

Oracle® Enterprise Manager

System Monitoring Plug-in Installation Guide for Oracle Big Data Appliance

Release 12.1.0.4

E37801-06

June 2014

This document describes how to set up Oracle Big Data Appliance for monitoring within Enterprise Manager Cloud Control. The document contains the following sections:

- [Description](#)
- [Versions Supported](#)
- [Prerequisites](#)
- [Deploying the Big Data Appliance Plug-in on OMS](#)
- [Performing Rediscovery to Synchronize Cluster Configuration Changes](#)
- [Performing Post-Discovery Configuration and Verification](#)
- [Verifying and Validating the Plug-in](#)
- [Undeploying the Big Data Appliance Plug-in](#)
- [Documentation Accessibility](#)

1 Description

Oracle Big Data Appliance is an engineered system of hardware and software optimized to capture and analyze the massive volumes of unstructured data generated by social media feeds, e-mail, web logs, photographs, smart meters, sensors, and similar devices.

Oracle Big Data Appliance is engineered to work with Oracle Exadata Database Machine and Oracle Exalytics In-Memory Machine to provide the most advanced analysis of all data types, with enterprise-class performance, availability, supportability, and security.

The Oracle Linux operating system and Cloudera's Distribution including Apache Hadoop (CDH) underlie all other software components installed on Oracle Big Data Appliance.

In Enterprise Manager, you can:

- Discover the components of a Big Data Appliance Network and add them as managed targets.
- Manage the hardware and software components that comprise a Big Data Appliance Network as a single target or as individual targets.
- Study collected metrics to analyze the performance of the network and each Big Data Appliance component.

- Trigger alerts based on availability and system health.
- Respond to warnings and incidents.

2 Versions Supported

Big Data Appliance for Enterprise Manager plug-in requires the following versions of products:

- Enterprise Manager platform version 12.1.0.4 (and earlier supported versions)
- CDH, Cloudera's Distribution including Apache Hadoop 5.0 (and earlier supported versions)
- Exadata Plug-in 12.1.0.6 (and earlier supported versions)
- Oracle Big Data Appliance 3.0 (and earlier supported versions)
- Oracle Big Data Appliance Plug-in 12.1.0.4

3 Prerequisites

The following prerequisites must be met before you can deploy the Big Data Appliance plug-in:

- Enterprise Manager 12.1.0.4 (or other supported version) is installed and up and running. Enterprise Manager can be installed anywhere in the network, provided the Big Data Appliance machines are visible from the location. For performance reasons, try to install Enterprise Manager such that there is minimal latency when connecting to Big Data Appliance machines.
- Oracle representative has set up Oracle Big Data Appliance hardware.
- Oracle representative has run the Mammoth Utility to install Oracle Big Data Appliance 3.0 software on the 18 servers in the rack. The utility also installs Management Agents on all the servers and performs automatic discovery of Big Data Appliance Network targets.

Before running the utility, ensure that the Oracle Management Service (OMS) has the necessary platform agent image as described in [Section 3.1, "Synchronizing the Agent Image on OMS."](#) See also [Section 3.2, "Notes on the Mammoth Utility."](#)

- As the Oracle Big Data Appliance plug-in is dependent on the Oracle Exadata plug-in for hardware monitoring, the Oracle Exadata plug-in should already be deployed on OMS.

3.1 Synchronizing the Agent Image on OMS

If the OS where the Management Agent is to be installed differs from the OS where Oracle Management Service is installed, you must install the agent image that matches the Management Agent OS. By default, OMS has the same agent image as the platform on which it is installed. So, for example, if OMS is installed on a solaris64 platform, it has the agent image for solaris64. If the Management Agent is to be installed on a linux64 platform and OMS is on a solaris64 platform, you must install the agent image for linux64 on the OMS host.

Use the Self Update feature to download and apply the required agent image. To use Self Update effectively, note the following requirements:

- The Software Library must be configured.

- MOS credentials must be set.
- There can be no refresh errors on the Self Update page (typically indicates a problem with the MOS credentials; try resetting the credentials).
- Allow time for the refresh job to complete (select **Check Updates** on the Self Update page **Actions** menu to speed the process).

To use the Self Update feature:

1. From the **Setup** menu, select **Extensibility**, then select **Self Update**.
Ensure that the connection mode is success and that the most recent refresh occurred within the past 24 hours.
2. Click **Agent Software** and select the image for the platform you need.
3. Download and apply the selected agent image.

Proceed with BDA installation.

3.2 Notes on the Mammoth Utility

The Mammoth Utility includes a reconfiguration variation for adding or removing optional services such as Auto Service Request support and Enterprise Manager Management Agents. For example, if Big Data Appliance initial setup did not include installing Management Agents, you can subsequently run the reconfiguration utility to perform this task. If you do so, you must deploy the BDA plug-in on OMS prior to executing the utility. Note, however, that Oracle recommends that you install Management Agents on servers in the rack as part of initial BDA setup.

