Using Oracle Enterprise Manager Cloud Control 13*c*

Lab Guide

Table of Contents

. Using Oracle Enterprise Manager Cloud Control

**Course Lab
Environment:
Security Credentials**

Course Lab Environment: Security Credentials

Overview

These pages provide a ready reference of host names, usernames, and passwords that you will use throughout the practices.

Security Credentials for All Practices

Lab: Getting to Know Your Classroom Environment

Host Name	Username and Passwords	Database Instance(s)	Applications
Your classroom PC, if available	Will be provided by your instructor		
emcc.example.com	root/welcome1 oracle/welcome1	**em13rep** system/welcome1 sys/ welcome1 dbsnmp/dbsnmp	**Enterprise Manager Cloud Control** sysman/welcome1 **WebLogic Server** weblogic/ welcome1

Practices for Lesson 1: Introduction

Overview

Practices for Lesson 1: Overview

Practices Overview

In these practices, you familiarize yourself with the virtual environment and the Oracle software preinstalled on it (databases, listeners, and Oracle Enterprise Manager Cloud Control).

Lab 1-1: Checking the Virtual Environment - OPTIONAL

Overview

In this Lab, you access your classroom PC and check your virtual machines.

Assumptions

You are logged in to your classroom PC as the instructor advises you.

Tasks

1. You are assigned two running VMs: `em13c` and `host01`. Double-click the Tiger VNC or NX icon on your desktop to connect. *Your instructor will recommend one or the other.*

2. Log in to your first virtual environment, `em13c`, as user `oracle`, as per your instructor's direction. Note the desktop background for this session indicates that you are connected to `em13c`.

3. Log in to your second virtual environment, `host01`, as user `oracle`, as per your instructor's direction. Note the desktop background for this session indicates that you are connected to `host01`.

   Do not exit these sessions. They will be used throughout your exercises.

4. Note the location of your **Student Guide** and **Activity Guide** as pointed out by your instructor. Ensure that you can view them.

5. Note the location of the reference document **Course Lab Environment: Security Credentials**. Refer to this document for **all** passwords (OS and Oracle software passwords) needed for these exercises.

Lab 1-2: Getting to Know Your Oracle Software Classroom Environment - (The environment details will not match up exactly)

Overview

In this Lab, you get to know your Oracle software environment by examining your host machines as the `oracle` user.

Assumptions

You are logged in to your classroom PC and have two VNC/NX sessions, one connected to `em13c` and one to `host01`.

Tasks

1. When your virtual environment is started, some tasks are automatically performed:

    *   Three databases (`em13rep` on `em13c`, and `orcl` and `test1` on `host01`) are pre-created and the instances are automatically started. Not all databases will be visible in Cloud Control until later in the exercises.
    *   One database, `test2` on `host01`, is pre-created but it is not running.
    *   The appropriate listeners are started, one on each host.
    *   Enterprise Manager Cloud Control is automatically started. BI Publisher is configured but not yet started.

    Navigate to the `em13c` session.

2. Your environment is configured so that the `em13rep` database instance is automatically started. This database is your Enterprise Manager Cloud Control repository.

    a. Check if the database has been started.

    ```
    [oracle@em13c ~]$ ps -ef | grep pmon
    oracle    11386     1  0 19:06 ?        00:00:00 ora_pmon_em13rep
    oracle    23733  4144  0 21:51 pts/0    00:00:00 grep pmon
    ```

    Note that your process IDs and times may not exactly match the numbers above.

    The Process Monitor (PMON) output shows you the database name (`em13rep`) that you use to set environment variables.

    b. Check if the associated listener has been started.

    ```
    [oracle@em13c ~]$ ps -ef | grep lsnr
    oracle    10825     1  0 18:59 ?        00:00:02
    /u01/app/oracle/product/12.1.0/dbhome_1/bin/tnslsnr LISTENER -inherit
    ```

c. An Oracle database instance is referred to by an Oracle System Identifier or SID. Oracle provides a script called `oraenv` that can be used to change the environmental variables $ORACLE_HOME, $ORACLE_SID, and $PATH and allow a user to connect to a given database instance. `oraenv` can be used to switch between different SIDs installed in the same environment. Set the environment variables for the repository database instance.

```
[oracle@em13c ~]$ . oraenv
ORACLE_SID = [oracle] ? em13rep
The Oracle base has been set to /u01/app/oracle
```

d. Log in to the database to confirm that it is available, run a simple SQL query, and then exit from SQL*Plus.

```
[oracle@em13c ~]$ sqlplus / as sysdba
SQL*Plus: Release 12.1.0.2.0 Production on Wed <date>
Copyright (c) 1982, 2014, Oracle.  All rights reserved.
Connected to:
Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production
With the Partitioning, OLAP, Advanced Analytics and Real Application Testing options
SQL>
```

```
SQL> select name, log_mode from v$database;
NAME      LOG_MODE
--------- ------------
EM13REP   NOARCHIVELOG
SQL>
```

The `V$DATABASE` view, used here as an example, stores the currently active database information. The `LOG_MODE` parameter value of `NOARCHIVELOG` (default) indicates that online redo logs will be overwritten without being archived first. This implies that your database is protected from instance failure but not from media failure.

```
SQL> exit
```

3. Explore the basic commands for controlling Cloud Control and start your test environment. The Oracle Management Service (OMS) and the agents are configured to start automatically at operating system startup.

a. Your environment has a number of custom, predefined shell scripts that simplify the task of setting up your environment. These are available only in your environment; they are not available by default with Cloud Control. For example, `myomsenv.sh` sets the correct environment variables for the OMS. View this script now:

```
oracle@em13c ~]$ cat myomsenv.sh
#!/usr/bin
export ORACLE_HOME=/u01/app/oracle/middleware
export PATH=$ORACLE_HOME/bin:/usr/bin:$PATH
```

b. Check the status of the OMS.

```
[oracle@em13c ~]$ . myomsenv.sh
[oracle@em13c ~]$ emctl status oms
Oracle Enterprise Manager Cloud Control 13c Release 2
Copyright (c) 1996, 2016 Oracle Corporation.  All rights reserved.
WebTier is Up
Oracle Management Server is Up
JVMD Engine is Up
BI Publisher Server is Down
```

c. Retrieve a detailed status of your OMS. Note that the sysman password is required.

```
[oracle@em13c ~]$ emctl status oms -details
Oracle Enterprise Manager Cloud Control 13c Release 2
Copyright (c) 1996, 2016 Oracle Corporation.  All rights reserved.
Enter Enterprise Manager Root (SYSMAN) Password :  <enter password>
Console Server Host       : emcc.example.com
HTTP Console Port         : 7788
HTTPS Console Port        : 7802
HTTP Upload Port          : 4889
HTTPS Upload Port         : 4903
EM Instance Home          : /u01/app/oracle/gc_inst/em/EMGC_OMS1
OMS Log Directory Location : /u01/app/oracle/gc_inst/em/EMGC_OMS1/sysman/log
OMS is not configured with SLB or virtual hostname
Agent Upload is locked.
OMS Console is locked.
Active CA ID: 1
Console URL: https://emcc.example.com:7802/em
Upload URL: https://emcc.example.com:4903/empbs/upload

WLS Domain Information
Domain Name          : GCDomain
Admin Server Host    : emcc.example.com
Admin Server HTTPS Port: 7102
Admin Server is RUNNING

Oracle Management Server Information
Managed Server Instance Name: EMGC_OMS1
Oracle Management Server Instance Host: emcc.example.com
WebTier is Up
Oracle Management Server is Up
JVMD Engine is Up

BI Publisher Server Information
BI Publisher Managed Server Name: BIP
BI Publisher Server is Down

BI Publisher HTTP Managed Server Port   : 9701
BI Publisher HTTPS Managed Server Port  : 9803
BI Publisher HTTP OHS Port              : 9788
BI Publisher HTTPS OHS Port             : 9851
BI Publisher is locked.
BI Publisher Server named 'BIP' is configured to run at URL:
https://emcc.example.com:9851/xmlpserver
BI Publisher Server Logs: /u01/app/oracle/gc_inst/user_projects/domains/GCDomain/servers/BIP/logs/
BI Publisher Log       :
/u01/app/oracle/gc_inst/user_projects/domains/GCDomain/servers/BIP/logs/bipublisher/bipublisher.log
```

.

d. Check the status of the agent. The agent installed on the same host as the OMS is called the Central Agent. The `myagentenv.sh` script sets the correct environment variable for the agent.

```
[oracle@em13c ~]$  . myagentenv.sh
[oracle@em13c ~]$  emctl status agent
Oracle Enterprise Manager Cloud Control 13c Release 2
Copyright (c) 1996, 2016 Oracle Corporation.  All rights reserved.
---------------------------------------------------------------
Agent Version         : 13.1.0.0.0
OMS Version           : 13.1.0.0.0
Protocol Version      : 12.1.0.1.0
Agent Home            : /u01/app/oracle/agent/agent_inst
Agent Log Directory   : /u01/app/oracle/agent/agent_inst/sysman/log
Agent Binaries        : /u01/app/oracle/agent/agent_13.1.0.0.0
Core JAR Location     : /u01/app/oracle/agent/agent_13.1.0.0.0/jlib
Agent Process ID      : 26594
Parent Process ID     : 26526
Agent URL             : https://emcc.example.com:3872/emd/main/
Local Agent URL in NAT : https://emcc.example.com:3872/emd/main/
Repository URL        : https://emcc.example.com:4903/empbs/upload
Started at            : <date>
Started by user       : oracle
Operating System      : Linux version 3.8.13-26.2.1.el6uek.x86_64 (amd64)
Number of Targets     : 32
Last Reload           : (none)
Last successful upload                       : <date>
Last attempted upload                        : <date>
Total Megabytes of XML files uploaded so far : 1.76
Number of XML files pending upload           : 0
Size of XML files pending upload(MB)         : 0
Available disk space on upload filesystem    : 16.25%
Collection Status                            : Collections enabled
Heartbeat Status                             : Ok
Last attempted heartbeat to OMS              : <date>
Last successful heartbeat to OMS             : <date>
Next scheduled heartbeat to OMS              : <date>
---------------------------------------------------------------
Agent is Running and Ready
```

4. Explore the `host01` host. Navigate to your `host01` session.

5. Your training environment is configured so that the `orcl` and `test1` database instances, their listener, and a Cloud Control agent are automatically started.

a. Check if the database and the associated listener have been created and started.

```
[oracle@host01 ~]$ ps -ef | grep pmon
oracle    3765     1  0 15:05 ?        00:00:02 ora_pmon_orcl
oracle    4318     1  0 15:06 ?        00:00:02 ora_pmon_test1
oracle   30801 18366  0 23:50 pts/0    00:00:00 grep pmon
[oracle@host01 ~]$ ps -ef | grep lsnr
oracle    3663     1  0 15:05 ?        00:00:08
/u01/app/oracle/product/12.1.0/dbhome_1/bin/tnslsnr LISTENER -inherit
oracle   30821 18366  0 23:51 pts/0    00:00:00 grep lsnr
```

b. Set the environment variables for the database instance `orcl`.

```
[oracle@host01 ~]$  . oraenv
ORACLE_SID = [oracle] ? orcl
The Oracle base has been set to /u01/app/oracle
```

c. Log in to the `orcl` database to confirm that it is available, run a simple SQL query, and then exit from SQL*Plus.

```
[oracle@host01 ~]$  sqlplus / as sysdba
SQL> select name, log_mode from v$database;
NAME      LOG_MODE
--------- ------------
ORCL      NOARCHIVELOG
SQL> exit
```

d. Check the status of the agent.

```
[oracle@host01 ~]$ . myagentenv.sh
[oracle@host01 ~]$ emctl status agent
Oracle Enterprise Manager Cloud Control 13c Release 1
[…]
Agent is Running and Ready
```

For your reference, here are the basic control commands for OMS and the agent:

To stop the OMS, including the Administration Server, HTTP Server, and Node Manager, use the following command:

```
emctl stop oms –all
```

Note that the `emctl stop oms` command will stop only the management service.

To start the OMS:

```
emctl start oms
```

To stop and start your management agent:

```
emctl stop agent
emctl start agent
```

Practices for Lesson 1: Introduction

Practices for Lesson 2: Cloud Control Core Concepts

Overview

Practices for Lesson 2: Overview

Practices Overview

In these practices, you act as an Enterprise Manager Super Administrator. You access Oracle Enterprise Manager Cloud Control 13*c* as the `emadmin` user. **Summary** is your home page.

Your instructor might suggest a time period for these tasks. Answering questions is optional. Try to complete the task within the suggested time period.

Lab 2-1: Accessing Enterprise Manager Cloud Control

Overview

In this Lab, you access Oracle Enterprise Manager Cloud Control 13*c* as the `emadmin`
Super Administrator.

Assumptions

- You are logged in to your classroom PC.
- Your instructor has given you a demonstration of the Cloud Control Console general
  navigation, or you have watched the "Console Overview and Customization" OLL
  demonstration, or have the equivalent navigation knowledge from a prerequisite
  course.

Tasks

1. Connect to the `host01` host as the `oracle` user.
2. Start a **terminal** session by double-clicking the Terminal icon.
3. Bring up **Firefox** for accessing the Enterprise Manager Cloud Control console.

   ```
   [oracle@host01 ~]$ firefox &
   ```

   Your browser's home page is set up as the Enterprise Manager Cloud Control login page
   (same as the **EMCC** bookmark on the Firefox toolbar). The location is of the format:
   https://<em_server_hostname>.<domain>:<port>/em. In your case, this location is
   https://emcc.example.com:7802/em.

   a. Add an exception to your browser for the OMS SSL certificate. This is required
      because your environment is installed with the default out-of-the-box certificate that the
      browser considers to be invalid. In a production environment, you would secure the
      Cloud Control Console with a certificate from a trusted source.

      1) Click **Advanced** on the "Your connection is not secure" page.
      2) Click **Add Exception** beneath the information about the invalid security certificate
         to display the Add Security Exception dialog box.
      3) After a few seconds, the **Confirm Security Exception** button will be enabled.
         Click **Confirm Security Exception** and leave Permanently Store this Exception
         selected.
      4) The Enterprise Manager Cloud Control 13*c* login page will now be displayed.

4. Best practices for using Cloud Control suggest that you create a new EM Administrator and
   reserve the use of SYSMAN (default EM Administrator and repository owner) only for tasks
   that are SYSMAN-specific. In your environment, a new EM Administrator, `emadmin`, with
   Super Administrator privileges, has already been created.

   Enter `emadmin` in the **User Name** field and the password for the `emadmin` user in the
   Password field. Then click **Login**.

The first time a new user logs in to Enterprise Manager, the "Welcome to Enterprise Manager Cloud Control" page appears and allows the user to select the Enterprise Manager Home Page. The choice of pages include, among others:

- Welcome Page
- All Targets
- Sitemap
- Summary
- Databases
- Incidents
- SOA
- Middleware
- Composite Application
- Services

Each choice has a Preview and a Select As My Home button. The emadmin user has the **Enterprise Summary** as the default page.

The default page has global menus with the following choices: **Enterprise**, **Targets**, **Favorites**, **History**, **Setup**, and **Search** (marked by the magnifier icon). Each of the menu items has drop-down menus with further choices.

Note that adjusting the browser font size controls the size of the icons and whether the menu titles are shown or not. Decrease the font size (Ctrl-dash) to see the menu titles.

5. *Question:* How can you change your home selection after the initial setup?

Answer: Navigate to a new page of interest, and click **EMADMIN > Set Current Page as My Home**.

