Oracle® Enterprise Manager

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

Release 13.1.1.0

E66322-03

March 2016

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

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, email, 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.

The Oracle Enterprise Manager Big Data Appliance plug-in enables you to use the same system monitoring tool for Oracle Big Data Appliance as you use for Oracle Exadata Database Machine or any other Oracle Database installation. With the plug-in, you can view the status of the installed software components in tabular or graphic presentations, and start and stop these software services. You can also monitor the health of the network and the rack components.

In Enterprise Manager you can monitor all Oracle Big Data Appliance racks on the same InfiniBand fabric. You can see summary views of both the rack hardware and the software layout of the logical clusters.

You can also do the following:

- 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 BDA 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 Cloud Control 13*c* Release 1 (and earlier 12.1.0.x supported versions)
- CDH, Cloudera's Distribution including Apache Hadoop 5.*x* (and earlier supported versions)
- Oracle Big Data Appliance 3.0 or later
- Oracle Big Data Appliance Plug-in 13.1.1.0

3 Prerequisites

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

- A supported version of Enterprise Manager Cloud Control 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 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, "About the Mammoth Utility."
- The Oracle Big Data Appliance plug-in has an engineered systems dependency for hardware monitoring. For Enterprise Manager 12.1.0.x, the appropriate Oracle Exadata plug-in should already be deployed on OMS. For Enterprise Manager 13*c* Release 1, the appropriate Systems Infrastructure plug-in should already be

deployed on OMS. In either case, these are default plug-ins and should always be available.

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 About the Mammoth Utility

Mammoth is a command-line utility for installing and configuring the Oracle Big Data Appliance software. Using Mammoth, you can:

- Set up a cluster for either CDH or Oracle NoSQL Database.
- Create a cluster on one or more racks.
- Create multiple clusters on an Oracle Big Data Appliance rack.
- Extend a cluster to new servers on the same rack or a new rack.
- Update a cluster with new software.

When you use the Mammoth utility to extend 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 extend a cluster by adding nodes from the same rack, the new nodes will also have DataNode and TaskTracker services.
- If you extend 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 reconfiguration considerations, adding or removing optional services such as Auto Service Request support for example, Oracle recommends use of the Oracle Big Data Appliance Command-Line Interface (`bdacli`).

For information on Big Data Appliance hardware and software setup, the Mammoth utility, and the `bdacli` 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 "Managing Plug-Ins" 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 `bdacli` 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 Using Guided Process**.

3. On the guided process page, select **Oracle Big Data Appliance,** then click **Add**.

   The Oracle Big Data Discovery wizard opens.

5.1 Starting Big Data Discovery

Big Data discovery occurs automatically as part of Big Data Appliance installation and setup using the Mammoth utility. You can subsequently use this wizard to perform rediscovery.

Complete the required fields as follows:

- Click the search icon and select any host in the Big Data Network.
- Provide named credentials for the "oracle" OS account that owns a Management Agent home.

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, Promoting, and Adding Systems Infrastructure Targets" chapter in the *Enterprise Manager Cloud Control Administrator's Guide*.

Continue with the next step in the wizard, setting hardware credentials.

5.3 Setting Hardware 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.

- **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.

> **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**.

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

5.4 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.

5.5 Discovering Big Data Software

The Big Data Discovery Software page displays the software components in the form of a Hadoop cluster discovered for each Big Data Appliance in a Big Data Appliance Network.

A Hadoop cluster consists of a myriad of servers, nodes, agents, trackers, and other components, each with specific responsibilities with regard to managing and organizing massive volumes of data.

This page is for information only, denoting the software components discovered, status, 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.

5.6 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:

- Configuring and Verifying SNMP for InfiniBand Switch Targets
- Configuring and Verifying ILOM Server SNMP for Enterprise Manager Monitoring
- Configuring and Verifying SNMP for Cisco Ethernet Switch Targets
- Configuring and Verifying SNMP for Power Distribution Unit (PDU) Targets

These procedures are not necessary to otherwise monitor BDA clusters.

6.1 Configuring and Verifying 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.

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 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" |
   spsh
   ```

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.

6.2 Configuring and Verifying 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=10.10.1
0.226),
(host=asrhostname2.mycompany.com,port=162,community=public,type=asr,fromip=10.10.1
0.226),
(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)
```

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 purposes only and does not reflect a true fault condition.

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

6.3 Configuring and Verifying 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 `bda1sw-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@bda1sw-ip
User Access Verification Password:
bda1sw-ip> enable
Password:
bda1sw-ip# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
bda1sw-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:

```
bda1sw-ip(config)# access-list 1 permit [EMagentIPaddr]
bda1sw-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:

   ```
   bda1sw-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:

   ```
   bda1sw-ip(config)# snmp-server enable traps envmon
   ```

5. Verify settings and save the configuration:

   ```
   bda1sw-ip(config)# end
   bda1sw-ip# show running-config
   bda1sw-ip# copy running-config startup-config
   ```

To verify the Cisco Switch configuration, run the `snmpwalk` command line utility or equivalent tool.

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 Configuring and Verifying 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 information on PDU threshold settings, see Section 11.8, "Monitoring the PDU Current," in the *Oracle Big Data Appliance Owner's Guide*.