Note: You can also install Management Agents post BDA-setup as described in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

When you use the Mammoth Utility to expand a cluster, Management Agents are added to the new nodes in the cluster. Rediscovery then exposes the roles on these new nodes. Also consider the following scenarios:

- If you expand a cluster by adding nodes from the same rack, the new nodes will also have DataNode and TaskTracker services.
- If you expand a cluster by adding nodes from another rack, a second NameNode service and its failover controllers together with some Zookeeper nodes move to the second rack.
- A reimaging of all nodes resembles a fresh installation. Any node that goes down is removed from the cluster.

For information on Big Data Appliance hardware and software setup, and the Mammoth Utility, see the *Oracle Big Data Appliance Owner's Guide*.

4 Deploying the Big Data Appliance Plug-in on OMS

Deploying the Big Data Appliance plug-in implies first downloading the plug-in from the Enterprise Manager Store to the Software Library from where it can be deployed on OMS. See the "Plug-In Manager" chapter in the *Oracle Enterprise Manager Cloud Control Administrator's Guide* for steps to download and deploy the plug-in.

Note that if you are installing Management Agents post BDA plug-in setup using the Mammoth Reconfiguration Utility, you must deploy the BDA plug-in on OMS prior to executing the utility.

5 Performing Rediscovery to Synchronize Cluster Configuration Changes

Cluster expansion performed through the Mammoth Utility results in automatic rediscovery of cluster configuration changes. The user interface offers an alternative path to rediscovery. Follow the steps below to synchronize cluster configuration changes. Be sure to restart all services before proceeding.

To synchronize cluster configuration changes:

1. From the **Setup** menu, select **Add Target**, then select **Add Targets Manually**.
Enterprise Manager displays the Add Targets Manually page.
2. Choose **Add Targets Using Guided Process (Also Adds Related Targets)**.
3. From the **Target Types** drop-down list, select **Oracle Big Data Appliance**, then click **Add Using Guided Discovery**.

The Oracle Big Data Discovery wizard opens.

If You Encounter a No Targets Found Condition

It's possible upon performing rediscovery to click within a cluster and get a No Targets Found condition. This can happen if all of the following events took place:

- You upgraded from the 12.1.0.1 plug-in release.
- You changed the cluster configuration.
- You performed rediscovery.

The condition occurs because of a cluster target naming convention change since the 12.1.0.1 release. The workaround is to delete the OMS cluster targets and run rediscovery again.

5.1 Starting Big Data Discovery

Start the discovery process by specifying parameters and providing credentials to connect to various components.

Discovery and Monitoring Parameters

Complete the required fields as follows:

- Click the search icon and select any host in the Big Data Network.
- Enter the SNMP community string for the Cisco switch. The read-only string is `public`.

Credentials

If the four sets of credentials described below are not already set as a result of the BDA installation process running the Mammoth Utility, provide them as necessary:

- **Host Agent**-Named credentials for the "oracle" OS account that owns a Management Agent home.

- **ILOM Server**–Named credentials for the "root" OS account on an Oracle® Integrated Lights Out Manager (Oracle ILOM) server in the Big Data Network.
- **InfiniBand Switch NM2** –Named credentials for the "nm2user" OS account on an InfiniBand switch in the Big Data Network.
- **Cloudera Manager**–Named credentials for the "admin" account of the Cloudera Manager that manages the CDH cluster. Note that step 3 of the wizard provides a means to edit or add Cloudera Manager configurations.

Continue with the next step in the wizard, hardware discovery.

5.2 Discovering Big Data Hardware

The Big Data Discovery Hardware page displays the hardware components discovered for each Big Data Appliance in a Big Data Network. Hardware components include:

- Hosts (one for each of the 18 servers in a rack)
- Switches (both Sun InfiniBand and Cisco Ethernet switches)
- Integrated Lights Out Manager (ILOM) servers
- Power Distribution Units (PDU)

Use the **Expand All** menu item to display all components.

For more information on hardware components as managed targets, see the "Discovering and Managing Exadata Targets and Systems" chapter in the *Enterprise Manager Cloud Control Administrator's Guide*.

Setting Credentials

If these credentials are not already set as a result of the BDA installation process running the Mammoth Utility, set them as necessary. You can set credentials on all or selected categories of components; that is, hosts, ILOM servers, and InfiniBand switches. For ease of use, it is common to use the same credentials to access all components of a given type.

Note: If you have more than one Big Data Appliance Network target and they have different credentials, you must provide each set of credentials to discover each target. This applies as well to discovering ILOM server and InfiniBand switch targets that have different credentials.

For example, to set credentials for all hosts:

1. Select the Hosts folder (or any host within).
2. From the **Set Credentials** menu, select **All Hosts**.
3. Complete the Set Credentials dialog, then click **OK**.

