery workflow (see Chapter 2, "Exadata Database Machine Discovery") and are grouped automatically under the group **Exadata Grid**.

Based on the Exadata Grid group, a group of Exadata cells can be managed together through Enterprise Manager Cloud Control 12*c*. To update the I/O Resource Manager (IORM) settings:

1. From the Enterprise Manager home page, click the **Targets** drop-down menu. Select **Oracle Exadata Database Machine**.
2. In the Target Navigation pane, select **Exadata Grid** from the list.

> **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.

3. In the Exadata Grid pane, click the Target drop-down. Select **Administration**, then **Manage I/O Resource**. The Exadata Grid pane will update to show the IORM settings:




4. Before continuing, confirm the IORM objective settings before performing the administration task in Enterprise Manager Cloud Control 12c. From the command line, run the following command:

```
dcli -g cell_group cellcli -e "list iormplan attributes objective"
```

Output should show a value of **off**:

```
cell01: off
cell02: off
cell03: off
.
.
.
cell14: off
```

> **Note:** Starting with Exadata Storage Server Software 11*g* Release 2 (11.2.3.2) and later, the default output value is **basic** instead of **off**.

5. From the I/O Resource Manager (IROM) Settings pane, select **Auto** from the Disk Objective drop-down box. Click **Update**.

   The Exadata Cell Administration Wizard will appear.

6. On the Command page, the Cell Control Command-Line Interface (CellCLI) value should be:

```
alter iormplan objective = 'auto'
```

   Click **Next**.

7. One the Admin Credentials page, enter the username and password for the selected cells.

   Click **Next**.

8. On the Schedule page, enter a job name (required) and job description (optional). Then select the for the administration job to begin. You can start the job immediately or at a later time.

   Click Next.

9. On the Review page, verify the settings are correct. If there are no changes, click **Submit Command**.

10. 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.

11. 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
    ```

### 4.3.2 Access Exadata Cell Metrics/Alert Settings

To access the settings for Exadata Cell metrics/alert:

1. From the Enterprise Manager home page, select **Targets**, then **Oracle Exadata Storage Server**.

2. Click **Monitoring**, then **Metric and Collection Settings**. The default "Metrics with thresholds" is displayed.

3. Select **All metrics** from the drop-down list to display all editable metric alert setting.

### 4.3.3 Delete an Exadata Cell

If you need to remove an Exadata Cell, you can perform this task within Enterprise Manager Cloud Control 12c.

1. From the Enterprise Manager home page, select **Targets**, then **Oracle Exadata Database Machine**.

2. In the Target Navigation pane, select the cell you want to remove. You may need to expand the Exadata Grid item to view all of the available cells.

3. In the Exadata Grid pane, click the **Target** drop-down. Select **Target Setup**, then **Remove Target**.

4. On the confirmation page, click **Yes**. The cell target is deleted, and a confirmation page displays.

## 4.4 InfiniBand Network Management

All InfiniBand Switches are discovered automatically during the database machine discovery workflow (see Chapter 2, "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.

### 4.4.1 InfiniBand Metrics

#### 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.

### 4.4.2 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.

# 5 Troubleshooting

Review the sections below for troubleshooting tips and techniques on installing and configuring the Exadata plug-in.

## 5.1 Establish SSH Connectivity

For Release 12.1.0.1, the SSH key location is `<EMDROOT>/.ssh` where `EMDROOT` 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, 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:

     ```
     cd <EMDROOT>/.ssh
     ssh-keygen -t dsa -f id_dsa
     ```

     Where `<EMDROOT>` is the installation directory of the Enterprise Manager Agent.

   - For Release 12.1.0.2:

     ```
     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/authorized_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
```

## 5.2 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.

### 5.2.1 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
Manager. 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, hostname.mycompany.com)

### 5.2.2 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.
- 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
```

### 5.2.3 Compute Node or InfiniBand Switch is not Discovered

If there are problems with discovery of the compute node or the InfiniBand switch, possible 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
  xdb1swib3.us.oracle.com" enhanced port 0 lid 1 lmc 0
  ```

- To verify discovery of the compute node, run the following command on the compute 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 compute nodes:

  ```
  /opt/oracle.cellos/ib_set_node_desc.sh
  ```

### 5.2.4 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.

### 5.2.5 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.

### 5.2.6 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.

### 5.2.7 Target is Down or Metric Collection Error After Discovery

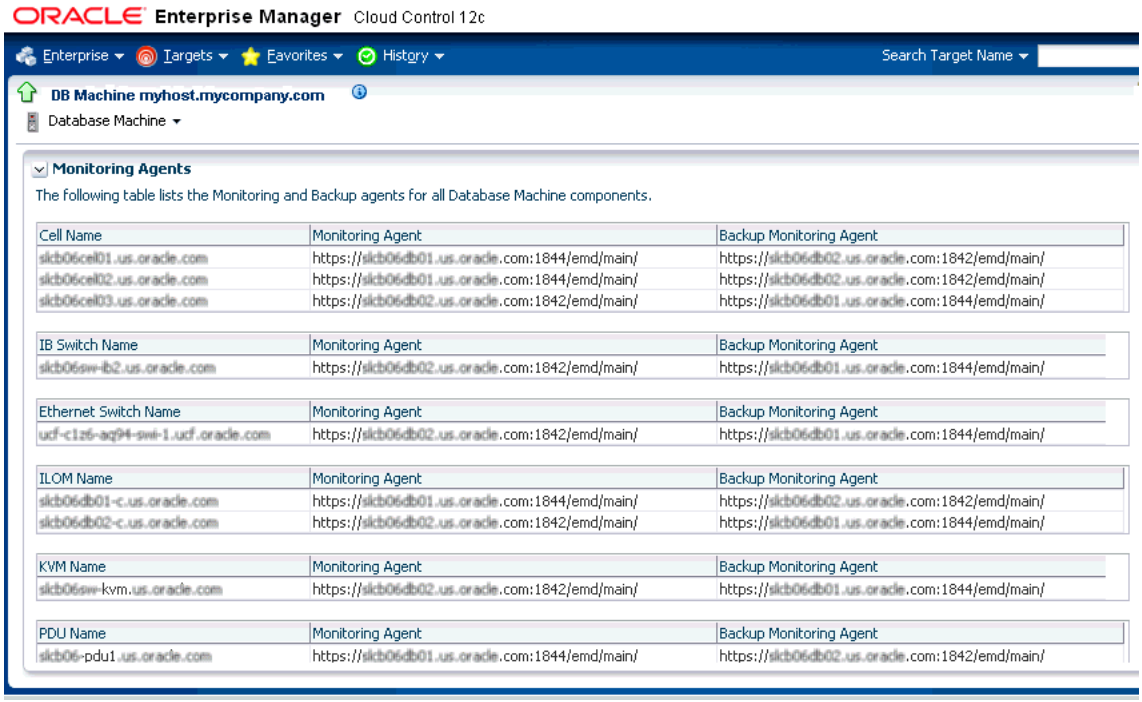
After the Exadata Database Machine guided discovery, an error that the target is down or that there is a problem with the metric collection may display. Possible causes and recommended solutions include:

- 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 5–1 shows an example of the monitoring agents:

***Figure 5–1 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.

## 5.2.8 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:
    ```

```
'weblogic.kernel.Default (self-tuning)']
ERROR model.DiscoveredTarget logp.251 -
ERROR: NMO not setuid-root (Unix only)
oracle.sysman.emSDK.agent.client.exception.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.

## 5.3 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.

## 5.4 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.