



Integrated Cloud Applications & Platform Services



Using Oracle Enterprise Manager Cloud Control 13c

Student Guide

D92199GC20

Edition 2.0 | August 2017 | D100889

Learn more from Oracle University at education.oracle.com

Author

Lachlan Williams

Editors

Nikita Abraham
Arijit Ghosh

Graphic Designers

Prakash Dharmalingam
Seema Bopiah

Publishers

Raghunath M
Giri Venugopal
Asief Baig
Srividya Rameshkumar

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Disclaimer

This document contains proprietary information and is protected by copyright and other intellectual property laws. You may copy and print this document solely for your own use in an Oracle training course. The document may not be modified or altered in any way. Except where your use constitutes "fair use" under copyright law, you may not use, share, download, upload, copy, print, display, perform, reproduce, publish, license, post, transmit, or distribute this document in whole or in part without the express authorization of Oracle.

The information contained in this document is subject to change without notice. If you find any problems in the document, please report them in writing to: Oracle University, 500 Oracle Parkway, Redwood Shores, California 94065 USA. This document is not warranted to be error-free.

Restricted Rights Notice

If this documentation is delivered to the United States Government or anyone using the documentation on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS

The U.S. Government's rights to use, modify, reproduce, release, perform, display, or disclose these training materials are restricted by the terms of the applicable Oracle license agreement and/or the applicable U.S. Government contract.

Trademark Notice

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

Contents

1 Introduction

- Course Goals 1-2
- Objectives 1-3
- What Is Enterprise Manager Cloud Control 13c? 1-4
- Why Do I Need Enterprise Manager Cloud Control 13c? 1-5
- Who Can Use Enterprise Manager Cloud Control? 1-6
- Enterprise Manager Cloud Control 13c Features 1-7
- Single Pane of Glass for Enterprise Management 1-9
- Course Schedule 1-10
- Classroom Setup 1-11
- Summary 1-12
- Practice 1-1 Overview: Checking the Virtual Environment 1-13
- Practice 1-2 Overview: Getting to Know Your Oracle Software Classroom Environment 1-14

2 Cloud Control Core Concepts

- Objectives 2-2
- Cloud Control Components 2-3
- Cloud Management: Hybrid Cloud 2-5
- Communication Between Components 2-6
- Oracle Management Service 2-8
- Discovery: What Is Host Discovery? 2-10
- Manual Discovery: How Do Hosts Become Managed Hosts? 2-11
- What Is Target Discovery? 2-12
- How Do Targets Become Managed Targets? 2-13
- Examples of Managed Target Types 2-14
- Oracle Management Repository 2-15
- Software Library 2-16
- EM Command-Line Interface 2-17
- Monitoring: Key Functionality 2-18
- Other Monitoring and Management Functionality 2-19
- Security: Overview 2-20
- Summary 2-21
- Practice 2-1 Overview: Accessing Enterprise Manager Cloud Control 2-22

Practice 2-2 Overview: Monitoring and Managing Cloud Control 2-23
Practice 2-3 Overview: Monitoring the Cloud Control Host 2-24

3 Organizing Targets

Objectives 3-2
Organizing Targets into Groups 3-3
Why Use Groups? 3-4
Understanding Properties of Targets 3-5
Cloud Control Group Types 3-6
Which Groups Should I Use? 3-7
Designing Target Groupings 3-8
Working with Dynamic Groups 3-9
Working with Administration Groups: Overview 3-10
Comparing Group Characteristics 3-12
Populating Groups: Best Practices 3-13
Quiz 3-14
Summary 3-16
Practice 3-1 Overview: Organizing Your Targets: Administrative Groups 3-17
Practice 3-2 Overview: Organizing Your Targets: Non-Privilege-Propagating Groups 3-18
Practice 3-3 Overview: Discovering Additional Targets 3-19