To set credentials on selected items, ILOM servers for example:

1. Open the ILOM Servers folder.
2. Multiselect servers within the folder.
3. From the **Set Credentials** menu, select **Selected Items**.

4. Complete the Set Credentials dialog, then click **OK**.

Cisco Switch Properties

To edit Cisco switch properties:

1. Select the Cisco switch table row in the hierarchy.
2. Click the **Cisco Switch Properties** button.
3. Enter appropriate values for the properties, then click **OK**.

PDU Properties

To edit PDU properties:

1. Select the PDU table row in the hierarchy.
2. Click the **PDU Properties** button.
3. Enter appropriate values for the properties, then click **OK**.

Continue with the next step in the wizard, Cloudera Manager configuration. This is an optional step.

5.3 Configuring Cloudera Manager

Each CDH cluster can have its own Cloudera Manager. Use the Cloudera Manager page to add and edit Cloudera Manager configurations. This is an optional step.

To edit the configuration:

1. Select the table row, then click the **Edit** button.
2. Make changes to the URL and credentials as appropriate.
3. Click **OK**.

Continue with the next step in the wizard, Big Data software discovery.

5.4 Discovering Big Data Software

The Big Data Discovery Software page displays the software components in the form of a CDH cluster discovered for each Big Data Appliance in a Big Data Network. A CDH cluster consists of the following components:

- MapReduce is the job system in which MapReduce jobs run using the file system (HDFS). The MapReduce system consists of a master node called JobTracker and multiple worker nodes called TaskTrackers. MapReduce2 (YARN), the next generation of MapReduce may also be present. YARN consists of one Resource Manager and multiple Node Managers.
- HDFS (Hadoop Distributed File System) High Availability consists of two master nodes called NameNodes and worker nodes called DataNodes. Each NameNode has a Failover Controller. There are also JournalNodes (typically three, but there can be more, provided it is an odd number), and a Balancer to balance disk space across the cluster.
- Cloudera Manager is the Hadoop administrative application.
- ZooKeeper is a centralized service for maintaining Hadoop configuration information.

This page is for information only, denoting the software components discovered, their associated hardware component and appliance. There are no actions to perform on this page.

Continue with the next step in the wizard, job review and submittal.

5.5 Submitting the Discovery Job

The Review page provides a summary of the discovery process, including the monitoring agents on all hardware components. When satisfied with the results, click **Submit** to promote the discovered targets to managed status.

6 Performing Post-Discovery Configuration and Verification

The Simple Network Management Protocol (SNMP) is a protocol used for managing or monitoring devices, where many of these devices are network-type devices such as routers, switches, and so on. SNMP enables a single application to first retrieve information, then push new information between a wide range of systems independent of the underlying hardware.

Post-discovery, perform the following setup procedures to monitor SNMP alert traps generated by hardware targets:

- [Setting Up SNMP for InfiniBand Switch Targets](#)
- [Setting Up the ILOM Server SNMP for Enterprise Manager Monitoring](#)
- [Setting Up SNMP for Cisco Ethernet Switch Targets](#)
- [Setting Up SNMP for Power Distribution Unit \(PDU\) Targets](#)

These procedures are not necessary to otherwise monitor BDA clusters.

6.1 Setting Up SNMP for InfiniBand Switch Targets

To configure 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 server 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
```

If a time-out message appears as output for the above command, it means that the InfiniBand switch is not yet configured for SNMP.

To remove the subscription:

```
echo "set /SP/alertmgmt/rules/12 destination='0.0.0.0' destination_port=0" |
spsb
```

Now, 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.

6.2 Setting Up the ILOM Server SNMP for Enterprise Manager Monitoring

The ILOM server targets are responsible for displaying a number of disk failure alerts for their respective server that are received as SNMP traps. For Enterprise Manager to receive these traps, the `/opt/oracle/bda/compmon/bda_mon_hw_asr.pl` script must be run to configure SNMP subscriptions for the agents that have been configured to monitor the ILOM server targets.

The `bda_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/bda/compmon/bda_mon_hw_asr.pl -set_snmp_subscribers
"(host=hostname1.mycompany.com,port=3872,
community=public,type=asr,fromip=11.222.33.444),(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 server:

- The host values should be the host names of the agents configured to monitor the ILOM server target associated with the server.
- The fromip values should be the IP address of the server that the ILOM server target is associated with.

For example, if you have a rack with server targets bda1node01 through bda1node18 and associated ILOM server targets bda1node01-c through bda1node18-c, then you would need to run the script once on each server—therefore, the script would be run 18 times in total.

- On server bda1node01, the host and port values would be the host names and ports of the agents monitoring ILOM server target bda1node01-c and the fromip value would be the IP address of the server itself, bda1node01.
- On server bda1node02, the host and port values would be the host names and ports of the agents monitoring ILOM server target bda1node02-c and the fromip value would be the IP address of the server itself, bda1node02... and so on.

This is a good example of where Manual selection of Management Agents for targets is useful. If the first two servers 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 servers.

The `bda_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 `bda_mon_hw_asr.pl` script to get the current set of subscribers using the `-get_snmp_subscribers` parameter.

For example:

```
# /opt/oracle/bda/compmon/bda_mon_hw_asr.pl -get_snmp_subscribers -type=asr
```

Suppose the current list is:

```
(host=hostname1.mycompany.com,port=162,community=public,type=asr,fromip=11.222.33.  
444),  
(host=hostname2.mycompany.com,port=162,community=public,type=asr,fromip=11.222.33.  
444)
```

Then new subscriptions can be added using the following command:

```
/opt/oracle/bda/compmon/bda_mon_hw_asr.pl -set_snmp_subscribers  
"(host=asrhostname1.mycompany.com,port=162,community=public,type=asr,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,fromip=11.222.33.  
.444),  
(host=hostname2.mycompany.com,port=3872,community=public,type=asr,fromip=11.222.33.  
.444) "
```

After adding the new subscribers, run the command `bda_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/bda/compmon/bda_mon_hw_asr.pl -get_snmp_subscribers -type=asr
(host=asrhostname1.mycompany.com,port=162,community=public,type=asr,fromip=10.10.10.226),
(host=asrhostname2.mycompany.com,port=162,community=public,type=asr,fromip=10.10.10.226),
(host=hostname1.mycompany.com,port=3872,community=public,type=asr,fromip=10.10.10.226)
,(host=hostname2.mycompany.com,port=3872,community=public,type=asr,fromip=10.10.10.226)
```

Verifying 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. From the **Targets** menu, select **BDA**. Select an Oracle ILOM Server target using the target navigation pane.

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

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

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

The output should be similar to:

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

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

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

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

The output should be similar to:

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

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

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

5. Repeat for the remaining configured ILOM Servers in the BDA Network.

6.3 Setting 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 `bdal-sw-ip` with the name of the Cisco Ethernet Switch target being configured):

1. Log in to the Cisco switch using Telnet or SSH and enter Configure mode. Note that Telnet is disabled by default on BDA for security reasons. So if Telnet is not available, use SSH as admin or root user.

```
# ssh admin@bdal-sw-ip
User Access Verification Password:
bdal-sw-ip> enable
Password:
bdal-sw-ip# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
bdal-sw-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:

```
bdal-sw-ip(config)# access-list 1 permit [EMagentIPAddr]
bdal-sw-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:

```
bdal-sw-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:

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

5. Verify settings and save the configuration:

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

Verify the Cisco Ethernet Switch SNMP Configuration

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

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

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

If a time-out message appears as output for the above command, then it means that the Cisco Switch is not yet configured correctly.

6.4 Setting 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://bda1-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 PDU threshold settings, see Section 7.4.3, "Configuring the Threshold Settings for the PDUs," in the *Oracle Big Data Appliance Owner's Guide*.

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
```

If a time-out message appears as output for the above command, then it means that the PDU is not yet configured correctly.

7 Verifying and Validating the Plug-in

Upon successful discovery of a Big Data Appliance Network and SNMP setup for hardware components, take the following steps to verify and validate that Enterprise Manager is properly monitoring the plug-in target:

1. From the **Targets** menu, select **Big Data Appliance**.

The Big Data page appears.

2. Select a discovered target in the Target Navigation panel on the left.

The Big Data Network page appears.

3. Select a Big Data Appliance Network target in the Target Navigation panel, then select **Expand All** in the **View** menu.

The components of the Big Data Appliance Network target appear in Target Navigation panel, including:

- InfiniBand network and switches
 - A CDH cluster that includes Cloudera Manager, a job system (MapReduce or MapReduce2), a file system (HDFS), and Zookeeper
 - Big Data Appliance target that includes hosts, ILOM servers, Cisco switches, and power distribution units (PDU)
4. Drill down to check on the availability and health of targets within the Big Data Appliance Network target.

For example, when you select the Big Data Appliance target, you see an overview that summarizes the hardware components in terms of the number and status of each component type as well as the number of related incidents and alerts. There is a summary of BDA target hosts that shows the status of all the CDH cluster components. There is also a schematic that denotes component placement by rack within the appliance and the status, color-coded by component type.

8 Undeploying the Big Data Appliance Plug-in

See the "Plug-In Manager" chapter in the *Oracle Enterprise Manager Cloud Control Administrator's Guide* for steps to undeploy the plug-in.

9 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.

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 END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

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

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

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

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

Cloudera, Cloudera CDH, and Cloudera Manager are registered and unregistered trademarks of Cloudera, Inc.