6. EM CLI is the Cloud Control command-line interface used to perform some common administrative tasks, especially tasks that need to be performed in bulk against a large number of targets. EM CLI is installed by default with the Oracle Management Service (OMS). In your environment, EM CLI is installed on the em13c host.

a. Navigate to your host em13c session, bring up a terminal session, and run the following commands to set up your EM CLI environment (same as the OMS environment), and then find out the status of the EM command-line interface on your OMS host:

```
[oracle@em13c ~]$ . myomsenv.sh
[oracle@em13c ~]$ emcli status
Oracle Enterprise Manager 13c Release 2 EM CLI.
Copyright (c) 1996, 2016 Oracle Corporation and/or its affiliates. All rights reserved.


Instance Home        : /home/oracle/.emcli
Verb Jars Home       : /u01/app/oracle/middleware/bin/bindings/13.2.0.0.0/.emcli
Status               : Configured
EM CLI Home          : /u01/app/oracle/middleware/bin
EM CLI Version       : 13.2.0.0.0
Java Home            : /u01/app/oracle/middleware/oracle_common/jdk/jre
Java Version         : 1.7.0_111
Log file             : /home/oracle/.emcli/.emcli.log
```

```
Log level             : SEVERE
EM URL                : https://emcc.example.com:7802/em :
EM user               emadmin
Auto login              : false
Trust all certificates : false
```

EM CLI is installed and minimally configured out-of-the-box with the first OMS installed. Only basic operational commands can be performed.

b. To fully configure EM CLI and install additional verbs (commands) in Standard as well as Interactive/Script modes, you must complete a *setup* step. For help on the setup, run the following command:

```
[oracle@em13c ~]$  emcli help setup
```

c. The setup step is required every time you connect to a new OMS. At a minimum, the required parameters for setup are as follows. Note that you are connecting as the Super Administrator emadmin, but it can be any valid EM user or administrator.

```
[oracle@em13c ~]$

emcli setup -url=https://emcc.example.com:7802/em -username=emadmin  Oracle
Enterprise Manager 13c Release 2 EM CLI.
Copyright (c) 1996, 2016 Oracle Corporation and/or its affiliates. All rights reserved.


Enter password  <emadmin password>


Warning: This certificate has not been identified as trusted in the local trust store
-------------------------------------
[…]
-------------------------------------
Do you trust the certificate chain? [yes/no] yes
Emcli setup successful
```

d. EM CLI in Standard mode can be used to quickly retrieve system configuration information (for example, to find all the plug-ins installed with the OMS or a particular management agent, and so on). Here is an example of EM CLI being used to send out a broadcast message to all users logged in. Do not forget to **log out**.

```
[oracle@em13c ~]$ emcli send_system_broadcast -
messageType="INFO" -toOption="ALL" -message="Cloud Control will
shutdown in 2 hours to apply a critical patch"
Successfully requested to send System Broadcast to users.


[oracle@em13c ~]$ emcli logout
Logout successful
```

e. Return to your host01 browser session and review the message received in Cloud Control. Click **Close** in the message window.

Lab 2-2: Monitoring and Managing Cloud Control

Overview

In this Lab, you explore your Cloud Control setup and review the configuration of the Cloud Control components (OMS) and the management repository database (OMR) by using the Cloud Control console.

Assumptions

You are logged in to Enterprise Manager Cloud Control as the `emadmin` user.

Tasks

Navigate to the **Enterprise Summary** page by selecting **Enterprise > Summary**.

Your Enterprise Summary page values depend on how long your environment has been running, its performance during this time, and other factors.

1. How many targets are being monitored with status? *(35)*
2. What is their status? *(26 are up)*
3. Do you have any open incidents? *(May vary on each environment)*
4. Do you have any open problems? *(May vary on each environment)*
5. What is the platform for your hosts? Hint: Select the option to show Hosts under Inventory and Usage. *(Oracle Linux Server release 6.5)*
6. Are you set up to receive patch recommendations? *(No)*
7. Review the overall status of Cloud Control.
   a. Navigate to **Setup > Manage Cloud Control > Health Overview**.
   b. Review your Management Services and Repository page to see the name of the host (top-right corner) and the main sections.
   c. Is there a job backlog? If yes, what is the estimated time to clear the job backlog?
8. Click the "**i**" quick information icon next to the **Management Services and Repository** page title.
   a. What is the version of the OMS and the Repository? *(13.2.0.0.0)*
   b. When you finish reviewing the information, click the "x" icon to close the pop-up page.
9. Drill down into **Management Service in Use**
   `emcc.example.com:4889_Management_Service`
   a. Which one is the monitoring agent? (*emcc.example.com:3872*)
   b. What is the Upload port? (*4889*)
10. Monitor the Repository Operations. Navigate to **Setup > Manage Cloud Control > Repository**.
    a. What is the name of the instance that holds the OMR? Hint: Look under the Initialization Parameter Compliance for Instance. *(em13rep)*
    b. Are there any noncompliant initialization parameters? (*Yes)*
    c. What is the space used? *(The number varies on each system)*

     d.   Is your repository volume growing or shrinking? (*Look for Trend*)

     e.   Navigate to the **Schema** tab and:

- View Tablespace Growth Rate
- View Retention and Purge Policies

11. Navigate to **Setup > Security > Security Console**.

     a.   Review the **Overview** tab. This page details Security-related information about your system. The left navigation links take you directly to a specific security area.

     b.   Click the **Fine-grained Access Control** link on the left-hand side. Navigate to the **Administrators** link. Note the two administrators listed. You are logged in as EMADMIN. SYSMAN is the owner of the repository schema.

     c.   Click the **Best Practices Analysis** link on the left-hand side. Review the findings for your system. There are best practices to follow in a production environment and you will apply some of them in the upcoming exercises.

12. To view the log files of various targets, navigate to **Enterprise > Monitoring > Logs**.

     a.   Click **Search** and then **Add** to access the **Select Targets** dialog box.

     b.   Sort the targets by Target Type, highlight the **Oracle HTTP Server** target, and click **Select**.

     c.   Click the icon in the **Target Log Files** column to view all the logs for this target.

     d.   Highlight the `access_log` and click the **View Log File** tab to view the content of this log. Note the various log entries that can be sorted by **Time**, **Message Type, Message ID**, or **Message name**.

Lab 2-3: Monitoring the Cloud Control Host

Overview

In this Lab, you familiarize yourself with the more common tasks performed with Cloud Control, such as monitoring your Cloud Control system hosts. You take a look at the type of operations you can perform against a target of type host, in this case the host that holds your repository database.

Assumptions

You are logged in to Enterprise Manager Cloud Control as the `emadmin` user, from a browser running on the host `host01`.

Tasks
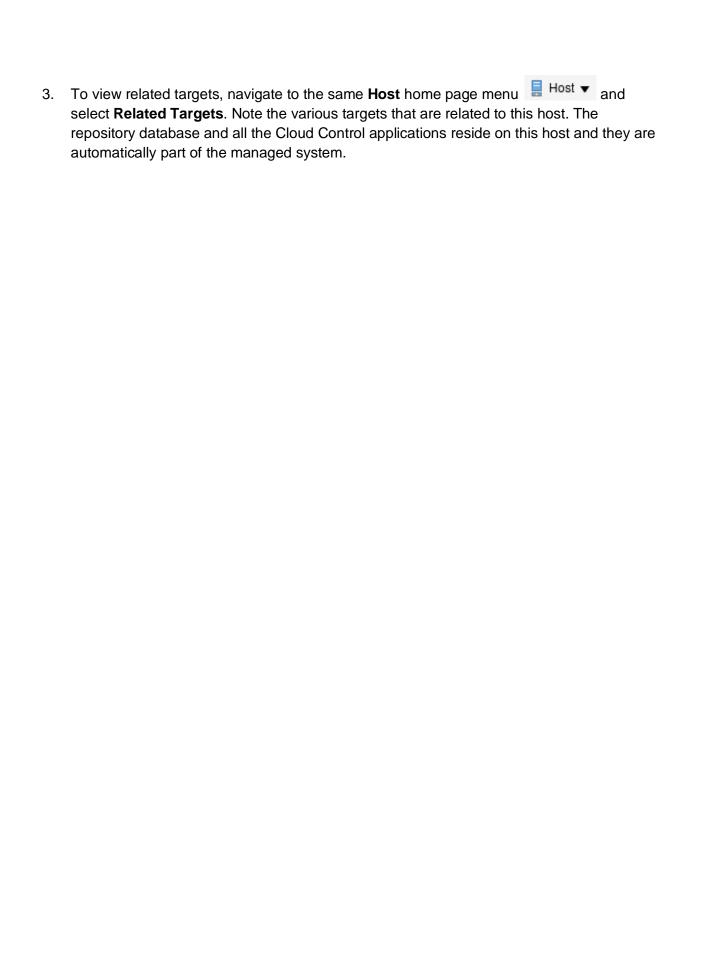
1. In your `host01` session browser, navigate to **Targets > Hosts**. Note all the discovered hosts in your system (there are two of them). As you learned, these hosts are now *managed* hosts that have agents running on them.

   To view all the information about `em13c`, click the `emcc.example.com` link.

   a. The top of a host home page displays a series of **dashlets** on a **dashboard** that provide the top statistics for that host. Review the dashlet information: **Linux version**, **Open Incidents**, and **CPU and Memory Utilization**.

   b. To view the second page of the Dashboard, click the horizontal line segment in the center of the page, right under the dashboard. Review the **OS Service State** and **configuration changes**.

   c. Explore the right-hand side navigation tabs and view the details about your host: its operating system statistics, storage, network interfaces, and so on.

      – Click the **CPU** tab .

      – Click the **Host Memory** tab .

      – Click the **Storage** tab .

      – Click the **Network Connectivity** tab .

      – Click the **Host Processes** tab .

2. Navigate to the top-left main menu for this host, marked by , and click the down arrow to display all the monitoring and management options. Note in particular that for a Linux host system **Administration**, you must have YAST installed. This is not set up in your lab environment.

3. To view related targets, navigate to the same **Host** home page menu and select **Related Targets**. Note the various targets that are related to this host. The repository database and all the Cloud Control applications reside on this host and they are automatically part of the managed system.

Practices for Lesson 3: Organizing Targets

Overview

Practices for Lesson 3: Overview

Practices Overview

In these practices, you review your managed targets and group them into an Administrative group.

Lab 3-1: Organizing Your Targets: Administrative Groups

Overview
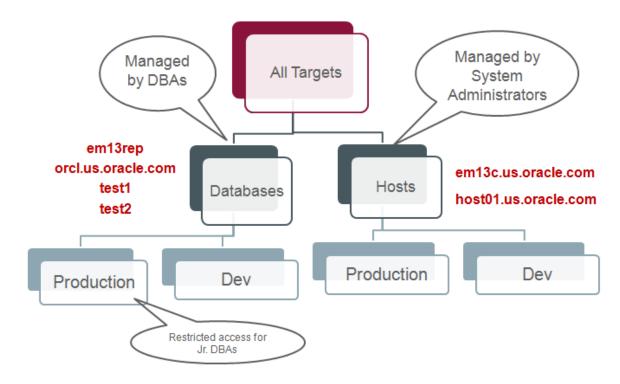
In this Lab, you assign target properties, create an Administrative group, which is by definition a privilege propagating group, and then explore the group.

Assumptions

You are logged in to Cloud Control as the `emadmin` user.

Tasks

1. In this Lab, assume that you have decided on the following grouping of your targets:

    *   You have two hosts, `emcc.example.com` and `host01.us.oracle.com`. They are both *Production* hosts.
    *   You have three databases initially and one discovered later:
        *   Two *Production* databases named `orcl.us.oracle.com` (a pluggable database, by default showing the Container database and a pluggable database) and `em13rep` (the OMR, discovered later)
        *   Two *Development* databases used for testing, named `test1` and `test2`

Navigate to **Targets** > **Hosts** and note the two hosts you have in your environment. Edit their properties to reflect their *Lifecycle* status:

a. Drill down into the host `emcc.example.com`.

b. Navigate to **Host > Target Setup > Properties** and click **Edit**.

c. Under **Lifecycle Status**, select **Production** and then click **OK**.

d. Navigate back to **Targets** > **Hosts** and repeat the steps a-c for host `host01.us.oracle.com`, specifying its **Lifecycle Status** as **Production.**

These were examples of how to change the Lifecycle Status from the GUI interface.

2. Target properties can also be modified in bulk for a large number of targets using EM CLI's `set_target_property_value` verb. These properties can also be assigned at discovery time. Use the EM CLI interface to set the next few properties: `orcl.us.oracle.com` as a **Production** database and `test1`/`test2` as **Development** databases**.**

a. Return to your `em13c` session or reconnect to it if you have exited. Run the script to set up your EM CLI environment (same as the OMS environment).

```
[oracle@em13c ~]$ . myomsenv.sh
```

b. Connect to EM CLI.

```
[oracle@em13c ~]$ emcli login -username=emadmin
Enter password : <emadmin password>
Login successful
```

c. Set the Lifecycle property for a single target, the `orcl.us.oracle.com` database, as **Production**.

```
[oracle@em13c ~]$ emcli set_target_property_value -
property_records="orcl.us.oracle.com:oracle_database:LifeCycle
Status:Production"
Properties updated successfully
```

d. Note that you can set all properties from a single command. For example, set the Lifecycle properties for both the `test1` and `test2` databases as **Development**.

```
[oracle@em13c ~]$ emcli set_target_property_value -
property_records="test1:oracle_database:LifeCycle
Status:Development;test2:oracle_database:LifeCycle
Status:Development"
Properties updated successfully
```

```
[oracle@em13c ~]$ emcli logout
Logout successful
```

3. Next, create **groups** for your targets based on the diagram given earlier. You will use Administration groups because of their unique properties discussed during your lecture session. **Administrative groups** are privilege propagating by definition, so that privileges on the group are propagated to its members. These groups are used for automating the application of management settings to targets.

Back in your browser session, on `host01`, navigate to **Setup > Add Target** and select **Administration Groups**. Review the *Getting Started With Administration Groups and Template Collections* information for a preview of this exercise and upcoming lessons.

4. Navigate to the **Hierarchy** tab and note the elements to set up here: the *levels* and *nodes*.

   a. Under **Hierarchy Levels**, click **Add** and select **Target Type** as the first level of the hierarchy.

   You will receive a warning that only ten property values can be used as criteria for determining eligibility for this hierarchy level. This is because there are many more than ten target types, and each type is a value of the Target Type property. In this way, Target Type is a special property in that it has predefined values.

   Click **OK** on the warning dialog box to proceed to the next step where you will address the issue that raised the warning.

   b. To simplify our group, under **Hierarchy Nodes**, select only the target types *Host* and

   Database Instance. Click the **Add** button under **Hierarchy Nodes**, click ⟪ to remove all items from the selected values, and then select `Host` and `Database Instance` and move them to the selected values. Click **OK**. Note the selected `Host` and `Database Instance` under the target types.

   c. Under **Hierarchy Levels**, click **Add** again and select **Lifecycle Status** as the second level in your hierarchy. Note that Lifecycle Status is also a special property that has predefined values.

   d. The only two status values of Lifecycle Status you will be using in this Lab are *Production* and *Development*. Delete all the others by highlighting them in the **Hierarchy Nodes: Lifecycle Status** table and selecting **Remove**.

5. Click **Create** in the top-right corner to define the hierarchy and bring the nodes into an Administration Group. Note that switching to other tabs before you click Create will cause all changes to be lost.

   a. Click **Continue** and then **OK** to submit a job to create this group.

   b. View the job details by clicking the **View Job Details** link on the top right.

   c. Return to **Setup > Add Target > Administration Groups** and view your newly created hierarchy. The **Associations** tab provides a graphical view of the hierarchy.

   d. The new group becomes a managed entity in Cloud Control. Navigate to **Targets > Groups** and evaluate the group you just created: **ADMGRP0**.

   e. Expand the **ADMGRP0** group to see the two subgroups, each with two subgroups of their own.

   f. Click the name of the group, the link **ADMGRP0**, and note all the rolled up information about your group. Select the **Dashboard** tab for more information. Note that the dashboard is automatically updated with the latest status on the group members. In addition, the dashboard can be customized.

   Note that only *one Administration* group can be defined in your environment in order to avoid conflicts in the monitoring definitions.

Lab 3-2: Organizing Your Targets: Non-Privilege-Propagating Groups

Overview

In this Lab, you create a group that does *not* propagate privileges to members when new targets are added. You will make use of this group later in the exercises.

Assumptions

You are logged in to Enterprise Manager Cloud Control as the emadmin user.

Tasks

1. Create another group you will use later in your exercises. Navigate to **Targets** (global menu) **> Groups**.
2. Click **Create > Group** and enter the **Name** as NPPG_TEST_DB.
3. Leave Privilege Propagation **deselected**.
4. Under **Members**, click **Add,** search by **Target Type** Database Instance, and **select** test1.
5. Leave the default for the **Timezone** and click **OK** to create this group. This group has one database member.
6. Click **OK** in the information dialog box that the group has been created. Note that your new group is listed under **Targets** > **Groups**.

Lab 3-3: Discovering Additional Targets

Overview

In this Lab, as a Super Administrator, you discover additional targets and note the groups they get assigned to.

Assumptions

You are logged in to Enterprise Manager Cloud Control as the `emadmin` user.