4 Oracle Cloud in Your IT Ecosystem

Objectives 4-2
Oracle Cloud as Part of Your IT Ecosystem 4-3
Tools for Monitoring and Managing Oracle Cloud Services 4-4
Why Use Cloud Control to Manage Oracle Cloud Services? 4-5
How Cloud Control Monitors and Manages Oracle Cloud Services 4-6
How to Get Past the Firewalls That Protect You 4-7
The Hybrid Cloud Agent: An Elegant Solution 4-8
Under the Covers of the Hybrid Cloud Agent 4-9
What the Hybrid Cloud Agent Enables 4-10
Summary 4-11

5 Cloud Control Access

Objectives 5-2
Designing Cloud Control Access 5-3
How Authentication Works in Cloud Control 5-4
Cloud Control Administrators 5-5
Cloud Control Authentication Options 5-6
How Authorization Works in Cloud Control 5-7

Privileges	5-8
Roles	5-9
Private Roles Versus System Roles	5-10
Who Can Create Roles?	5-11
Privileges and Roles: Best Practices	5-12
Cloud Control Initial Access: Best Practices	5-13
Managing Securely with Credentials	5-14
Target Authentication	5-15
Target Access Using Credentials	5-16
Preferred Credentials	5-18
Global Preferred Credentials	5-19
Correlating Administrators, Roles, and Groups	5-20
Correlating Administrators and Target Credentials	5-21
Quiz	5-23
Summary	5-25
Practice 5-1 Overview: Creating Roles and Administrators	5-26
Practice 5-2 Overview: Creating Named and Default Credentials	5-27
Practice 5-3 Overview: Performing DBA Role Tasks: View Host Targets, Set Backup and Recovery Parameters, and Back Up a Tablespace	5-28
Practice 5-4 Overview: Performing Tasks as a Junior DBA Administrator: View Targets and Privileges	5-29

6 Monitoring

Objectives	6-2
Cloud Control Monitoring: Overview	6-3
Enterprise Monitoring with Cloud Control	6-4
Always-On Monitoring	6-5
Defining Monitoring Standards	6-6
Using Administration Groups for Monitoring	6-7
Concept: Metrics and Metric Thresholds	6-8
Customizing Metric Settings	6-9
Concept: Monitoring Templates and Template Collections	6-11
Using Monitoring Templates and Template Collections	6-12
Example of Template Modifications	6-14
Keeping Targets and Templates Synchronized	6-15
Administration Groups and Template Tasks Prerequisite Privileges	6-16
Extending Your Monitoring Scope	6-17
Developing and Deploying Metric Extensions	6-18
Securely Dividing Metric Extension Tasks	6-19
Quiz	6-20
Summary	6-22

Practice 6-1 Overview: Reviewing the Oracle-Provided Monitoring Templates	6-23
Practice 6-2 Overview: Creating a Monitoring Template	6-24
Practice 6-3 Overview: Applying a Monitoring Template Using a Template Collection	6-25

7 Managing Events and Incidents

Objectives	7-2
Goals of Incident Management	7-3
Understanding Events	7-4
Understanding Incidents	7-5
Distinguishing Between Incidents and Events	7-6
Example: Incident with One Event	7-7
Example: Incident with Multiple Events	7-8
Understanding Problems	7-9
Monitoring Oracle Software Problems	7-10
Example: ADR Incidents and Cloud Control Problems	7-11
Enterprise View of Incident Manager	7-12
Performing Incident Lifecycle Operations	7-13
Who Can Use Incident Manager?	7-14
Quiz	7-15
Summary	7-17
Practice 7-1 Overview: Preparing an Incident	7-18
Practice 7-2 Overview: Finding and Resolving an Incident	7-19

8 Responding to Events, Incidents, and Problems

Objectives	8-2
Why Do You Need Incident Rules?	8-3
What Is an Incident Rule?	8-4
Defining Rules	8-5
Rule Sets	8-6
Setup of Notifications	8-7
Prioritization of Rules and Notifications	8-8
Best Practices for Using Incident Rule Sets	8-9
Rule Set: Example	8-10
Corrective Actions	8-11
Defining and Using Corrective Actions	8-12
Using Blackouts	8-13
Using Notification Blackouts	8-14
Quiz	8-15
Summary	8-17
Practice 8-1 Overview: Creating a Corrective Action	8-18