To verify the PDU configuration, use the `snmpwalk` command line utility or equivalent tool.

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. Click the Target Navigation hierarchy icon to the left of the BDA Network target.

   Top-level targets appear for Big Data Appliance, Hadoop Cluster, and Systems Infrastructure Rack.
3. Expand any one of these top-level targets to display respective components in the tree hierarchy:
   - Big Data Appliance–host targets that support the BDA network.
   - Hadoop Cluster– Cloudera Manager and the various file system, framework, engine, and platform components that cooperate to manage massive volumes of data
   - Systems Infrastructure Rack–the hosts, ILOMs, PDUs, and switches that store and distribute massive volumes of data
4. Drill down to check on the availability and health of targets within the BDA Network target.

   For example, when you select the Hadoop Cluster target, you can see the following information at a glance:
   - The status of all the software components.
   - The security measures in play for the cluster.

- Host utilization in terms of CPU, memory, and file system as a percentage, and network in terms of megabytes per second.
- Hadoop performance in terms of containers (running and allocated), name and data node activity, and storage capacity used.
- A summary of incidents by target and severity.

8 Performing Administrative Tasks

You can perform a limited range of administrative tasks in the Enterprise Manager Cloud Control console, including:

- Modifying Cluster Components
- Administering InfiniBand Network from the Host Page
- Administering InfiniBand Network from the Systems Infrastructure Switch Page

8.1 Modifying Cluster Components

1. From the **Targets** menu, select **Big Data Appliance**.
2. Expand the Big Data Network target and select the Hadoop Cluster component.
3. From the Hadoop Cluster menu, select **Cluster Administration**, then **Modify Components**.
4. Choose to enable, disable, or modify cluster components.
5. Provide root credentials for the primary host to perform selected actions on the cluster components
6. Satisfy additional requirements depending on the cluster, as detailed in Table 1.

Table 1 Cluster Component Requirements

Component	Requirements
Automatic Service Requests	▪ ASR Manager host name and port ▪ ASR user and password
Kerberos	▪ Host names of Kerberos domain controllers ▪ Kerberos realm ▪ KDC password ▪ Oracle OS password ▪ Cloudera Manager admin password
Big Data Connectors	▪ MySQL root password ▪ ODI MySQL password ▪ Cloudera Manager admin password
Audit Vault	▪ Audit Vault admin user ▪ Audit Vault server, port, and password ▪ Audit Vault service
Big Data SQL	▪ Cloudera Manager admin password

Table 1 (Cont.) Cluster Component Requirements

Component	Requirements
Disk Encryption	■ Post install root password ■ Disk encryption password ■ Oracle OS password ■ Cloudera Manager admin password
Network Encryption	■ Kerberos enabled ■ Oracle OS password ■ Cloudera Manager admin password
Sentry	■ Kerberos enabled ■ Oracle OS password ■ Cloudera Manager admin password

8.2 Administering InfiniBand Network from the Host Page

Administer an InfiniBand Network from the Systems Infrastructure Server page by taking the following steps:

1. From the **Targets** menu, select **Big Data Appliance**, then select the Big Data Network target.
2. In the Software Overview section, click a Host link.
3. From the **Host** target menu, select **Administration**, then select **InfiniBand Network Administration**.
4. At the Command step, select an operation and an appropriate port from the respective drop-down menus, then click **Next**.
5. At the Credentials & Schedule step, select or enter applicable target credentials and specify scheduling parameters, then click **Next**.
6. At the Review step, verify the settings and, if satisfied, click **Submit**.
7. At the Status step, confirm that the job submission succeeded. Click the job name to view job status in the Jobs System. When you are finished, click **Done** to close the wizard.

8.3 Administering InfiniBand Network from the Systems Infrastructure Switch Page

Administer an InfiniBand Network from the Systems Infrastructure Switch page by taking the following steps:

1. From the **Targets** menu, select **Big Data Appliance**.
2. Expand the Big Data Network target and select the Systems Infrastructure Rack component.
3. From the **Systems Infrastructure Rack** target menu, select **Administration**, then select **InfiniBand Network Administration**.
4. At the Command step, select an operation as follows:
   - To switch the LED on or off, select the appropriate command from the drop-down menu.

- To enable or disable a port, or to clear performance or error counters, select the appropriate command and then the applicable port from the respective drop-down menus.
- To set up an SNMP subscription, select the Agent URL from the drop-down menu and provide the associated SNMP community string.

Click **Next**.

5. At the Credentials & Schedule step, select or enter applicable target credentials and specify scheduling parameters, then click **Next**.
6. At the Review step, verify the settings and, if satisfied, click **Submit**.
7. At the Status step, confirm that the job submission succeeded. Click the job name to view job status in the Jobs System. When you are finished, click **Done** to close the wizard.

9 Undeploying the Big Data Appliance Plug-in

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

10 Documentation Accessibility

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

Access to Oracle Support

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

System Monitoring Plug-in Installation Guide for Oracle Big Data Appliance, Release 13.1.1.0
E66322-03

in an applicable agreement between you and Oracle.

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