Tasks

1. Discover an additional database that will automatically be added to a group you created in the previous exercise. It is recommended that repository databases are managed targets in Cloud Control, so you will add the repository database to your managed system.

   Databases are automatically discovered on a host that has an agent running on it. In your setup, the OMS and the repository reside on the same host and an agent was automatically installed when the OMS was installed.

   a. Navigate to **Setup > Add Target > Auto Discovery Results** and click the **Targets on Hosts** tab to view the targets discovered on the repository host.

   b. Your Cloud Control system automatically discovered new targets on the managed hosts. Select the `em13rep` database instance and click **Promote.**

   c. In the Databases table, select the `em13rep` instance and enter the **Monitor Password** for user `dbsnmp` (refer to the *Course Lab Environment: Security Credentials* document), Role **Normal** (default).

   d. Click "**Test Connection**" to test the monitoring connection and look for the **Information** dialog box: "The connection test was successful." Click **OK** to dismiss the dialog box.

   Note: `dbsnmp` is a predefined Oracle database account used by Cloud Control, specifically the management agent, for target discovery and monitoring those Oracle databases. This user is referred to as the database monitoring credential. By default, the `dbsnmp` account is locked in most databases. In your environment, `dbsnmp` has been unlocked.

   e. Check that the database listener `LISTENER_emcc.example.com` is also listed in the lower **Listeners** table.

   f. Next, click the **Set Global Target Properties** tab to set target properties that will aid in placing them in the correct groups**.** A database is by definition a Database Instance target type. In addition, for your Lab, the **Lifecycle Status** value is also a defined hierarchy. Select **Production** and then click **OK.**

   g. Check that both targets, `em13rep` and `LISTENER_emcc.example.com`, are still selected and click **Next**. Review the targets that are about to be promoted. Make sure that *both* a database system and a listener are being promoted at this time.

   h. Click **Save** to promote the discovered targets to monitored targets. You will be presented with a dialog box showing that the promotion is being processed, and finally a **Confirmation** dialog box showing the message "`The following targets have been saved…`" Dismiss the confirmation dialog box by clicking **Close**.

i. Navigate to **Targets > Databases** and view by **Search List** (top-left option button View ○ Database Load Map ⦿ Search List). The repository database `em13rep` should now be listed under the monitored databases. Refresh the page until the status of the database shows **Up** (green up arrow).

j. Do you think this new database is part of the Administration Group you created? Why? Check by clicking the `em13rep` link. Under the **Oracle Database** menu, click **Target Information** and note the **Member of** field. At promotion time, you marked this database as Lifecycle status Production. Therefore, this database automatically was added to the `DI-Prod-Grp`.

k. You can now review the `DI-Prod-Grp` again to see all its members. Click the `DI-Prod-Grp` link. The newest member is the new Production database `em13rep`. Its availability status may be still pending.

Practices for Lesson 4: Oracle Cloud in Your IT Ecosystem

Overview

Practices for Lesson 4

There are no practices for this lesson.

Practices for Lesson 5: Cloud Control Access

Overview

Practices for Lesson 5: Overview

Practices Overview

In these practices, you create roles for different administrators, create and assign named credentials for your targets, and then perform various administrative tasks as these administrators.

Lab 5-1: Creating Roles and Administrators

Overview

In this Lab, you create typical administrator roles to illustrate how various privileges can map to various job descriptions.

Assumptions

You are logged in to Enterprise Manager Cloud Control as the `emadmin` user.

Tasks

1. Create the first Role for a DBA type of job. DBAs typically have full access to databases and they also require some privileges to the operating system for running certain jobs, writing files, and so on.

   a. Navigate to **Setup > Security > Roles** to create a role that applies to all targets and click **Create**.

   b. In the name field, enter `DBA_ROLE` and click **Next**.

   c. Note the predefined roles available. It is recommended that you make use of these roles in Production environments. However, for the purpose of showing the granularity of privileges, skip these roles and click **Next**.

   d. A DBA's job requires access to the OS on the managed targets for running jobs such as a backup database job. In addition, just to keep it simple at this time, assume that you would like the DBA to be able to monitor host targets as well. Under **Privileges Applicable to all targets**, select `Manage Any Target Metric` and `Execute Command Anywhere`.

   e. At the bottom of the page, under **Target Privileges**, click **Add**.

   f. Select the **Target Type** as **Database Instance** and click **Select All** to select all databases found. Then, click **Select**.

   g. Back in the **Target Privileges** table, click **Grant to All**, select **Full**, and click **Continue**.

   h. Back under **Target Privileges**, click **Add**. Select the **Target Type** as `Group` to sort your list.

   i. Select the group named `Host-Grp` and click **Select**. Note that under **Manage Target Privilege Grants**, the `View` privilege is given to the `Host-Grp` by default.

   j. Edit the `View` privilege by clicking its pencil Edit icon and select `Manage Template Collection Operations` as well. (*Hint*: This privilege is the last one on the list; look at the last page.) Click **Continue**.

   k. Click **Next** to proceed to the **EM Resource Privileges** page. A DBA will also need access to the Job System for submitting jobs such as backups. Therefore, in the **Job System** row, click the **Edit** pencil icon in the **Manage Privilege Grants** column and select **Create** to allow a DBA to create a job. Click **Continue**.

   l. Click **Review** and note the privileges you are about to add for this role: `Manage Any Target Metric` and `Execute Command Anywhere` on all targets, `Full` privileges on Databases, `View` and `Manage Template Collection Operations` privileges on all the hosts in the `Host-Grp` group, and `Create Job System resource privilege`. Click **Finish**.

2. Certain jobs may require restricted access to databases. This type of job may be performed by a Junior DBA. Create a new role that maps to this kind of job responsibility.

   a. Navigate to **Setup > Security > Roles** again to create another role that applies to all targets. Click **Create**.

   b. In the name field, enter `JR_DBA_ROLE` and click **Next**.

   c. Skip the predefined roles and click **Next**.

   d. At the bottom of the page, under **Target Privileges**, click **Add**.

   e. You want this DBA to perform various tasks on databases from two of your groups, but have limited access on the *Production* databases. Select the **Target Type** as **Group**, select both the `DI-Prod-Grp` and `NPPG_TEST_DB` groups, and then click **Select**. Note the default `View` privileges given for these groups.

   f. You want the Jr. DBA to have full access to the nonprivilege propagating group `NPPG_TEST_DB`. In the **Target privileges** table, **select** the group `NPPG_TEST_DB` and click **Grant to Selected**.

   g. Select the `Full` privileges and click **Continue**. Note that for the Production databases, a Junior DBA still only has `View` privileges.

   h. Click **Review**. Note the `Full` privileges to the nonprivilege propagating group `NPPG_TEST_DB`, `View` privileges to the Production database group `DI-Prod-Grp`, and no other target privileges. Then click **Finish**.

3. Roles can be granted to any new user/administrator created in Cloud Control. This way, if any of the privileges need to change, a Super Administrator will only need to edit the Role. Create the `DBA1` user.

   a. Navigate to **Setup > Security > Administrators**.

   b. Click **Create** and enter the following values: `DBA1` as the **Name**, and as **Password**, your choice of password for user `DBA1`. *Make a note of this password! You will need it later.* Note that the password cannot be same as the username. The password must be at least 8 characters long and it must have at least one letter, digit, and punctuation character.

   c. Select `MGMT_ADMIN_USER_PROFILE` as the Password Profile (the recommended profile for administrators due to the built-in security restrictions) and optionally enter a Description.
   Note that the Super Administrator box is NOT selected. Click **Next**.

   d. On the "Roles" page, select the following roles: `DBA_ROLE`, `EM_USER` (already selected), and `PUBLIC` (already selected). Then click **Next**.

   e. Click **Review** to review your `DBA1` definitions and click **Finish**. You should receive a confirmation that the `DBA1` user was created successfully.

4. Create the `JR_DBA1` user.

   a. Navigate to **Setup > Security > Administrators**.

   b. Click **Create** and enter the following values: `JR_DBA1` as the **Name**, and as **Password**, your choice of password for user `JR_DBA1`. *Make a note of this password! You will need it later.* Note that the password cannot be same as the username. The password must be at least 8 characters long and it must have at least one letter, digit, and punctuation character.

c. Select MGMT_ADMIN_USER_PROFILE as the Password Profile and optionally enter a Description.

Note that the Super Administrator box is NOT selected. Click **Next**.

d. On the "Roles" page, select the following roles: JR_DBA_ROLE, EM_USER (already selected) and PUBLIC (already selected). Then click **Review**.

e. Review your JR_DBA1 definitions and click **Finish**.

f. You should receive a confirmation that the JR_DBA1 user was created successfully.

Lab 5-2: Creating Named and Default Credentials

Overview

Named credentials are a way to share credentials with various users without sharing the passwords. For this exercise, you evaluate the existing Named Credentials and create new ones as needed by your administrators, JR_DBA1 and DBA1.

1. Take a look at the Database Named Credentials and create a Global database credential:
   a. Navigate to **Setup** > **Security** > **Named Credentials**. Note a couple of credentials specific to the test1 database. These are called *target scoped* named credentials, applicable to only that target. For your Lab, you want DBAs to have access to credentials that apply to *all* targets of a specific type. These named credentials are called *Global scoped*. Click **Create**.
   b. Create a named credential for an Oracle database user with SYSDBA privileges. Enter the credential name as SYS_SYSDBA and choose the Authenticating Target Type of **Database Instance**.
   c. Select the **Credential type** of **Database Credentials** and select the scope **Global**.
   d. Enter the Username SYS, the password for SYS as given to you, and role SYSDBA.
   e. This type of credential is typically shared with DBAs who have full access to database targets. Under **Access Control**, click **Add Grant** and then select DBA1 as the grantee.
   f. Click **Test and Save** against the orcl.us.oracle.com database and note the message Credential Operation Successful.
2. You will also want to define a Global Host named credential to be used by your administrators. DBAs who run backup jobs or other OS administrators would be given access to this type of credential.
   a. Navigate back to **Setup > Security > Named Credentials**.
   b. Note the existing Host credential NC_HOST_HOST01 that was created at target (host01) discovery time. Highlight it and note the Scope is Global.
   c. Click **Manage Access**.
   d. Click **Add Grant** and then select DBA1 as the grantee.
   e. Click **Save** and note the message Credential Operation Successful.
3. *Preferred* credentials are set for specific targets for ease of login or for tasks that are automatically run. In your practices, a DBA is also given the responsibility of managing database listeners; therefore, a DBA must have access to OS credentials on the targets where listeners are running. In addition, if the DBA is expected to run automatic listener management jobs, you must set up *preferred* credentials for those targets.
   a. Navigate to **Setup > Security > Preferred Credentials** to set up a preferred credential for a host. Note that named credentials must already be created.
   b. Highlight the Target Type as **Listener** and click **Manage Preferred Credentials**.
   c. From this menu, under the My Preferences tab, you can set your own Default Credentials for all hosts, or you can specify a credential for each of your hosts. In the section **Target Preferred Credentials**, highlight the row LISTENER_host01.us.oracle.com Host Credential and then click **Set**.

Make sure you are setting these credentials for the *host01* listener. You will use these later!

d. Select NC_HOST_HOST01 and click **Test and Save**. Acknowledge the successful message at the top.

Note also that this is the menu where you can also set *Global Preferences*, preferred credentials that apply to all targets of a certain type. You will not perform this task in this exercise.

Lab 5-3: Performing DBA Role Tasks: View Host Targets, Set Backup and Recovery Parameters, and Back Up a Tablespace

Overview

In this Lab, you review the tasks available to an administrator with DBA_ROLE and perform a database instance backup operation to confirm that the user indeed has the privileges expected.

It is important to remember that a backup database task is a critical operation for a database instance hosting a repository. However, if the repository database is shut down, the Cloud Control system will be brought down as well. Therefore, in this Lab, you perform the backup tasks on a nonrepository database, namely the orcl.example.com database.

Assumptions

You have created the DBA1 user successfully.

Tasks

1. Log out of the emadmin session if you are already logged in.

2. Log in to Enterprise Manager Cloud Control as the DBA1 user with the password you have chosen. Accept the defaults with **Save and Continue** and select a Home page option button (the Summary page is a good option).

3. First, navigate to **Targets > All Targets** and note all the targets that you have access to. What groups do you have access to? In particular, explore the Host targets. Click Host-Grp. Do you have access to view all the monitoring data? Why? (*The View privileges to the Host-Grp group propagate to the group members because an Administration group is by definition a privilege propagating group.*)

4. Can you perform any administration tasks? Examine, for example, tasks performed from the menu **Group > Members > Target Operations**. Can you see any operations? (*No. Administration tasks, as opposed to View operations, require Operator or Full privileges to targets. Note the message "User DBA1 does not have enough privileges to perform this operation" if you click Run Host Command.*)

5. Next, evaluate the tasks you can perform against database targets. Navigate to **Targets** (global menu) **> Databases** and select the **Search List** view.

    View ○ Database Load Map ◉ Search List

6. Click the database instance link: orcl.us.oracle.com. Note the tasks menus and all the options available to this administrator with a DBA_ROLE: All menus at the top, *Oracle Database, Performance, Availability, Security, Schema*, and *Administration* are enabled. All resources are available because this user has Full access to the database targets.

7. Next, you perform a backup of the database. To perform database administration tasks, your access authorization is checked either explicitly by your providing database login credentials, or implicitly through preferred credentials.

In this training environment, you use the user SYS with the SYSDBA role. However, in a production environment, it is recommended that you create a user and grant the SYSBACKUP privilege in order to perform backup and recovery operations.

Note: Starting with database version 12*c*, the SYSBACKUP user, with the SYSBACKUP privilege, is created automatically at installation time. The SYSBACKUP privilege, a subset of the SYSDBA privileges, includes all the privileges required to back up and recover the database.

First, confirm or change your backup settings. Navigate to **Availability > Backup & Recovery > Backup Settings**.

8. Select the database Named Credential you were given access to, Username SYS, and then click **Login**.

9. Click the **Policy** tab and **select** or confirm the following options:

   a. Under Backup Policy:

      - *Automatically back up the control file and server parameter file (SPFILE) with every backup and database structural change*
      - *Optimize the whole database backup by skipping unchanged files such as read-only and offline data files that have been backed up*

   b. Under Archived Redo Log Deletion Policy:

      Delete archived redo log files after they have been backed up the specified number of times. Backups: 1

   c. Under Host Credentials, confirm the **Named Host Credential** NC_HOST_HOST01 you were granted access to. Note that this is your *operating system* credential.

10. Click the **Device** tab, review the default settings, and then click **Test Disk Backup**. You see a processing indicator, which should be followed by a success message "Disk Backup Test Successful."

11. Click **Apply** to save your backup settings.

12. To change your recovery settings and determine if a restart of the database is needed, navigate to **Availability > Backup & Recovery > Recovery Settings**.

13. A database in ARCHIVELOG mode allows hot backups and recovery to the latest point in time, but you must provide extra space for the archived redo log files. Check **ARCHIVELOG Mode**.

14. In **Fast Recovery Area**, enter the **Fast Recovery Area Size** as **500MB** and then click **Apply**. These changes require a database restart.

15. Accept the named credential as NC_HOST_HOST01, review the entire Confirmation, and then click **Yes**.

16. To restart the database, select NC_HOST_HOST01 as the host named credential and SYS_SYSDBA as the database named credential. Then click **OK**.

17. On the next screen, click **Show SQL**, followed by **Return**.

18. Click **Yes** to restart your database.

A progress indicator is displayed, followed by the success message: `The database has been restarted successfully with the new parameters.`

19. Next, perform a backup of a critical tablespace. To schedule this backup, navigate to **Availability > Backup & Recovery > Schedule Backup**. Ensure that **Tablespaces** is selected under Customized Backup and `NC_HOST_HOST01` is selected as the **Named Credential** for the Host.

   a. Click **Schedule Customized Backup** and click **Add** to add a tablespace.
   b. Select the `USERS` tablespace and click the **Select** button. Click **Next**.
   c. Confirm the following settings, which are chosen to save space in the training environment, and then click **Next**.
      - Full Backup is selected.
      - Back up all archived logs on disk is deselected.
      - Delete obsolete backups is selected.
   d. Accept **Disk** as the destination and click **Next**.
   e. Accept the default **Job Name** and Schedule of **One Time (Immediately),** and click **Next**.
   f. Review your job definition and click **Submit Job**. You must have the `Create Job` privilege to perform this task. You may remember that this privilege was included in your role, `DBA_ROLE`.
   g. You should receive a job submission success message. Click **View Job** and **Refresh** the Execution job page until the job finishes successfully. You may also navigate to **Enterprise > Job > Activity**. Since this is a fast job, you may find it under Succeeded jobs.
   h. On the job execution page, review the backup steps by highlighting the step name, especially **Backup Step**.
   i. Use the global menu **Targets** > **Databases** and navigate to the `orcl.us.oracle.com` home page. Note the status of the Last Backup on the top dashboard.
   j. To review the backup report, click the **Last Backup date** link and review the details. The status should show `Completed`.