Practice 8-2 Overview: Creating a Rule Set 8-19

Practice 8-3 Overview: Observing How a Rule Set Is Applied 8-20

9 Using the Job System

Objectives 9-2

What Is a Job? 9-3

How Do Jobs Work in Cloud Control? 9-4

Job Elements 9-5

Job Executions and Job Runs 9-6

Defining Jobs 9-7

Using Predefined Jobs 9-8

Job System Chef-Solo Support 9-9

Job Interfaces in Cloud Control 9-10

Creating Jobs 9-11

Creating a Multitask Job 9-12

Details of a Multitask Job 9-13

Reviewing Job Execution Results 9-14

Performing Job Operations 9-16

Jobs and Groups 9-18

Job Events 9-19

Jobs Privileges 9-20

Enterprise Level: Monitoring Jobs and Job System Status 9-21

Quiz 9-22

Summary 9-24

Practice 9-1 Overview: Creating and Executing a Simple SQL Job 9-25

Practice 9-2 Overview: Creating and Executing OS Jobs on Multiple Targets 9-26

Practice 9-3 Overview: Creating a Multitask Job (Optional) 9-27

10 Managing Systems and Services

Objectives 10-2

Systems and Services 10-3

Example: System and Service 10-4

Creating a Generic System 10-5

Using the System Home Page 10-6

Other System Views 10-7

Defining Services 10-8

Understanding Service Types 10-9

Defining the Availability of a Generic Service 10-10

Defining a Service Test 10-11

Using Beacons 10-12

Defining a Web Transaction Service Test 10-13

Defining Service Performance	10-14
Defining and Monitoring Usage Metrics	10-15
Viewing Additional Service Information	10-16
Defining Service Level Rules	10-17
Specifying Service Level Rule Elements	10-18
Using Root Cause Analysis (RCA)	10-19
Creating a Generic Service: Sample Wizard	10-20
Viewing the Service Topology	10-21
Example: Implementing Systems and Services	10-22
Quiz	10-23
Summary	10-25
Practice 10-1 Overview: Reviewing Existing Systems and Services	10-26
Practice 10-2 Overview: Creating a System	10-27
Practice 10-3 Overview: Creating a Generic Service	10-28
Practice 10-4 Overview: Monitoring the Availability of a Web Application	10-29
Practice 10-5 Overview: Creating and Testing a Web Transaction	10-30

11 Patching and Provisioning

Objectives	11-2
Software Lifecycle Management	11-3
Software Lifecycle Management Requirements	11-4
Configuring the Software Library: Review	11-6
Provisioning Elements	11-7
Provisioning Specific Roles and Privileges	11-8
Bare Metal or OS Provisioning	11-9
Database Software Provisioning Workflow	11-10
Deployment Procedures for Provisioning and Patching Automation	11-11
Deployment Procedures: Properties	11-12
Deployment Procedures: Phases and Steps	11-13
Examples of Customized Deployment Procedures	11-15
Software Patching	11-17
Patching Workflow	11-18
Software Patching Modes	11-20
Out-of-Place Patching	11-21
Patching Rollout Cycles Using Templates	11-22
Oracle Database Software Upgrades	11-23
Oracle Database Software Upgrades: Using Breakpoints	11-24
Quiz	11-25
Summary	11-27
Practice 11-1 Overview: Preparing for Offline Patching	11-28
Practice 11-2 Overview: Patching Offline	11-29

12 Managing Configurations

- Objectives 12-2
- What Is Configuration Management? 12-3
- Configuration Management 12-4
- Examples of Configuration Information 12-5
- Comparing Configurations 12-6
- Searching the Enterprise Configuration 12-7
- Types of Enterprise Configuration Searches 12-8
- Drift and Consistency Management 12-9
- Change Activity Planner 12-10
- Quiz 12-11
- Summary 12-13
- Practice 12-1 Overview: Viewing Configuration Details 12-14
- Practice 12-2 Overview: Viewing Configuration History and Topology 12-15
- Practice 12-3 Overview: Comparing Configurations and Managing Drift 12-16
- Practice 12-4 Overview: Searching Configurations 12-17