Lab 5-4: Performing Tasks as a Junior DBA Administrator: View Targets and Privileges

Overview

In this Lab, you review all the tasks available to an administrator with a JR_DBA_ROLE.

Assumptions

You have created the JR_DBA1 user successfully.

Tasks

1. Log out of the DBA1 session by selecting **Logout of Enterprise Manager and all targets**, if you are still logged in.

2. Log in to Enterprise Manager Cloud Control as the JR_DBA1 user with the password you have chosen. Accept the defaults and select a Home page.

3. Navigate to **Targets** (global menu) **> All Targets** and note all the targets that you have access to. What groups do you have access to? What targets are part of your groups?

4. Click the NPPG_TEST_DB link to access its home page.

   a. Navigate to **Group > Target Setup > Administrator Access** to view the access you have to this group.

   b. What are your Privilege Grants? (*Full for the group NPPG_TEST_DB*)

   c. How were the privileges granted? (*Via the JR_DBA_ROLE*)

   d. Click **OK** to return to the group home page.

   e. Click the **Target Information** icon next to the group name (top left):

   What is the Privilege Propagation Status? (*Disabled*)

5. Click the group member database test1 link to access its home page.

   a. Click the **Administration** menu.

   b. Are any of the submenus enabled? Why not? (*Privileges to the group do NOT propagate to the group members.*)

6. Log out of the JR_DBA1 session.

Practices for Lesson 6: Monitoring

Overview

Practices for Lesson 6: Overview

Practices Overview

Enterprise Manager Cloud Control monitors all its managed targets. This means that metrics are collected for each managed target according to predefined collection schedules. In these practices, you make use of templates to apply monitoring settings.

Lab 6-1: Reviewing the Oracle-Provided Monitoring Templates

Overview

In this Lab, you review the Oracle-provided templates.

- Do all monitored items have the same collection schedule?
- Which setting is used to prevent false alerts due to spikes in metric values?
- Can you edit or delete Oracle-provided templates?

Assumptions

You are logged in to Enterprise Manager Cloud Control as the `dba1` user.

Tasks

1. Log in as `dba1` and navigate to **Enterprise** (global menu) > **Monitoring** > **Monitoring Templates**.

2. If the Oracle-provided templates are not displayed, select "Display Oracle Certified Templates" and then click the search icon.

3. Review the list of Oracle-provided templates, search by **Target Type** `Host`, click the Search icon, and then click the "**Oracle Certified Template for Host targets**" link.

4. On the "**View Monitoring Template: Oracle Certified Template for Host targets**" page, click the **Metric Thresholds** tab.

5. Click **Collapse All** and then expand the "Oracle Certified Template for Host targets" folder. Do all monitored items have the same collection schedule?

   Answer: No

6. Expand the `Load` node and click the **View** icon for **CPU in I/O Wait %**.

7. Review the **View Advanced Settings: CPU in I/O Wait %** page. Which setting is used to prevent false alerts due to spikes in metric values?

   Answer: Number of Occurrences

8. Click **OK** twice to return to the Monitoring Templates.

9. Select any Oracle-provided template that interests you in the Monitoring Templates list, and then try to click **Edit**. Can you edit Oracle-provided templates?

   Answer: No

10. Select another Oracle-provided template and then click Delete. Can you delete Oracle-provided templates?

    Answer: No

11. Take a look at the current values of the metric you looked at in the previous steps. Compare this metric to the other hosts you have in your environment.

    a. Navigate to **Targets** (global menu) > **Hosts** and click the `host01.us.oracle.com` link.

    b. Navigate to **Host** (drop-down list) > **Monitoring** > **CPU Details**. Note that the metrics are grouped by category for ease of management.

c.   One of the top metrics tracked on this page is **CPU in I/O Wait (%)**. Click the link below the center chart. The metric details are displayed.

d.   Are the Warning and Critical threshold values set out-of-the-box? *Answer: No.* Note that you *can* edit the thresholds from this page since you have privileges to do so. However, to ensure consistency in your monitoring, you will change these values later by using a Template Collection.

e.   Click **Compare Targets** at the top right of the chart.

f.   In the **Select Targets** dialog box, select the `emcc.example.com` host, and click **Select**.

g.   The Metric Value History graph now shows values for both hosts. Which host shows a higher wait time? You may want to switch to table view (lower-right corner) if the metrics are too close in value to see on a graph. Click **Close** and return to the **Enterprise Summary** home page by clicking the large Oracle logo, at the top left of the page.

Lab 6-2: Creating a Monitoring Template

Overview

In this Lab, you use the Create Like functionality to create your own monitoring template for a host. You want to track the metric CPU in I/O Wait %. Configure the system to send alerts if the set of thresholds is exceeded. You want alerts to trigger and clear in about 10 minutes.

Assumptions

You are initially logged in to Enterprise Manager Cloud Control as the dba1 user.

Tasks

1. Navigate to **Enterprise > Monitoring > Monitoring Templates**.

2. On the Monitoring Templates page, highlight "**Oracle Certified Template for Host targets**" and try to select **Create Like** from the **Actions** menu. Is the menu enabled? *Answer: No, you do not have privileges to create a monitoring template, only to apply a template you have access to.*

3. Log out of the dba1 session and log in as the emadmin user.

4. Navigate to **Enterprise > Monitoring > Monitoring Templates**.

5. Select "Display Oracle Certified templates," search by **Target Type** Host, and then click the search icon.

6. On the Monitoring Templates page, highlight "**Oracle Certified Template for Host targets**" and select **Create Like** from the **Actions** menu.

7. Enter My Host Template as Name and, optionally, change the description to read: "**This is based upon the Oracle Certified Template for Host targets**."

8. Click the **Metric Thresholds** tab.

9. In the **Load** section, select CPU in I/O Wait % and click the **Edit** (pencil) icon.

10. Before you specify your threshold values, use the **Threshold Suggestion** on the bottom part of the page to adjust (if needed) the values of this Lab. Click **Select Targets** and select the host01.us.oracle.com host.

11. The results are automatically displayed. Assume that based on these results, you decide to set the **Warning Threshold** to **40** and the **Critical Threshold** to **80**.

12. Confirm that **Number of Occurrences** is set to **2**, because the **Collection Schedule** is set to **Every 5 Minutes** and you want alerts to trigger and clear in about 10 minutes. Click **Continue**.

13. You should receive the information message, "The settings have been modified but not saved to the repository. You can make further changes to the settings and click on the OK button to save the data." Click **OK** to save My Host Template in the management repository.

14. Confirm that your newly created monitoring template appears in the list of monitoring templates.

   Hint: Sort by `Owner` and you should see your template listed first, or search for templates with "host" in the name.

15. Compare the template settings with the existing settings on the host `host01.us.oracle.com`.

   a. Select the newly created **My Host Template** and click **Compare Settings**.
   b. On the Compare Monitoring Template My Host Template: General page, click **Add**.
   c. Select the `host01.us.oracle.com` target and click **Select**.
   d. Click **Continue** to initiate the comparison.
   e. Note the red values and the **Diffs** icon. The icons are explained at the bottom of the page. The change in the collection frequency will affect a number of metrics. If you are working with a small window, you might need to scroll to see both your template and the target values.
   f. Click **Cancel** to cancel out of this operation. Note that this step seamlessly allows you to apply a template for the host you just compared with, if you choose so.

Lab 6-3: Applying a Monitoring Template Using a Template Collection

Overview

The recommended way to use the monitoring templates is via the Template Collections applied to an Administration group. This way, any change to the monitoring setting will be automatically applied to the appropriate targets in that Administration group.

Assumptions

You are still logged in to Enterprise Manager Cloud Control as the `emadmin` user, a Super Administrator.

Tasks

1. Create your own Template Collection. `Create Template Collection` is a resource privilege and an administrator needs at least the `VIEW` privilege on the monitoring template to be added to the template collection or the `VIEW` privilege on any monitoring template. In your case, as a Super Administrator, you have the appropriate privileges to create a template collection.

    a. Navigate to **Enterprise** > **Monitoring** > **Template Collections**.
    b. Click **Create** and enter the name as `My Template Collection`.
    c. Click **Add** to add a monitoring template. Note that, by default, the Oracle templates are not listed, so the only template available should be the one you created in a previous Lab. Highlight `My Host Template` and click **Select**.
    d. Click **Save** to save the collection and note the successful confirmation notice. The Template Collection is now saved in the library.

2. The template you created as a Super Administrator is only visible to you and can only be used by those administrators, or roles, you explicitly give access to.

    a. You may edit a role and add access to this specific template collection, OR you may edit the template collection privileges to include access to a particular role or administrator. Choose the latter option by **highlighting** the newly created template and clicking **Privileges**.
    b. Click **Add** and then click the **Search** icon to see all Administrators and Roles.
    c. Select `DBA_ROLE` and click **Select**.
    d. In the privilege column, select the **Full Template Collection** option from the drop-down menu. This will give any administrator with `DBA_ROLE` privileges full access to this collection.
    e. Click **Update** and look for the `Access granted/revoked successfully` confirmation message.

3. Log out of the `emadmin` session and log in as the `dba1` user to observe your privileges and perform monitoring tasks.

    a. Navigate to **Enterprise** > **Monitoring** > **Template Collections** and view the collection that is available to you. Note that having full access to the template collection does not necessarily mean that you have edit access to the templates that are part of it. Only the

template owner and those specifically given edit access have editing privileges to a template.

b. Click `My Template Collection` to view its settings.

c. To return to the **Administration Groups and Template Collections** page, click the top-left link with the name:

Administration Groups and Template Collections > Edit Template Collection My tempalte collection

d. In order to associate a template collection with an Administration group, you must have the `Manage Template Collection Operation` privilege on the group. You may recall that you were given this privilege in the previous Lab. Navigate to **Targets > Groups**.

e. Highlight the `Host-Grp` group and click **Associate Template Collection**.

f. Highlight `My Template Collection`, click **Select**, and then click **Continue**. Look for the Association Successful message.

g. Click the group link called `Host-Grp` and note that the Synchronization Status is pending on both targets in this group:

Pending Targets

2

Targets in an Administration Group are synchronized with the Template Collection where applicable. If an error occurred during synchronization, those targets will be marked with a 'Failed Targets' status.

h. Synchronization of targets with Template Collections occurs on a periodic basis (set up out-of-the-box to once a day). You may also click **Start Synchronization** to perform it immediately. Do so now. Refresh the page and note that the two targets are now synchronized.

i. Navigate to the home page of any of the hosts (for example, `host01.us.oracle.com`) and locate the menu **Monitoring > Metric and Collection Settings**. Note the informational message: "This target is part of Administration Group hierarchy and is managed by one or more Monitoring Templates through the hierarchy." Also, note that the `CPU in I/O Wait` metric now has the thresholds set by the template you created.

j. Log out of the `DBA1` session.

Practices for Lesson 7: Managing Events and Incidents

Overview

Practices for Lesson 7: Overview

Practices Overview

In these practices, you use Incident Manager to administer incidents. First, you intentionally introduce an error by stopping the listener on the `host01` host so that Enterprise Manager produces an availability incident.

Then you find and resolve the incident. You start by gaining an overview. Then select an incident, perform some administration tasks, and drill down into the incident details, including the guided resolution.

Lab 7-1: Preparing an Incident

Overview

In this Lab, you intentionally introduce an error by stopping the listener on the `host01` host so that Enterprise Manager produces an availability incident.

Assumptions

You are logged in to Enterprise Manager Cloud Control from a browser on `host01` as the `emadmin` user.

Tasks

Before using Incident Manager, create an availability incident as a training example.

1. Bring up a terminal window and enter the following commands:

```
[oracle@host01 ~]$ . oraenv
ORACLE_SID = [oracle] ? orcl
The Oracle base has been set to /u01/app/oracle
```

```
[oracle@host01 ~]$ lsnrctl stop
LSNRCTL for Linux: Version 12.1.0.2.0 - Production on <date>
Copyright (c) 1991, 2014, Oracle.  All rights reserved.
Connecting to
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=host01.us.oracle.com)(PORT=1521)))
The command completed successfully
```

2. Log in to Cloud Control as `emadmin` and navigate to **Enterprise > Summary**. Under **Incidents**, you should see at least one fatal incident in the **Availability** section. Some of your targets are down so you will see additional incidents. This is expected behavior.

   Refresh the page until you see an additional incident. The Listener on `host01` is a managed target. Therefore, any Listener status changes will be indicated in the Cloud Control console.

   Hint: You may choose to set the Auto Refresh on the Home page to 15 seconds and watch for an increase in the number of *Availability* incidents (for example, from 9 to 10).

3. Click the **Availability** incidents to view the details. Note initially a new incident: The listener is down: TNS-12541: TNS:no listener.
   When the Listener is down, the system can no longer connect to the `orcl` database. Therefore, you *may* see another incident getting created: A `Metric Alert` (Password Invalid) creates an incident automatically due to the same root problem. Whether you see this incident immediately or not depends on the timing of the metric evaluation.

Lab 7-2: Finding and Resolving an Incident

Overview

In this Lab, you find and resolve an incident in your data center. You could just start on the Enterprise Summary page by clicking a specific digit, which will give you an incident view filtered by that category and type.

In this Lab, your workflow is different (just for training purposes). You start by gaining an overview, and then select an incident, perform some administration tasks, and drill down into the incident details, including the guided resolution.

Assumptions

- You are logged in to Enterprise Manager Cloud Control as the `emadmin` user.
- You completed the previous Lab, which caused Enterprise Manager to create a backup incident.
- Your instructor has given you a demonstration or you have watched the following OLL demonstrations:
  - Incident Management Overview
  - Creating an Incident Management View
  - Viewing Incident Details

  Alternatively, you have the equivalent Incident Management navigation knowledge.

Tasks

1. For an overview of all incidents, navigate to **Enterprise > Monitoring > Incident Manager**. (You may already be on this page from the previous exercise.)

2. Click the **Dashboard** icon at the top and note the categories of incidents and various charts that aggregate data for all the incidents.

3. Switch to the List View and click All Open Incidents. Note the incident: `The listener is down: TNS-12541: TNS:no listener.`

4. Highlight the name to see the incident details. In the bottom-right pane, note the recommendations for resolving this incident.

   How you will work with the administration of incidents in your organization depends, of course, on your business rules. The following steps cover an example that assumes the collaboration of several administrators.

5. To perform incident administration tasks, click **Acknowledge**. Note the changes: The `Last Comment` is updated, and the user is assigned as the `Owner`.

6. Click **Add Comment**, enter the text `Starting research`, and click **OK**.

7. Next, click **Manage**.

8. On the Manage page, select **Work in progress** as Status and click **OK**. Click **Refresh Page** to see the changes.

9. Normally, you would bring up a *Down* target as quickly as possible, but for training purposes, assume that you first want to view the topology to see the effects on other targets of this *Down* target. Locate the **Guided Resolution** pane at the bottom right of the Incident Details screen. Click **View topology**. You can view dependent targets and their details by hovering over the target to display a tool tip and then on the chevrons in that tool tip.

10. On the Listener home page, you could restart the listener by selecting Oracle Listener > Control > Startup/Shutdown. However, for training purposes, return to the **Incident Manager** by navigating to **Enterprise** > **Monitoring** > **Incident Manager**.

11. The Listener incident is now acknowledged. Click "My open incidents and problems," and highlight "`The listener is down.`" Locate the **Restart Listener** link (at the bottom, under **Guided Resolution**) and click it.

12. On the Net Services Administration: Host Login page, confirm the `host01` named credential and click **Login**.

13. On the **Start/Stop: LISTENER** page, confirm that **Start** is selected as Operation and click **OK**. A processing window may appear, followed by a page refresh showing the listener with the Up status.