13 Managing Compliance

- Objectives 13-2
- Compliance: Overview 13-3
- Understanding Compliance Management 13-4
- Understanding Compliance Standards 13-5
- Understanding Compliance Standard Rules 13-6
- Implementing Compliance Management 13-7
- Understanding Compliance Measurement 13-9
- Score and Its Factors 13-10
- Accessing the Compliance Library 13-11
- Associating Targets to Compliance Standards 13-12
- Investigating Compliance Violations 13-13
- Viewing Compliance Evaluation Results 13-14
- Viewing Compliance Scores 13-15
- Viewing Out-of-the-Box Compliance Reports: Dashboard 13-16
- Quiz 13-17
- Summary 13-19
- Practice 13-1 Overview: Reviewing Predefined Compliance Objects 13-20
- Practice 13-2 Overview: Using Compliance Standards 13-21

14 Using the Cloud Control Reporting Framework

- Objectives 14-2
- Introduction to BI Publisher 14-3
- BI Publisher Configuration with Enterprise Manager 14-4

- BI Publisher Access 14-5
- Reporting on Targets 14-6
- BI Publisher Elements 14-7
- Report Definitions 14-8
- Running and Scheduling Reports: Workflows 14-9
- Creating Custom Reports: Workflow 14-10
- Scheduling Reports 14-11
- Reports Output Options 14-12
- Oracle-Provided Reports 14-13
- Quiz 14-14
- Summary 14-16
- Practice 14-1 Overview: Reviewing and Running Oracle-Provided Reports 14-17
- Practice 14-2 Overview: Editing a Report with BI Publisher 14-18
- Practice 14-3 Overview: Scheduling a Report with BI Publisher 14-19

Introduction

ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Course Goals

After completing this course, you should be able to:

- Use Cloud Control to organize your managed enterprise
- Describe roles and privileges
- Monitor the overall performance and health of your managed system
- Manage incidents and set up notifications
- Use the Job System to automate commonly performed tasks
- Patch and provision new systems
- View, search, and compare configurations
- Explain compliance policies and evaluate policy violations
- Create and use Cloud Control reports



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

This course is designed to show IT administrators various Enterprise Manager Cloud Control features that will enable them to be successful in their jobs.

In this course, you learn to use the core functionality of Oracle Enterprise Manager Cloud Control 13c. After a brief review of the underlying architecture, you use Cloud Control to manage an enterprise-computing environment. This includes tasks such as managing and monitoring Cloud Control; creating and managing groups, systems, and services; monitoring targets; using the Job System and the reporting system; viewing and comparing configurations; and managing compliance.

Hands-on practices help students learn how to use the robust features of Cloud Control to manage, monitor, and administer their data center.

This course is not intended to train you in detail about how to administer the individual target types or the Cloud solutions in general. For courses that cover the administration and monitoring of various Oracle target types presented in this course, see the Oracle University website at <http://education.oracle.com>.

Objectives

After completing this lesson, you should be able to:

- Describe Enterprise Manager Cloud Control as a single point of management and explain the benefits it provides
- Describe the course structure and its relationship with other courses
- Explain the system configuration for the course practices



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

What Is Enterprise Manager Cloud Control 13c?

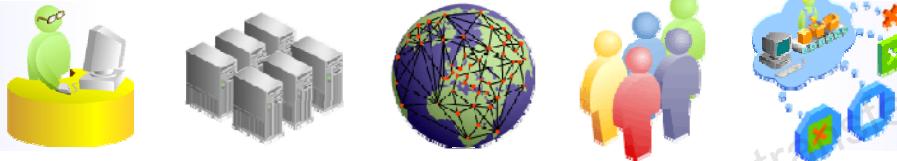
- An on-premises management platform
- Provides management and automation support for Oracle products:
 - Applications
 - Databases
 - Middleware
 - Hardware and engineered systems
- Private cloud and Oracle Cloud management
- Separation of duties through user roles and privileges
- Third-party product management via vendor plug-ins



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Why Do I Need Enterprise Manager Cloud Control 13c?