14. Assume that the rules in your organization require you to set the incident status to Closed and that your username is stored in the OMR. Navigate again to **Enterprise > Monitoring > Incident Manager** page. By default, only open incidents are displayed.

15. Click the Search icon with the magnifying glass. You may have to expand the Search panel from the top right of the page, if the search options are not displayed. Select **Show closed only** and then click **Get Results**. Scroll down to see the results of the search.

16. To confirm all new attributes of this incident, close the Search pane, highlight "`The listener is up`" incident, and note that the `emadmin` username is displayed as Owner and Status is displayed as `Closed`.

    In your environment, you may notice other incidents; it depends on the availability of various components at that point in time. If needed, click Refresh Page to see the changes.

Practices for Lesson 8: Responding to Events, Incidents, and Problems

Overview

Practices for Lesson 8: Overview

Practices Overview

In these practices, you make use of rules and rule sets which include a corrective action. As the rule set is applied to your system, you watch the corrective action take place.

Lab 8-1: Creating a Corrective Action

Overview

In this Lab, you create corrective actions for alerts or events generated in your system. Corrective actions are set up for metrics on monitored targets, and they ensure that alerts or events are cleared automatically by resolving the problem that caused them.

Assumptions

You are logged in to Enterprise Manager Cloud Control as the `emadmin` user.

Tasks

1. In order to use a corrective action, you must first create it. Navigate to **Enterprise > Monitoring > Corrective Actions**.

2. Under **Create Library Corrective Action**, select **Startup Listener** and click **Go**.

3. Enter a name for your action: `MyListener Startup`.

4. Under **Event Types**, associate this corrective action with a **Target Availability** event so that it can be used to correct a Listener Down event.

    This corrective action does not take any parameters.

    Corrective actions can be shared with other administrators and roles. The owner of an action has Full privileges on it and can give access to other administrators. Super Administrators have Full privileges on all the corrective actions in the library. For this exercise, you will not give access to this action to anyone else.

5. Click **Save to Library**. The action should now be listed in your library of corrective actions. Note that the status of the corrective action is Draft. It cannot yet be associated with an event or incident.

6. With the corrective action selected in the corrective action library (option button), click **Publish** and then click **Yes** to confirm. Note that the status of the corrective action changes to Published. The action is now ready to be used in a rule set or associated with an event.

7. This corrective action will use the preferred credentials setup for that target. You set up these preferred credentials in a previous Lab. Check that the credentials are in place.

    a. Navigate to **Setup > Security > Preferred Credentials** to set up/check a preferred credential for a host. Note that named credentials must already be created.

    b. Select `Listener` as the **Target Type** and click **Manage Preferred Credentials**.

    c. In the **Target Preferred Credentials** table, note that the preferred credentials are set for the following target name:

    `LISTENER_host01.us.oracle.com   (Host Credentials)`

    Your listener startup corrective action will make use of this preferred credential.

Lab 8-2: Creating a Rule Set

Overview

In this Lab, you create a rule set, which is a collection of rules that applies to a target. In your case, the rule set will contain only one rule. A rule is a set of automated actions to be taken on specific events, incidents, or problems.

Assumptions

You are logged in to Enterprise Manager Cloud Control as the `emadmin` user and have already created a corrective action in your Corrective Actions Library.

Tasks

1. Navigate to **Setup > Incidents > Incident Rules**. Note a couple of rule sets that are available out-of-the-box. These are sets of best practices that are automated for your system. Click **Create Rule Set** to create your own rule set.
2. Enter the name of your set: `MyIncidentRuleSet.`
3. Select **Applies To Targets**.
4. In the Targets section, select **All targets of types: Listener**.
5. Under **Rules**, click **Create** and enter the Rule Type as **Incoming events and updates to events** and then click **Continue**.
6. Select the events as **Type: Target Availability**.
7. Next, select the option button: **Specific events of type Target Availability**.
8. Click **Add** and select **Target Type as Listener**.
9. Select the **Down** check box to run this action when a listener is down and then click **OK**.
10. Click **Next** to add the actions to be taken by this rule. Click **Add** and towards the bottom of the page, click the **Select corrective action** button.
11. Select the corrective action you created earlier and click **OK**. Note that the corrective action will use preferred credentials of the administrator you are logged in as (EMADMIN, the rule set owner) to execute scripts on the specified targets. Note all the conditions and other options on this page. Leave them as default.
12. Click **Continue** and then click **Next** to specify a name and description for this rule. Enter the name as: `My Rule for Listener Down.`
13. Click **Next** to review the details you entered and then click **Continue**.
14. On the next page, click **Save** to save the rule set with the one rule you created. Note the Rule Set in the list of all enterprise rules. It automatically gets assigned the next available order number. You can choose to reorder the rule sets.

    Note: Enterprise rule sets are evaluated sequentially in the order listed in the rules table. When a new event, incident, or problem arises, the first rule set in the list is checked to see if any of its member rules apply and appropriate actions specified in those rules are taken.

The second rule is then checked to see if its rules apply and so on. Personal Notification rule sets are only evaluated once all enterprise rule set evaluations are complete and in no particular order. The rule sets order defines the event, incident, and problem handling workflow so you must fully understand their impact on your system.

Lab 8-3: Observing How a Rule Set Is Applied

Overview

In this Lab, you see the rule you just created being automatically applied for an incident.

Assumptions

You are logged in to Enterprise Manager Cloud Control from a browser on `host01` as the `emadmin` user, and have set your default preferred credentials for the listener host as guided in Lab 5-2.

Tasks

1. First, navigate to **Enterprise > Monitoring > Incident Manager**, click **All open incidents** in the list of out-of-the-box views, and then click the **Dashboard** icon (because the list view does not have an auto refresh option). Set **Auto Refresh** to 15 seconds.

2. Cause the incident to occur, just as you did in Lab 7-1. Bring up a terminal window and enter the following commands:

   ```
   [oracle@host01 ~]$ . oraenv
   ORACLE_SID = [oracle] ? orcl
   The Oracle base has been set to /u01/app/oracle
   ```

   _

   ```
   [oracle@host01 ~]$ lsnrctl stop
   LSNRCTL for Linux: Version 12.1.0.2.0 - Production on 06-JAN-2016 21:20:19
   Copyright (c) 1991, 2014, Oracle.  All rights reserved.
   Connecting to
   (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=host01.us.oracle.com)(PORT=1521)))
   The command completed successfully
   ```

3. Within 2-3 minutes, you should see the number of *Fatal* incidents increase on the Unacknowledged incidents dashboard.

4. Click **List View** and note the `The Listener is Down…` incident. Highlight it to see its details.

5. In the bottom-right pane, note the **Corrective Action History**. Hover over the message to see the status. Note that the corrective action is using the default preferred credentials that you have set for `host01`. If the credentials are not set, the listener startup job will fail. You can manually submit the corrective action from the library (see the Guided Resolution pane).

6. Refresh this page until the incident clears automatically and the Summary becomes "The listener is up." The incident will be removed from the list of incidents, but the details pane will still show the incident that you had highlighted. The Cloud Control system automatically runs a job to start the listener and, in the next cycle, it clears the incident. Note the incident Status is now **Closed**.

Practices for Lesson 9: Using the Job System

Overview

Practices for Lesson 9: Overview

Practices Overview

In these practices, you perform the following tasks with the Enterprise Manager Job System:

- Create and edit a job that runs a SQL script immediately.
- Create a job and execute it on multiple targets.
- Create a job that includes multiple tasks against different types of targets.

Lab 9-1: Creating and Executing a Simple SQL Job

Overview

In this Lab, you create and edit a job that runs a SQL script immediately. (The steps are divided into "create" and "edit" only for training purposes.)

Create a simple job called MY SQL Job that runs a SQL script against the Enterprise Manager Repository. Save the job to the Job Library. Then, edit the job and execute the job.

Assumptions

You are logged in to Enterprise Manager Cloud Control as the `emadmin` user.

Tasks

1. Navigate to **Enterprise** (Global Menu) **> Job > Library**.

2. Expand the **Create Library Job** drop-down list and review the different types of jobs that Enterprise Manager supports.

3. Select **SQL Script** and click **Go**.

4. On the General tabbed page, enter `MY SQL JOB` in the Name field and, optionally, `Run a simple SQL query` in the Description field.

5. The job will run against a **Database Instance**. To add a target, click **Add**.

6. Ensure that the Target Type is **Database Instance**, select the target database `orcl.us.oracle.com`, and click **Select**. You should see your database listed in the Target section.

7. Click the **Parameters** tab and enter the following query in the SQL Script box (replacing the default script that is displayed):

   ```
   SELECT TABLESPACE_NAME, USED_SPACE, TABLESPACE_SIZE,
   USED_PERCENT FROM SYS.DBA_TABLESPACE_USAGE_METRICS;
   ```

8. Click **Save to Library** for now. You should see a confirmation message indicating that the job was created.

9. To edit your job, select the `MY SQL JOB` job on the Job Library page (option button selection) and click **Edit**.

   Note that drilling into the job name from the confirmation message will allow you to only *view* the new job, not view and edit.

10. Click the **Credentials** tab.

11. Job credentials must be global and can be created from this menu or selected from here, if you have already created them. Click the **Named** option button, and then click **More Details** to see the options already available: The credential for the `SYS` user with the `SYSDBA` role is saved as `SYS_SYSDBA` and the host credential for the `oracle` user with Run Privilege `None` is saved as `NC_HOST_HOST01`. They both have the Scope as Global and will work for running jobs.

12. Click the **Schedule** tab and confirm that the Type is "One Time (Immediately)."

13. Click the **Access** tab and give **Full** Access Level to the SYS and SYSTEM users. Also note the E-Mail Notification options. Skip them in this exercise.

14. Click **Save to Library**. You should see a confirmation message.

15. Select the newly created job and click **Submit** to execute your job.

16. On the "Submit 'SQL Script' Job From Library Job 'MY SQL JOB'" page, click **Submit** again, to confirm submission.

17. You should receive a message that your job was created successfully. Note that the Job System adds a "." (period) and a digit to your job name. Click this job name link. Your job run should be displayed with the status Succeeded. If its status is Running, refresh the page until the status is Succeeded.

18. Note the Output Log displayed in the lower-right pane. This is the output of the SQL query.

Lab 9-2: Creating and Executing OS Jobs on Multiple Targets

Overview

In this Lab, you create a job that runs a host command. You want the job to list a path and directory content (`pwd ; ls`) each day at 8:00 AM on all your hosts.
Tip: Make sure you select a time that enables you to see the job run while you are working on this Lab.

Assumptions

You are logged in to Enterprise Manager Cloud Control as the `emadmin` user.

Tasks

1. Navigate to **Enterprise** (global menu) **> Job > Library**.
2. Confirm that "**OS Command**" is selected in the Create Library Job drop-down list and click **Go**.
3. On the "Create 'OS Command' Library Job – General" tabbed page, enter `My OS Job` in the Name field and, optionally, `List path and directory content` in the Description field. Confirm that the Target Type is **Host**.
4. To add targets, click **Add**.
5. On the "**Search and Select: Targets**" page, click **Select All**, and then click the **Select** button.
6. You should see your two hosts listed in the Target section. Now click the **Parameters** subtab.
7. Confirm that the Command Type is Single Operation and enter **pwd ; ls** in the Command field.
8. Click the **Credentials** tab.
9. Provide the existing `NC_HOST_HOST01` as the Named Host credential to be used.
10. Click the **Schedule** tab. This Lab creates a **Repeating** job. Enter the following values (or adjust them to your training environment):

Description	Choices or Values
Frequency Type	`By Days`
Repeat Every	`3 Days`
Time Zone	Recommendation: Select the time zone of your host computer.
Start Time	Recommendation: Select the time to be 5 minutes from now.

Skip the **Access** tab for this job.

11. Click **Save to Library**.

12. In the Library, ensure that `My OS Job` is selected and then submit the job. Note that the job is scheduled to run on both hosts. You will be able to check its output only after the first execution.

13. Navigate to **Enterprise > Job > Activity**, and in the search criteria, under **Active**, select the option to see only the **Scheduled** jobs. Note the job you created is scheduled. Click it to see its details.

14. When the job completes, you will see the job runs under **Succeeded** jobs. Click the **name** of the job to see the output (Output log) of the OS commands.

Lab 9-3: Creating a Multitask Job (Optional)

Overview

In this optional Lab, you create a job that includes multiple tasks against different types of targets. In this example, assume you want to shut down a database target and, if that job succeeds, you want to create a new directory where trace files will be written.

Assumptions

- You are logged in to Enterprise Manager Cloud Control as the `emadmin` user.

Tasks

1. Navigate to **Enterprise > Job > Library**.
2. From the Create Library Job drop-down list, select **Multi-Task** and click **Go**.
3. On the "Create 'Multi-Task' Library Job" page, enter CHANGE TRC LOCATION in the Name field.
4. For the Target field, select **Different targets for different tasks**.
5. Click the **Tasks** tab and under Type, select **Shutdown Database,** and click **Add.** This takes you to the Create Task dialog box (essentially creating a new job).
    a. Enter a name for your first job, SHUTDOWN TEST1 DB.
    b. Under **Target**, click **Add** and select the `test1` database.
    c. On the **Parameters** tab, select Immediate.
    d. Click the **Credentials** tab and select the credential for the SYS user with the SYSDBA role saved as SYS_SYSDBA and the host credential for the `oracle` user with Run Privilege None saved as NC_HOST_HOST01. Click **Continue**.
6. Create the second task. On the **Tasks** tab, under Type, select **OS Command** and click **Add**.
    a. Enter a name for your task (job), CREATE_NEW_TRC_DIRECTORY.
    b. Keep the target Type as **Host**.
    c. Under **Condition**, select On Success and ensure that the prior task, SHUTDOWN TEST1 DB, is listed under **Depends On**.
    d. Under **Target**, click **Add** and select the `host01` host.
    e. On the **Parameters** tab, enter the following information:
        – Command Type: Single Operation
        – Command: mkdir /home/oracle/test1_trc
    f. On the **Credentials** tab, select the `host01` **named** credential saved as NC_HOST_HOST01. Click **Continue**.
7. On the **Schedule** tab, keep the default of One Time.
8. Keep the defaults on the **Access** tab.
9. Review the multitask job definition by clicking the **Tasks** tab. The `test1` database is being shut down first; if the first job succeeds, then a new trace files directory is created.

    At this time, you can save the job definition to the library to be used at a later time. Click **Save to Library**.

10. From the Job Library page, select the CHANGE TRC LOCATION job, click **Submit**, and since there will be no changes to the job, click **Submit** again.

11. On the confirmation dialog box at the top, click the job name CHANGE TRC LOCATION.1 to see the details of the job run. Refresh until the job succeeds.

12. Review the results of each task by highlighting the task and examining the output log.

13. Extra **optional** steps: If time permits, you may verify that the directory was created and that the test1 database is now shut down.

    Keep the test1 database down.

Practices for Lesson 10: Managing Systems and Services

Overview

Practices for Lesson 10: Overview

Practices Overview

In your organization, you might have customized applications that you want to monitor with Enterprise Manager. These practices cover the following topics to enable you to Lab the workflow of such tasks:

1. Review existing systems and services and answer the following questions (choose the ones that are relevant for you):
   - What is the status of the Daily Maintenance job?
   - When was the Daily Maintenance job last executed?
   - Is there a Beacon job that tests availability? If yes, what is its frequency?
   - Are there any jobs for which information is not available?
   - What is the name of the Management Service for the OMS and the OMR?
   - Which OMS applications does it include?
   - What is this service a member of?
   - What are the service levels over the last seven days for each of the services displayed on the Enterprise Manager Dashboard?
   - To which system do they belong?
   - Which service is monitored by a beacon (use the Services overview page to determine this information)?
2. Create a sample *System* named `MY_AGENT_SYSTEM` to observe how multiple components can be managed and monitored as a single unit.
3. Create a *Generic Service* named `MY_AGENT_SERVICE` and select the `MY_AGENT_SYSTEM` system to host this service. In this case, the availability of your service is based on the system you created. To measure the availability, you also define and enable a Service Level Agreement (SLA).
4. Establish access to a web application you want to monitor. First, you monitor the *application availability*. You create a *test-based generic service*, called `My_WLConsole_Service`, for a web transaction type and define its availability based on a test performed by a beacon. In addition, you enable an SLA that is based on the availability of your service.
5. Second, you monitor the login access to your application by defining another web transaction and then include this test as part of your SLA measurement.

Lab 10-1: Reviewing Existing Systems and Services

Overview

In this Lab, you review the systems and services that Enterprise Manager has defined for you. If you are already familiar with them, you can skip this Lab.

Assumptions

You are logged in to Enterprise Manager Cloud Control as the `emadmin` user.

Tasks

1. A Cloud Control *System* is a collection of related manageable entities that together provide business functions. Members of any system can have relationships among themselves, called associations. **Management Services and Repository** is a special target in Cloud Control, which is set up as a System. To examine the existing systems in your environment, such as the OMS and the Repository, navigate to **Targets > Systems**.

2. Expand the **Management Services and Repository** system to see all its members.

3. Click the **Management Services and Repository** link. Note that various details about this system can also be accessed by navigating to **Setup > Manage Cloud Control > Repository** or **Setup > Manage Cloud Control > Health Overview**.

4. Navigate to **Setup > Manage Cloud Control > Repository** to view information about the repository DBMS jobs and to answer the questions that follow.

    a. Examine the **Repository Scheduler Jobs Status** section. Select the option button **All** to view all jobs.

    b. What is the status of the EM Daily Maintenance job? *(Up)*

    c. In the left-middle pane, what is the size of the Cloud Control setup (repository)? *(Small)*

    d. Is the Data Rollup Throughput increasing or decreasing? *(It can vary, most likely decreasing)*

5. Click the **Schema** tab. Review all details about the repository schema.

6. Click the **Metrics** tab. Which target type collects the most data in your system? *(Application Deployment).* Click the Application Deployment "bubble" to see only that subset of rows loaded.

7. Cloud Control *Services* are groupings of targets that represent business functions or applications that run in your enterprise and can be monitored for availability. SLA management is critical to business applications. Services can be monitored for performance and availability by defining key tests to be executed by one or more *Beacons* located in different user communities.

    Navigate to **Targets** (global menu) **> Services** to view examples of the services already defined in Cloud Control.

    a. Which service is monitored by a beacon? Why? *(EM Console Service, a test-based system)*

    b. What beacon monitors the EM Console Service? (*EM Management Beacon*)

c. What kind of service is the EM Jobs Service? (*System-based*)

d. What system is the EM Jobs Service based on? (The Management Services and Repository system that includes the OMS Console, the OMS Platform, and the Oracle Management Service)

Practices for Lesson 10: Managing Systems and Services

Lab 10-2: Creating a System

Overview

In this Lab, you create a system called MY_AGENT_SYSTEM, with target members associated with the agent on host01. Assume that the system is located in New York. Note that this is just an example of grouping based on the limited set of targets you have in your environment.

Assumptions

You are logged in to Enterprise Manager Cloud Control as the emadmin user.

Tasks

1. Navigate to **Targets > Systems**.
2. Select **Add > Generic System** from the drop-down list.
3. On the "Create Generic System: General" page, enter the following values. Be sure to expand "System Properties" and scroll down to access all of the fields.

Field Name	Value
Name	`MY_AGENT_SYSTEM`
Comment	`Test system`
Privilege Propagating System	**Not Selected**
Time Zone	`New York –Eastern Time`
Contact *(expand System Properties)*	**<your name>**
Lifecycle Status	`Test`
Line of Business	`Financials`
Location	`New York`

4. In the Members section (*middle of the page*), click **Add**.
5. Order by Host name, locate members on host01.us.oracle.com, hold down the *Ctrl* key and select the following target members, and then click **Select**.
   - agent13c1_2_host01.us.oracle.com_8586 (the agent home)
   - host01.us.oracle.com (the agent host)
   - host01.us.oracle.com:3872 (the agent)
6. Select the check box "Include targets that selected members directly depend on" and then click **Next**. Note that in this case, there are no dependent members.
7. On the "Create Generic System: Define Associations" page, select **Show associations automatically detected by Enterprise Manager** if no associations are displayed. Review the list and click **Next**.

8. On the "Create Generic System: Availability Criteria" page, select **Any Of The Key Members**. Move the `host01.us.oracle.com (Host)` and `host01.us.oracle.com:3872 (Agent)` to the Key Members list. Click **Next**.

9. Accept the Oracle-suggested charts and click **Next**.

10. Review your definitions and click **Finish**. You receive a confirmation message that your system was created. You see the system `MY_AGENT_SYSTEM` with status of "Up" (green). All its members are up.

11. Click the **MY_AGENT_SYSTEM** link in the Name column and review your `MY_AGENT_SYSTEM` home page.

Lab 10-3: Creating a Generic Service

Overview

In this Lab, you create a system-based generic service (that performs a specific business function) named `MY_AGENT_SERVICE` and select the `MY_AGENT_SYSTEM` system to host the service. System-based services provide functional grouping of components, mapping to system components, and provide the ability to set monitoring and evaluate availability and performance based on your company SLAs.

Assumptions

You are logged in to Enterprise Manager Cloud Control as the `emadmin` user.

Tasks

1. Navigate to **Targets** (global menu) **> Services**.
2. Select **Generic Service – System Based** from the **Create** drop-down list.
3. On the "Create Generic Service: General" page, enter `MY_AGENT_SERVICE` in the Name field and click **Next**.
4. Select the previously created `MY_AGENT_SYSTEM`, click **Select**, and then click **Submit**. You should receive a confirmation message and the new service shows on the Services page.

   Why did the Create Generic Service wizard not request to add beacons for your service creation?

   Answer: Because your service is defined based on a system. Its status will be derived from the system status and not measured by a Beacon.

5. Review your new `MY_AGENT_SERVICE` home page by drilling down into the `MY_AGENT_SERVICE` link.

   a. Review Generic Service > Monitoring > All Metrics and Generic Service > Monitoring > Metric and Collection Settings to see the default metrics.

   b. Review **Generic Service > Administration** to see all options available.

6. Navigate to **Generic Service > Service Level Agreement > Configuration** and create your own SLA**.** Note that there is a default SLA in place, but it is not enabled.

   a. Click **Create**.

   b. Give the SLA a name: `MY Agent SLA` and review the defaults.

   c. Click **Next** and then **Create** to create a Service Level Objective (SLO).

   d. Give the SLO a name, `Agent SLO,` and select **Type** `Availability` (assume you are interested in its up/down status). Review the rest of the defaults and then click **Next** to proceed to the Service Level Indicators.

   e. Accept the target status equal to Up as a measure of its availability and click **Submit**.

   f. Click **Next** to proceed to the Enable Service Level Agreement page.

   g. Select the option to Enable Later starting three days from now.

h. Click **Next**, review the definition, and click **Submit**. Note the initial Lifecycle Status is *Scheduled*. The SLA will be enabled and start measuring availability three days from now when it will become *Active*.

Practices for Lesson 10: Managing Systems and Services

Lab 10-4: Monitoring the Availability of a Web Application

Overview

In this Lab, you use a web application to define another *service* (that performs another business function) and define its *availability* based on a Service Test. Cloud Control is a WebLogic Application itself so you use components that are already available in your environment. You also create a new beacon that will be used to perform the availability test. In addition, you define an SLA measure for this application based on its availability.

Assumptions

You are logged in to Enterprise Manager Cloud Control as the `emadmin` user.

Tasks

1. For this Lab, you use the WebLogic Administration page as your application. This page is accessible from the browser. However, you do not need to log in to WebLogic Administration. Verify this page:

   a. Open a new browser tab or window and enter a URL similar to the following:

   https://<hostname>.<domain>:7102/console

   In your environment, you can click the bookmark called `Admin Svr` or navigate to: `https://emcc.example.com:7102/console`

   b. You should be presented with a "Your connection is not secure" page as WebLogic Server's default out-of-the-box certificate is considered to be invalid by the browser, so you need to add a security exception.

      1) Click **Advanced** on the "Your connection is not secure" page.

      2) Click **Add Exception** beneath the information about the invalid security certificate to display the Add Security Exception dialog box.

      3) Click **Confirm Security Exception** and leave Permanently Store this Exception selected.

      4) The WebLogic Server Administration Console appears.

      There is no need to log in as the `weblogic` user.

   c. Return to your Cloud Control console window.

2. A "beacon" is a function of the management agents that allows you to remotely monitor a service. A beacon is defined as a Cloud Control target and executes tests at regular intervals. A service is considered available if the test executes successfully on at least one key beacon.

   When monitoring a web application, you may use existing beacons or create new ones. For this exercise, you use an existing beacon and create an additional one as well. It is recommended that you create only one beacon per host or agent.

   a. Navigate to the **Targets > All Targets** page and sort the targets by target types. Note the existing beacon "EM Management Beacon" and drill down to see its details. Note the following: Its status is Up, it resides on the host `emcc.example.com` (the

OMS host), and it monitors the "EM Console Service" as a key beacon. This beacon is created by default.

b. To create a new beacon, from the **Setup** menu, select **Add Target**, and then select **Add Targets Manually**.

c. On the Add Targets Manually page, select **Add Target Declaratively by Specifying Target Monitoring Properties.**

d. Select `host01.us.oracle.com` as the **Host**, select **Beacon** from the Target Type drop-down list, and click **Add**.

e. On the `Beacons: Create Beacon` page, enter `New York Beacon` as the name. Leave the other fields as default and click **OK**.

f. Click the **Refresh** button until you see the status is up. It may take some time for the status to be up. This beacon will be attached to the `host01` agent.

3. Next, you define the new service for which you want to measure availability. Because this is a service measured by tests performed by a beacon, it is called a *Test-Based Generic Service*. Navigate to **Targets > Services**, click **Create**, and select the **Generic Service – Test Based** option.

4. Enter `My_WLConsole_Service` in the Name field, leave the time zone as default, and then click **Next**.

5. The "Create Generic Service: Service Test" page changes depending on the Test Type that you choose. A web application's availability can be tested in a number of ways, for example:

   – Using a Web Transaction, by providing a URL that clients use to access the application, but not authenticating the application (not logging in)

   – HTTP Ping, which is similar to the UNIX `ping` utility, but works over HTTP/S instead of ICMP, and checks a URL instead of a host/IP address

For this Lab, select **Web Transaction** (default) as the Test Type, enter or confirm the following values, and then click **Next**:

Field	Value
Name	`WLConsole_Availability`
Description (optional)	`Measures WebLogic Administration Console availability without login`
Collection Frequency (minutes)	`3`
Basic Single URL	`https://emcc.example.com:7102/console`

6. On the "Create Generic Service: Beacons" page, click **Add**.

7. Select the **New York Beacon** and **EM Management Beacon** on the Select Beacons page (or Select All) and click **Select**. Back on the `Create Generic Service: Beacons` page, verify that both the beacons are added. Click **Next**.

8. Review the entire page and click **Finish**.

9. The web application service is successfully added. The status shows "Pending." After a little while, it should change automatically to "Up." Refresh the page to see the new status.

   This service derives its status based on the tests performed by the key beacons against the URL provided. Since the new service becomes a Cloud Control target, it inherits the management and monitoring options applicable to this type of target. Some are set by default. For example, if the availability test fails, the target is considered `Down` and a Critical event is automatically generated.

10. *Service Level* is a measure of service quality. Service Level is calculated as the percentage of time during business hours that a service meets the specified availability and performance criteria. An SLA is automatically defined for your target by default but it is not enabled.

    a. Navigate to the `My_WLConsole_Service` Service home page.

    b. From the main menu, Generic Service, navigate to the Service Level Agreement > Configuration menu.

    c. Note the default SLA created: Monthly SLA requiring 85% on expected service level for service target availability.

    d. Highlight the SLA in the lower table and click **Edit**. Step through all the definition pages (1-4). Note the one Service Level Objective (SLO): *Your application must be available Monday-Friday all day a total of no less than 85%. When availability reaches 90% you receive a warning.* When you get to page 4, cancel out of this menu.

    e. Next, click the **Enable** button to enable this SLA and select the option to **Enable Now**. Then, click **OK**. Note the success message at the top.

    f. Refresh the page. Once the **Lifecycle Status** changes to `Active`, the **SLA Dashboard** (on the top menu) will display the availability of your service over a period of time. Click the **SLA Dashboard** to see its format. It will take a while for valid data to display.

Lab 10-5: Creating and Testing a Web Transaction

Overview

In this Lab, you manually define a web transaction, enable it, and then test it with your web application. You determine that this transaction also measures the availability of your application. Therefore, you mark its testing as *key* testing. The results of this test will be taken into account when calculating the SLA you have enabled.

Assumptions

You are logged in to Enterprise Manager Cloud Control as the `emadmin` user.

You have opened a browser with a URL in the following format:
`https://<hostname>.<domain>:7102/console`

For example: `https://emcc.example.com:7102/console`

The WebLogic Server Administration Console is displayed. Initially, there is no need to log in.

Tasks

1. Navigate to **Targets** (global menu) **> Services**.
2. Click `My_WLConsole_Service`.
3. The `My_WLConsole_Service` home page is displayed.

   In addition to the availability of your web application, simply measured by whether it is responding or not, you are interested in its *accessibility*, measured by whether you can perform a login transaction.

   To create this transaction, click the main menu: **Generic Service > Administration > Service Tests and Beacons**.
4. To create a new transaction, select the Test Type **Web Transaction** and click **Add**.
5. Specify the transaction name as `WLConsole_Access` for this Service Test and keep the default **Collection Frequency** as 5 minutes.
6. Scroll down and click **Create** to create the steps of the transaction.
7. To define Step 1 of the test:
   a. Enter **Step 1** in the **Name** field, at the very top of the page.

   b. Enter the URL of the WebLogic Server Administration Console home page in the **Request URL** field: `https://emcc.example.com:7102/console`.
   c. Verify that **GET** is selected from the **HTTP Method** drop-down list.
   d. Review and accept the rest of the default values and click **Continue**.
8. Under **Steps**, click **Insert After** and add the second step.
   a. Enter **Step 2** in the **Name** field.

b. Enter the URL of the WebLogic Server Administration Console login page `https://emcc.example.com:7102/console/login/LoginForm.jsp` in the **Request URL** field.

c. Select **POST** from the **HTTP Method** drop-down list.

d. Expand the POST Data field and enter the following string:
`j_username=weblogic&j_password=<weblogic_password>`

(where **weblogic_password** is the password for `weblogic` as it was given to you)

e. Click **Continue**.

9. Scroll again to the Steps section and click **Insert After**. Define the third step.

a. Enter **Step 3** in the **Name** field.

b. Enter the WebLogic Server Administration Console Log Out URL in the **Request URL** field:

To obtain the URL, you can log in to the WebLogic Server Administration Console as the `weblogic` user, with its given password. Then, move the cursor over **Log Out**, right-click, click Copy Link Location to copy the URL from the Log Out link, and then paste it in the URL field in the Cloud Control console.

It should be:

`https://emcc.example.com:7102/console/jsp/common/warnuserlockheld.jsp`

c. Verify that **GET** is selected from the **HTTP Method** drop-down list.

d. Click Continue.

10. To create the Service Test, click **OK** to save these steps. You should receive a confirmation message that the service has been created.

11. Once the web transaction is successfully saved, confirm the beacons that will be performing this service test: the **New York Beacon** you created earlier and the built-in EM Management Beacon.

12. The next step is to enable the web transaction. To do so, select the **WLConsole_Access** transaction and click the **Enable** button. You should receive a confirmation that the service test has been successfully enabled.

13. If you determine that this test must also be a measure of your web application availability, you can make this test a *key* test. To make this service test a key service test, select the check box in the **Key Service Test** column and then click **Change Key Tests**. You should receive a confirmation that the tests have been updated successfully.

These tests results are now automatically taken into account for the SLA you have enabled.

14. Verify that the service test `WLConsole_Access` is working.

a. Select `WLConsole_Access` and click **Verify Service Test**.

b. There are no test results initially. Select one of the beacons and then click **Perform Test**.

c. Scroll horizontally to review all the results. The table should display response times and rates. The status should show Up (green up arrow).

15. Navigate to the **Test Summary** page: ![Test Summary] . In time, as tests are automatically performed according to the defined collection frequency, more meaningful data will be displayed.

16. Highlight each test to see the details of the collected metrics.

17. Optionally, if you have allowed some time to collect some data, you can explore the **SLA Dashboard** ![SLA Dashboard] and navigate to **Generic Service > Service Level Agreement > Dashboard** to see additional service level indicators.