- Administering hardware from different manufacturers and a variety of operating systems
- Maintaining patch levels and meeting compliance standards
- Monitoring application as well as hardware performance
- Managing on-premises and cloud-based systems and services
- Responding to alerts and incidents
- Satisfying and anticipating the needs of operators, business owners, and end users



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The Trials and Tribulations of a Modern IT Administrator

Unlike the early days of computing when an IT administrator could stand in a machine room and view their entire IT infrastructure in a single glance, modern IT administrators find themselves confronted with challenges every working hour:

- Geographically distributed data centers, including co-locations
- A mixture of hardware brands and architectures
- A mixture of operating systems and versions
- Bespoke applications, off-the-shelf applications, customized applications, cloud applications and services, and associated integrations
- Meeting service-level agreements with both internal and external parties
- Complying with internal and external regulations
- Managing the latest technologies whilst maintaining legacy systems
- Applying appropriate monitoring to new systems and services
- Reporting back to end users, business owners, and other interested parties
- Providing a highly available monitoring and management tool that allows delegated management

Who Can Use Enterprise Manager Cloud Control?

- Operators
- System administrators
- Database and Middleware administrators
- Business intelligence reporters
- Self-service users
- Whoever you allow to log in



ORACLE

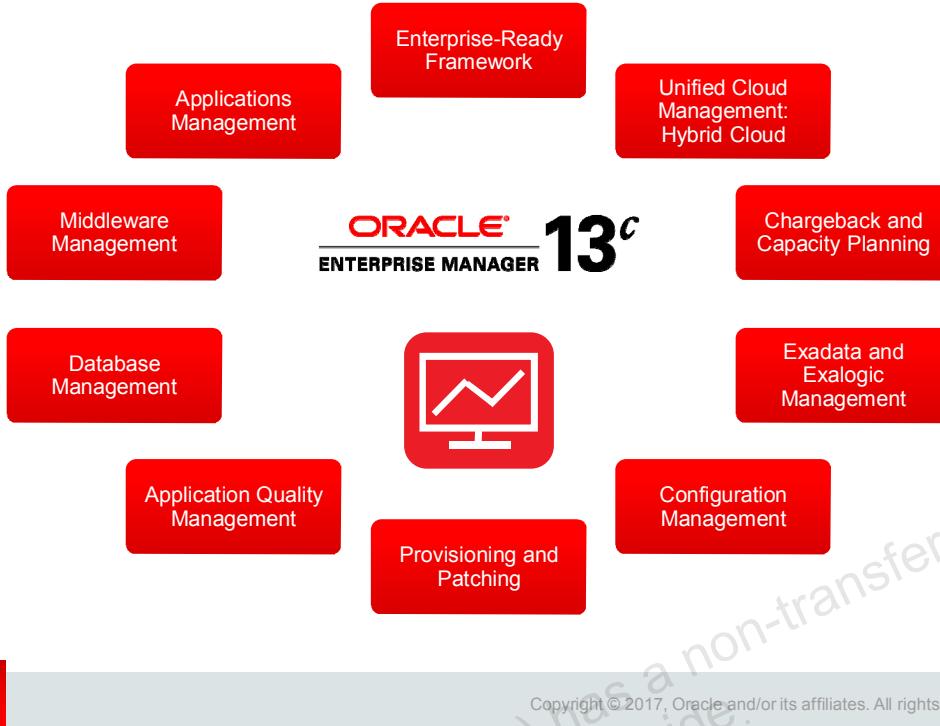
Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

You Build It and They will Come

An Enterprise Manager Cloud Control 13c rollout should be planned and take into account the needs and use-cases of potential users across the organization. For example:

- Operations
 - Manage and monitor hardware and applications
- System administrators
 - Provisioning and compliance management
 - Incident management
- Database and Middleware administrators
 - Platform lifecycle management
 - Lift-and-shift load between on-premises and Oracle Cloud
- Business reporting
 - Infrastructure inventory, chargeback, and more
- Self-service users
 - Developers, testers, and others who use your private on-premises clouds
- Whoever you allow to log in
 - Anyone you deem has a legitimate need to use Enterprise Manager Cloud Control

Enterprise Manager Cloud Control 13c Features



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Key objectives in the design of Enterprise Manager Cloud Control 13c include:

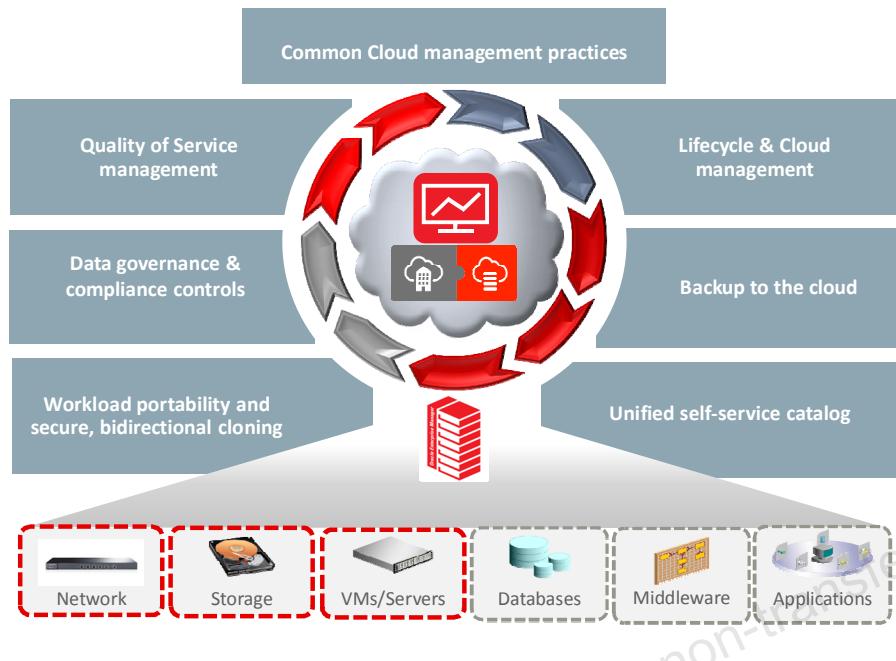
- Providing a complete integrated cloud management solution for a combination of on-premises cloud configurations and Oracle Cloud Services solutions (Hybrid Cloud)
- Delivering enhanced engineered systems management
- Enhancing middleware and database management
- Maintaining a robust, cloud-scale platform

Enterprise Manager Cloud Control 13c includes the following features:

- **Enterprise-Ready Framework:** Provides modular and extensible architecture, self-updateable entities, centralized incident management, in-context diagnostics management, as well as flexible job scheduling and security sub-systems
- **Cloud Management:** Provides complete cloud lifecycle management for both on-premises clouds and PaaS services on Oracle Cloud
- **Chargeback and Capacity Planning:** Provides chargeback based on target types, and uses Automatic Workload Repository (AWR) Warehouse to consolidate AWR reports from multiple databases across the enterprise
- **Exadata and Exalogic Management:** Provides an integrated view of the hardware and software in an Exadata machine, and complete lifecycle management for Exalogic systems
- **Configuration and Management:** Provides an integrated set of tools, agent-less discovery, integration with My Oracle Support, and custom configuration capabilities

- **Provisioning and Patching:** Provides profiles for provisioning known configurations, user-defined deployment procedures, and a Software Library integrated with self-updating capabilities
- **Application and Quality Management:** Provides Database Replay, Application Server Replay, Real Application Testing integrated with Data Masking, and test database management that includes Application Data Model
- **Database Management:** Provides management of Oracle Database systems, including performance management and change lifecycle management
- **Middleware Management:** Provides complete management of Middleware systems
- **Applications Management:** Provides management of Fusion Applications

Single Pane of Glass for Enterprise Management



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

One Management Tool to Oversee Them All

Enterprise Manager Cloud Control 13c has capabilities to intelligently manage traditional and cloud-based services, mitigating the need to use multiple management and monitoring tools for what were previously two disparate environments.