Practices for Lesson 11: Patching and Provisioning

Overview

Practices for Lesson 11: Overview

Practices Overview

In these practices, you learn how to automate the provisioning and patching of software in your data center. To use the Oracle-provided "Patch Oracle Database" Deployment Procedure in offline mode, you need to fulfill the following requirements:

- Set up and configure the Software Library.
- Set My Oracle Support to "offline."
- Upload the updates (metadata) file.
- Review the "Refresh From My Oracle Support" job in offline mode.
- Download the patch files to a known location and upload them to the Software Library.

The prerequisites for configuring a Software Library storage location are available storage space and setting appropriate host credentials.

Lab 11-1: Preparing for Offline Patching

Overview

In this Lab, you perform one-time steps to prepare your environment for offline patching:

- Set/review the **Normal Host Credentials** and the **Privileged Host Credentials** for the host that you are patching.
- Verify the default software storage location, `default_loc`, which points to an area with sufficient available storage space.
- Configure offline patching.
- Upload the metadata updates file and run the "`Refresh From My Oracle Support`" job.

Note: This job is also required in offline mode because it computes patch recommendations.

Completing this Lab is a prerequisite for Lab 11-2, "Patching Offline."

Assumptions

You are logged in to Enterprise Manager Cloud Control as the `emadmin` user.

Tasks

1. A prerequisite for patching is having a configured Software Library, a storage area for your software. In your lab environment, a Software Library was already configured with appropriate space. The user that configured the Software Library, `emadmin`, has View privileges on all the OMSs (in your case, one OMS on the `em13c` host).

   To check the existing Software Library, navigate to **Setup > Provisioning and Patching > Software Library**.

   a. Select `default_loc` and then click **Actions > Check Accessibility**.
   b. You should receive a confirmation that the location is accessible.
   c. Optionally, you can click **Show** in the Associated Entities column to view many predefined entity associations. When you have finished reviewing the associated entities, click **Cancel**.
   d. By default, your system is set up to allow online patching by connecting to My Oracle Support (MOS) to download patches, latest health checks, or self-updates. In your environment, you do not have access to MOS and therefore you must set up Offline patching. Navigate to **Setup > Provisioning and Patching > Offline Patching** and select the **Offline** option.

2. Take a look at the **Patches & Updates** page to see the current state of your patching. Navigate to **Enterprise > Provisioning and Patching > Patches & Updates**. Note that your system is set up for **Offline** patching and there are currently no patch recommendations for your system.

3. To set up your patching, navigate to **Setup > Provisioning and Patching > Offline Patching**.

On the **Offline Patching** page:

a. Confirm that the **Connection** is **Offline**.

b. In the **Offline** case, the up-to-date patch recommendations must be downloaded separately and made available to this system. The updates have already been downloaded and saved in your environment. Click **Browse** and navigate to `/home/oracle/labs/updates`.

c. Select `em_catalog.zip` and click **Upload**.

You should receive a success message indicating that the Catalog file has been uploaded.

A dedicated job called "`Refresh From My Oracle Support`" is scheduled by default to run periodically to extract information from the metadata file and display it in the Cloud Control console. Click the "`Refresh From My Oracle Support`" link to view the job details. Refresh periodically to view its up-to-date status. The job does not actually connect to MOS in this mode, but it computes patch recommendations based on the data uploaded to the repository page until you see the Succeeded status.

Hint: Turn on auto-refresh.

d. Optionally, click **Show All Details**, and then click **View Complete Log** to review the entire Output Log. The XML files are parsed and loaded. This job could take 5 to 9 minutes.

4. Navigate to **Enterprise > Provisioning and Patching > Patches & Updates** to view the recommended updates based on the uploaded information.

a. Click the **All Recommendations** link.

b. Review the patches recommended for each target. To filter the patches, you can select one of the categories from the drop-down menu. Note that in this case only **Security** patches have been released. You will be selecting one of them to apply to your system in an upcoming Lab. Note in particular Patch `21359755`.

Lab 11-2: Patching Offline

Overview

Offline mode does not require network connectivity to MOS. In this Lab, you perform offline patching steps:

1. Upload a patch to the Software Library.
2. Apply the uploaded patch via a patch plan, which defines deployment details. A patching wizard guides you through the steps.

Assumptions

You are logged in to Enterprise Manager Cloud Control as the `emadmin` user. You completed Lab 11-1: Preparing for Offline Patching.

Tasks

1. It is recommended that before you patch, the **EM Target Patchability Report** is run to analyze your targets and make sure they are "patchable."

   a. Navigate to **Enterprise > Provisioning and Patching > Patches & Updates**.

   b. Under **Patching**, locate the **Target Patchability Report** and click it. A preview of the report is displayed. Note that all targets are patchable.

2. To perform any patching tasks in Cloud Control, you need to set up Named Credentials for normal operating system user accounts (in your case `oracle`) and privileged user accounts (`root`). If you do not have access to either the Oracle software owner account or the `root` account, then you can use Privilege Delegation. Privilege Delegation is a framework that allows you to use either Sudo or PowerBroker to perform an activity with the privileges of another user (usually locked accounts).

   Ideally, these named credentials are saved as Preferred Credentials for your hosts. In general, Preferred Credentials can be set up per target type by setting up Default Preferred Credentials, in which case each target of that type inherits that credential. Or you can define a specific credential for each target of that type.

   In this Lab, you set up Normal and Privileged credentials for a Host type.

   a. Assume that you do not have `root` privileges to your target. Navigate to **Setup > Security > Privilege Delegation**.

   b. You will be patching the `host01.us.oracle.com` host, so note that the **Sudo** delegation tool is set up for it.

   c. You must also have preferred host credentials set up for the target host. Navigate to **Setup > Security > Preferred Credentials**.

   d. On the Preferred Credentials page, select **Host** and click **Manage Preferred Credentials**. Note that **Normal Host Credentials** and **Privileged Host Credentials** are set for `host01.us.oracle.com`.

3. When working in Offline mode, patches must be pre-saved in a known location. A patch administrator would have to connect to *https://support.oracle.com* and download all patches of interest for your environment.

   In your environment, one patch was downloaded for use in this Lab: `Patch 21359755`. This patch contains one archive file, `p 21359755_121020_Generic.zip`, and a metadata file: `p 21359755_121020_American` (a text file).

   Note that along with most patches, you must have saved in the Software Library a copy of the latest OPatch (saved as a patch itself under Universal Installer). In your environment, you have `OPatch patch` saved as files `p6880880_121010_Linux-x86-64.zip` and `p6880880_121010_American`.

   The next step is to make these patches available to Cloud Control from their current location `/home/oracle/labs/offline_patch/` to the Software Library.

   a. To upload and save a patch in the Software Library, navigate to **Enterprise > Provisioning and Patching > Saved Patches**.

   b. Click **Upload** to first upload the latest OPatch patch to the Software Library. On **Upload a Patch**, select the following:

      • Browse for the patch ZIP file: `/home/oracle/labs/offline_patch/ p6880880_121010_Linux-x86-64.zip`.

      • Browse for the patch metadata file: `/home/oracle/labs/offline_patch/ p6880880_121010_American`.

      Click **Upload**. Look for the success message at the top of the window.

   c. Repeat the previous step for the next patch. Click **Upload** to upload a new patch to the Software Library. On **Upload a Patch**, select the following:

      • Browse for the patch ZIP file: `/home/oracle/labs/offline_patch/p 21359755_121020_ Linux-x86-64.zip`.

      • Browse for the patch metadata file:

        `/home/oracle/labs/offline_patch/p 21359755_121020_American`.

      Click **Upload**. Look for the success message at the top of the window.

4. To prepare for this patching Lab, start the database you will be patching. Note that the database *may* already be up if you did not perform the optional exercise in Lab 9-3. Navigate to **Targets > Databases** and click `test1`.

   a. If the `test1` database is up, skip to Step 5.

   b. Navigate to **Oracle Database > Control** and click **Startup/Shutdown**.

   c. Keep the credentials selected by default, click **OK**, and then click **Yes**. Note the database *up* status at the end of this step.

5. To perform a patching task, you first add a patch to a plan. Navigate to **Enterprise > Provisioning and Patching > Saved Patches**.

   a. Click the name of the latest patch you uploaded: `21359755`.

   b. Review the patch details and what targets it applies to. Next, click **Create Plan**.

   c. Enter a name for your plan: `dbpsu_121025`.

   d. Click **Add** to add a target, select `test1`, and then click **Create Plan**.

e. This patch impacts other targets in the same Oracle home. In this case, you want to only apply it to one target, which happens to be your development/test database. Click **Add Original Only** so that only one instance in that Oracle home is set as your target.

6. Next, you review and submit the patch plan.

a. Navigate to **Enterprise > Provisioning and Patching > Patches & Updates** and view the plan you just created. Click the plan name.

b. Review the defaults on Step 1 and Step 2, clicking **Next** to move between steps. Then, under Deployment Options (Step 3), keep the default patching to be **Out of Place**.

You may recall *preferred* credentials have already been set for all targets affected by this patch application: the host `host01.us.oracle.com` (normal and privileged credentials), the `test1` database instance (Normal, SYSDBA, and Database Host credentials), as well as the database home (normal and privileged credentials).

c. Click **Next** to accept all other defaults and advance to **Step 4: Validation**. Click **Analyze**. It should take 3-5 minutes.

d. Click **Show Detailed Results**. This opens a new window for the results. The analysis is a Deployment Procedure, a series of steps, directives, and jobs that simulates the patch application on the given target and ensures that all prerequisites are met. When the validation is completed, close this browser window.

e. Back in the original browser window, navigate to the top-left link **Patches & Updates**

    Patches & Updates >   and under Plans, note the successful status of your plan.

f. Click the plan name, and note the "Ready for Deployment" message. There are no issues to resolve. Click **Review** and note the details of the patching procedure: "Out of Place Patching, Switch 1 database instances out of 3 database instances to the new Oracle home. No down time is required."

   Hint: Make sure that the patch you are applying is indeed listed in the summary table as one to be applied without conflicts.

g. Click **Prepare and Deploy**, check **Deploy**, and then click **Submit** to submit this patching job immediately. Note the `Deployment In Progress` status at the top of the page.

h. Monitor the patching task from **Enterprise > Provisioning and Patching > Procedure Activity**. It should take approximately 14 minutes.

i. Navigate back to **Enterprise > Provisioning and Patching > Patches & Updates** and note that the plan that you created shows a status of **Deployed Successfully.** Also note that the Oracle home that hosts the target that you just patched, `OraDB12Home1_1_host01.us.oracle.com`, shows the applied patch.

   The plan now becomes locked because the patches were deployed. To apply these patches on a new set of targets, you must save this plan as a template. You can do this directly from the Review and Deploy page after successful deployment, by clicking the **Save as Template** link.

7. During the patching task, your instructor might suggest additional activities, such as viewing the "Perform Out-of-Place Database Patching" demonstration and answering related questions:

a. The demonstration mentions several tests that are performed for you. Which one is the most important for your organization?

b. True or False: Before starting the patching operation, you can specify the new Oracle home. It can be validated only after creation.

c. True or False: While patches are applied to a new Oracle home, the original one is not affected by this operation.

d. True or False: The switching from the original to the new Oracle home occurs during a regular maintenance window.

Practices for Lesson 12: Managing Configurations

Overview

Practices for Lesson 12: Overview

Practices Overview

In these practices, you view, compare, and search the configuration information in the OMR to monitor and manage your enterprise configuration:

1. View the installed OS packages and their version numbers under Operating System Components.
2. View the configuration history and use the topology viewer.
3. Compare your host configuration with another host configuration.
4. Search for the Oracle products installed in Oracle homes.

Lab 12-1: Viewing Configuration Details

Overview

In this Lab, you view the installed OS packages and their version numbers under Operating System Components.

Assumptions

You are logged in to Enterprise Manager Cloud Control as the `emadmin` user.

Tasks

1. Navigate to **Enterprise > Configuration > Inventory and Usage Details** for a complete view of your enterprise configuration.

   a. You see initially the configuration information for your *hosts:* summarized information on the top part of the page and hosts details at the bottom viewed by host name, platform, vendor, and so on.

   b. In the Summary table, from the drop-down menu, select another entity to view its details. Select **Database Installations**. Note your database installations in your enterprise by host names, locations, platforms, and so on.

2. Each target in your enterprise will have configuration information that applies to its type. Navigate to **Targets > Hosts** and click `host01.us.oracle.com`.

   a. From the host home page, navigate to **Host > Configuration > Latest**. Note the latest information about this host. A Refresh will trigger the agent to collect a new set of configuration data.

   b. On the **Latest Configuration** page, click any hardware or operating system item that interests you. For example, review the installed OS packages and their version numbers under **Operating System Components**.

   c. Clicking **Host > Configuration > Saved** would show the saved configurations that can later be compared with other systems. In your case, none have been saved.

Lab 12-2: Viewing Configuration History and Topology

Overview

In this optional Lab, you view the configuration history and use the topology viewer.

Assumptions

You are logged in to Enterprise Manager Cloud Control as the `emadmin` user.

Tasks

1. If you closed the previous page, navigate back to **Targets > Hosts** and click `host01.us.oracle.com`.

2. On the host home page, navigate to **Host > Configuration > History**.

    If there were any configuration changes, this page displays all the configuration changes that occurred on the host during the last seven days. You can change the date parameters to view changes over a longer period of time.

3. For example, note the Lifecycle status change for this host. In the **Configuration Changes** table, in the first row, click the **History Records** number. You may recall that you changed its status from undefined to `Production`.

4. Navigate to **Host > Configuration > Topology** and select **Used By** in the View menu.

5. The topology map may be too small to read. Click the Control Panel icon ⊘ to reveal the zoom controls, and zoom in as desired. Drag the cursor around the topology map to reposition the viewable portion.

6. Optionally, click **Display > Table** Display ○ Graph ◉ Table and expand targets to view additional configuration in the table format.

Lab 12-3: Comparing Configurations and Managing Drift

Overview

In this Lab, you compare your host configuration with another host configuration. The Compare wizard allows you to compare various types of current or saved configurations with one or more current or saved configurations from other hosts.

Assumptions

You are logged in to Enterprise Manager Cloud Control as the emadmin user.

Tasks

1. To compare configurations, navigate to **Enterprise > Configuration > Comparison & Drift Management**.

2. Review the Overview page and note all the comparison options: One-Time Comparison, Drift Management, or Consistency Management.

3. Click **Create Comparison** under the **One-Time Comparison** section.

   a. Click **Search,** search by **Target Type** Host, and then click **Search.**

   b. Highlight host01.us.oracle.com and click **Select** to define your **Reference Target.**

   c. Select the **Default Host** Comparison Template.

   d. Give the comparison a name: My Host Comparison.

   e. In the Compared Targets table, click **Add** and select emcc.example.com.

   f. Click **Submit**. A job run begins. "Comparison – In Progress" is displayed while the job runs. It will take a few seconds to complete. The report page shows detailed results of the target properties, the hardware, and the operating system comparison for the two

      hosts. The "no equal" symbol   indicates values that are not the same as the

      reference target, and the presence symbol   indicates values that are present versus not present in each system.
      Results can be saved as a zip file.

4. Navigate back to **Enterprise > Configuration > Comparison & Drift Management**. Drift management allows you to manage targets from departing from standard configurations.

   a. Under **Drift Management**, click **Create Definition**.

   b. Select **Target Type** Host and **Template** Default Host, and click **OK.**

   c. Select the **Latest Configuration** as your Source Configuration and search for host01 as your **Source Target**.

   d. Click **Save and Associate Targets**, and then click **Add**.

   e. Select emcc.example.com and click **OK**.

   f. Confirm with **Yes** and your drift definition will be associated with the host em13c.

   g. Return to the **Comparison & Drift Management** main page (**Enterprise > Configuration > Comparison & Drift Management**).

h. On the left navigation tabs, click the **Drift Results** tab and note a critical drift notice.

i. Click the **One-Time Comparison Results** tab and the **Definition Library** tab to view the comparison and drift definition you created.

j. The last tab, **Comparison Templates** , has the predefined Oracle templates for targets of various types. Review these templates.

Lab 12-4: Searching Configurations

Overview

In this Lab, you search for the Oracle products installed in Oracle homes.

Assumptions

You are logged in to Enterprise Manager Cloud Control as the `emadmin` user.

Tasks

1. To search configurations, navigate to **Enterprise > Configuration > Search**.
2. A number of searches are already predefined for you. Sort by Target Type and examine the `Oracle Home` type searches available. Select **Search Oracle Products installed in Oracle homes** and click **Run**.
3. The Search details page is displayed. Note that you can save configuration searches by clicking **Save As** and providing a name.

   The search results are shown at the bottom of the page. Scroll to see all the values.
4. Edit the columns of the search by removing unwanted columns. Refine your search by customizing the Configuration Items. Change the display of the results by navigating to **View > Columns > Manage Columns**. Searches can be saved and also exported to an Excel spreadsheet.

Practices for Lesson 13: Managing Compliance

Overview

Practices for Lesson 13: Overview

Practices Overview

In these practices, you learn about monitoring and managing compliance with business rules. Many compliance rules are predefined in Cloud Control. You can also define your own rules. Compliance rules are grouped together in "compliance standards," which you can assign to a specific target type. After being assigned, compliance is evaluated when there is a configuration change. Compliance standards can be grouped together in "compliance frameworks," which can span multiple target types.

You work as a Super Administrator in these practices. By default, the `emadmin` user has access to the Compliance Framework tabbed page, because it is a Super Administrator. A summary of the tasks is as follows:

- View predefined compliance frameworks, standards, rules, and rule details. If you are already familiar with compliance objects and how to search and review them, consider Lab 13-1 optional and continue with Lab 13-2, "Using Compliance Standards."
- Create a new compliance standard based on **Storage Best Practices for Oracle Database**. Assign both of your database instances to this compliance standard. Then view the compliance evaluation results.

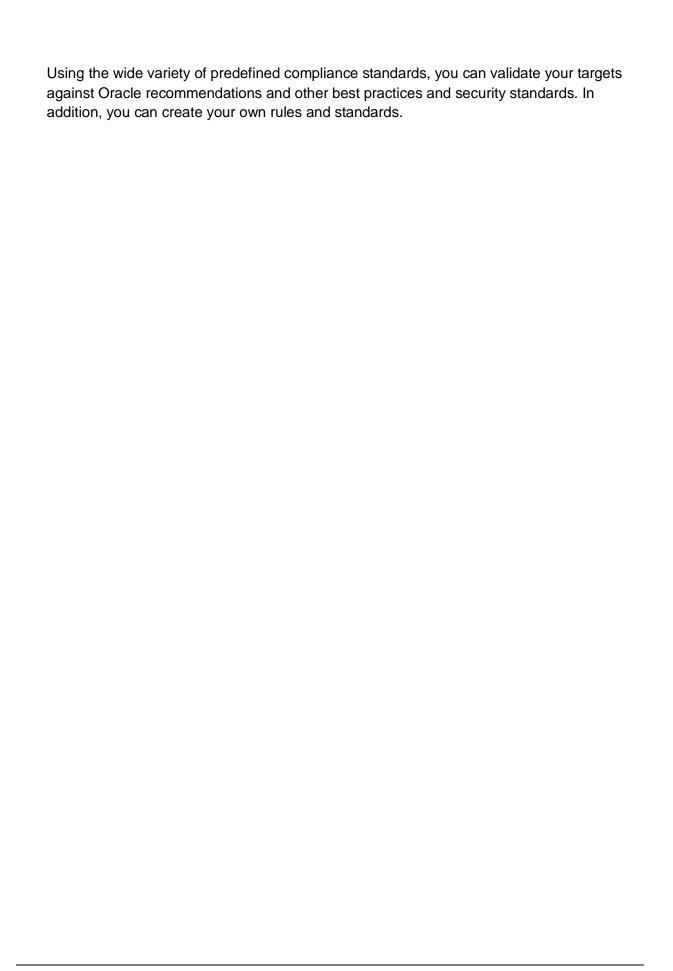## Lab 13-1: Reviewing Predefined Compliance Objects

Overview

In this Lab, you view predefined compliance frameworks, standards, rules, and rule details. If you are already familiar with compliance objects and how to search and review them, consider Lab 13-1 optional. (Continue with Lab 13-2, "Using Compliance Standards.")

Assumptions

- You are logged in to Enterprise Manager Cloud Control as the `emadmin` user.
- You reviewed the "*Oracle Enterprise Manager 12c: Lifecycle Management*" OLL demos or have the equivalent navigation knowledge.

Tasks

1. To review predefined compliance objects, navigate to **Enterprise > Compliance > Library**.

2. The Compliance Library has several tabbed pages. On the Compliance Frameworks tab, select a framework that interests you and click **Show Details**. Note in particular the Oracle-enhanced Security Technical Implementation Guidelines (STIG) frameworks that can be associated with your targets.

3. Expand the hierarchy nodes at several levels and review the descriptions, and then click **Done**.

4. Click the **Compliance Standards** tab. There are quite a few standards, each for a specific target type.

5. Review the predefined standards, select **Storage Best Practices For Oracle Database** (which is applicable to the Database Instance target type), and click **Show Details**. This standard checks for proper storage settings in order to avoid space and performance problems.

6. Expand the hierarchy nodes, if necessary, until you can click **Default Temporary Tablespace Set to a System Tablespace** to view its description.

7. Review any other descriptions that may interest you and then click **Done**.

8. Click the **Compliance Standard Rules** tab.

9. Because there are many rules, use the Search functionality for finding the previously viewed **Default Temporary Tablespace Set to a System Tablespace**. Click the icon to expand the Search options.

10. Enter `%tablespace%` as Rule and click **Search**.

11. Select **Default Temporary Tablespace Set to a System Tablespace**, applicable to **Database Instance**, and click **Show Details**.

12. Scroll to review all details, including the SQL Source of how this rule is checked in the data dictionary.

13. Click **Done** when you finish reviewing the rule details.

Using the wide variety of predefined compliance standards, you can validate your targets against Oracle recommendations and other best practices and security standards. In addition, you can create your own rules and standards.

Lab 13-2: Using Compliance Standards

Overview

In this Lab, you create a new compliance standard based on **Storage Best Practices For Oracle Database**. Assign one of your database instances to this compliance standard. Then view the compliance evaluation results.

Assumptions

You are logged in to Enterprise Manager Cloud Control as the `emadmin` user.

Tasks

1. To assign compliance standards to your database instances, navigate to **Enterprise > Compliance > Library**.
2. Click the **Compliance Standards** tabbed page and then expand the Search field.
3. Select **Database Instance** from the **Applicable To** drop-down menu, enter the keyword `storage`, and click **Search**.
4. Because you want to ensure that there are no unexpected changes coming from predefined standards (which may be updated in the future), you create your own set. Highlight **Storage Best Practices for Oracle Database** and click **Create Like**.
5. Enter `My Storage BP for DB` as Name and click **Continue**.
6. Review the definitions, make modifications if required, and then click **Save** and **OK** in the Information window.
7. Once created, you must associate compliance standards with targets. Select **My Storage BP for DB** and click **Associate Targets**.
8. To associate targets, click **Add**.
9. In the "Search and Select: Targets" window, select the `orcl.us.oracle.com` database instance and click the **Select** button.
10. Click **OK** and **Yes** to confirm association.
11. You should receive the information that the compliance standard is submitted for processing. Click **OK**.
12. To evaluate the compliance standards, navigate to **Enterprise > Compliance > Results**.
13. Question: What is the compliance score for storage best practices in each database? Click a digit under Target Evaluations.
14. You can drill down into the compliance main page to see the **Compliance Results** page.
15. Navigate to **Enterprise > Compliance > Dashboard** for an overview of the compliance status of your entire enterprise.

Practices for Lesson 14: Using the Cloud Control Reporting Framework

Overview

Practices for Lesson 14: Overview

Practices Overview

Oracle Business Intelligence (BI) Publisher is Oracle's primary reporting tool. Oracle BI Publisher offers a variety of report and dashboard layouts, and enables you to create all types of highly formatted documents. Starting with 13c Release 1, Oracle BI Publisher is installed and configured by default on the OMS. For every additional OMS you deploy, you deploy another Oracle BI Publisher by default.

Lab 14-1: Reviewing and Running Oracle-Provided Reports

Overview

In this Lab, you review the Oracle-provided reports and execute the Availability History report for one of your targets. You change the time period to the last seven days.

Assumptions

You are logged in to Enterprise Manager Cloud Control as the `emadmin` user.

Tasks

1. Connect to the `em13c` host as the `oracle` user.
2. Start a terminal session by double-clicking the Terminal icon.
3. Oracle BI Publisher (BIP) is already enabled in your environment, but the services are not running. Start the BIP services:
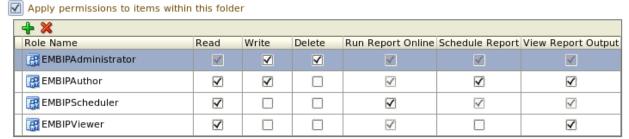
   ```
   [oracle@em13c ~]$ . myomsenv.sh
   [oracle@em13c ~]$ emctl start oms -bip_only
   ```

4. Navigate to **Enterprise** (global menu) **> Reports > BI Publisher Enterprise Reports**. Note all the predefined reports available in Cloud Control.
5. Click any of the reports to see the details. This will open BI Publisher in a new browser tab, and you will need to add an exception for BI Publisher's SSL certificate.
   1) Click **Advanced** on the "Your connection is not secure" page.
   2) Click **Add Exception** beneath the information about the invalid security certificate to display the Add Security Exception dialog box.
   3) Click **Confirm Security Exception** and leave Permanently Store this Exception selected.
   4) The BI Publisher login page will now be displayed.
6. Log in as `emadmin`/<emadmin password> and the report you chose in Enterprise Manager Cloud Control will be displayed.
7. Click the **Catalog** (top right) menu to see all the BIP elements:
   - Predefined reports, under the Enterprise Manager Cloud Control folder
   - Data Models, under the Samples folder
8. Typically, a BIP Administrator will create folders where various users can place their reports.
   a. Click **Shared Folders**. These folders will store reports that other administrators also have access to.
   b. Click the **New** icon and then select **Folder** to create a new folder.
   c. Enter a name for the folder. For example, assume that the `dba1` user will be the one creating your reports, so name it `DBA1 Custom Reports` and then click **Create**.

d. Highlight the new folder you created, and in the bottom-left pane, click **Permissions**.

e. The page should display all available BIP built-in roles. Allow the following access, as an example. Note the **check box** at the very top!

Role Name	Read	Write	Delete	Run Report Online	Schedule Report	View Report Output
EMBIPAdministrator	✓	✓	✓	✓	✓	✓
EMBIPAuthor	✓	✓	☐	✓	✓	✓
EMBIPScheduler	✓	☐	☐	✓	✓	✓
EMBIPViewer	✓	☐	☐	✓	☐	✓

9. Navigate to the **Enterprise Manager Cloud Control** folder**, Availability** reports subfolder, and click the **Availability Report (Target)** `Open` link. This is the availability report for your targets, based on your monitored data. Note the target selection menu at the top. The **EMBIPAdministrator** role is automatically included for Super Administrators, such as the `emadmin` user you are logged in as, to allow initial setup of all BIP administrators. Therefore, you have access to all report tasks (Read, Write, Delete, Run Report Online, Schedule Report, and View Report Output).

10. **Optionally**, sign out of the `emadmin` BIP session and log in as the DBA user you created, `dba1`. Note that no predefined elements or reports are available to you as an administrator with the `DBA_ROLE`. This role has no special BIP privileges.

11. If you have logged in as `dba1`, log out and log back in as `emadmin`. Grant appropriate privileges to your other users. For example, your DBA can have the **EMBIPAuthor** role to create reports and the Junior DBA can be given the **EMBIPScheduler** and **EMBIPViewer** roles. You use the EM CLI interface to grant these privileges.

a. Navigate to your `em13c` host session, logged in as the `oracle` user, and set up EM CLI:

```
[oracle@em13c ~]$ . myomsenv.sh
[oracle@em13c ~]$ emcli login -username="emadmin"
Enter password :
Login successful
```

Note that if you have not logged out from the `emcli` session in a prior exercise, you may still be logged in. In this case, you will receive an error message: "*Error: Already logged in as user "emadmin". Use "emcli logout" to log out the current user.*"

b. Grant the **EMBIPAuthor** privileges to dba1 and the **EMBIPScheduler** and **EMBIPViewer** privileges (in order to view reports to be scheduled) to jr_dba1.

```
[oracle@em13c ~]$ emcli grant_bipublisher_roles -
roles="EMBIPAuthor" -users="dba1"
EMBIPAuthor role successfully granted to dba1


[oracle@em13c ~]$ emcli grant_bipublisher_roles -
roles="EMBIPScheduler;EMBIPViewer" -users="jr_dba1"
EMBIPScheduler role successfully granted to jr_dba1
EMBIPViewer role successfully granted to jr_dba1
```

c. Check the roles you have granted and then log out:

```
oracle@em13c ~]$ emcli list_bipublisher_roles -user="dba1"
The user "dba1" has the following roles granted:
EMBIPAuthor


[oracle@em13c ~]$ emcli list_bipublisher_roles -user="jr_dba1"
The user "jr_dba1" has the following roles granted:
EMBIPScheduler
EMBIPViewer


[oracle@em13c ~]$ emcli logout
Logout successful
```

d. Back in your browser session, log out of the BIP emadmin session (top right) and log back in to the administrator dba1. You now have the **EMBIPAuthor** role. Note this time that all folders that include the data models and all options for authoring/creating reports are available to you.

Lab 14-2: Editing a Report with BI Publisher

Overview

In this Lab, you edit a report as an administrator that has the **EMBIPAuthor** privileges**.**

Assumptions

You are logged in to BI Publisher as the `dba1` user.

Tasks

1. To edit an existing report, navigate to the **Catalog Folders > Enterprise Manager Cloud Control** folder:

    Browse/Manage ...
    📁 Catalog Folders
    📇 Report Jobs
    📑 Report Job History

    Note that if you do *not* see the shared folder, it means that the permissions were not given as directed in the first Lab.

2. In the Availability reports subfolder, highlight the Availability Report (Target).

3. Click the **Copy** icon 📋 located in the top menu.

4. Navigate to the **Shared Folders** main folder and then **DBA1 Custom Reports**, and now click the **Paste** icon. A copy of the Availability report should be placed in that folder, with a "Created by dba1" label. Note that you do *not* have permissions to delete items from this folder.

5. Click **Open** to view the report. Toggle between the various targets from the top menu.

6. Back in the **Catalog > DBA1 Custom Reports** folder, click the **More > Rename** menu of the report you copied. Give your report a new name: `Custom Database Availability Report` and click **Rename**.

7. Next, click **Edit**. Then click **Parameters** (top right) 🔤 Parameters and edit some parameters to enable better defaults for this report and administrators that have access to it.

8. Change the **Select Target** label to have `orcl.us.oracle.com` as the default value and **Timezone** as `America/Anchorage (CAPT)`. Click **OK**.

9. Click **View Report** (top right) 🖼️ View Report to view the report again. Does it run correctly?

10. Sign out of the `dba1` session (top right).

Lab 14-3: Scheduling a Report with BI Publisher

Overview

In this Lab, you schedule a report as an administrator that has the **EMBIPScheduler** privileges.

Assumptions

You are not logged in to BI Publisher.

Tasks

1. Log in to BI Publisher as the `jr_dba1` user.
2. Navigate to **Catalog Folders** (main folder) and then **DBA1 Shared Reports**.
    Note that if you do *not* see the shared folder, it means that the permissions were not given as directed in the first Lab.
3. Locate the report created by the `dba1` user and click **More**. Are any of those tasks enabled? All the tasks available to you are *Open, Schedule, Jobs*, and *Job History*. You do not have privileges to perform any other tasks.
4. Click **Schedule**. Review the General default parameters.
5. Click the **Output** tab and make the output **Public**.
6. On the **Schedule** tab, select the option to run it now.
7. Examine the **Notification** tab. Notifications are not set up on this system, but when they are set up, you can choose to Email or FTP this report as soon as it is run.
8. Click **Submit**, enter a Job **Name**, and click **OK**.
9. Click **OK** and then **Return** to go back to the report main page.
10. Active report jobs can be viewed from the Report Jobs menu. When they complete, the status of the report jobs is available from the **Job History** menu. Click it now.
11. Click the **name** of your job report. Note that you can review the output and you can also choose to send this report to Email, Printer, Fax, or Web Folder, if these were set up by your administrator.
12. Sign out of your `jr_dba1` session.

    Ensure that you watch the Oracle Enterprise Manager Cloud Control 13*c* BI Publisher video series for details on how to create a custom report.

Practices for Lesson 14: Using the Cloud Control Reporting Framework