- Complete solution for management of the Oracle stack, including engineered systems, with real-time integration of Oracle's knowledge base with customer environments
- End-to-end performance management and automation
- Integrated Ops Center functionality to monitor and manage both hardware and software from a single interface
- Common management practices applicable to on-premises targets and Oracle Cloud targets
- Quality of Service (QoS) management to ensure delivery of the best service possible to internal and external customers
- Lifecycle and cloud management for simplified provisioning and patching of applications and platforms
- Data governance and compliance controls for conforming with internal and external standards and requirements
- Ability to back up to the cloud to leverage the Oracle Cloud capacity
- Hybrid cloud option to move workloads and clone targets between on-premises and Oracle Cloud

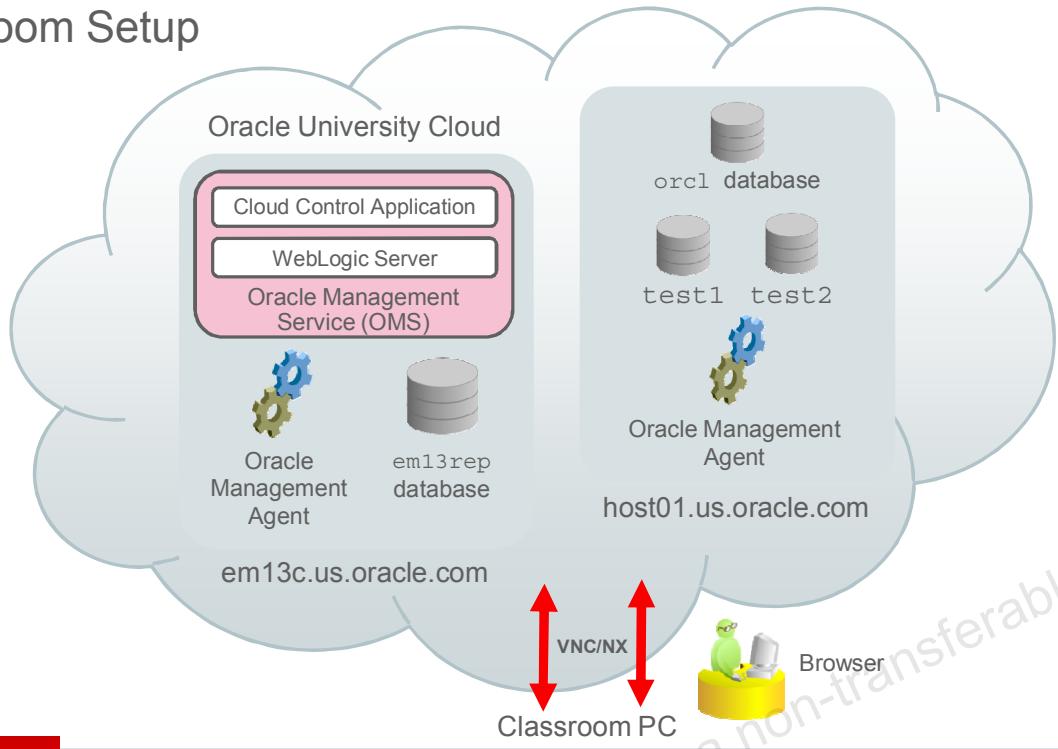
Course Schedule

Day	Lessons
1	1. Introduction 2. Cloud Control Core Concepts 3. Organizing Targets: Groups 4. Oracle Cloud in Your IT Ecosystem 5. Cloud Control Access: Roles, Privileges, and Credentials
2	6. Monitoring: Design and Setup 7. Managing Events and Incidents 8. Responding to Events, Incidents, and Problems 9. Using the Job System 10. Managing Systems and Services
3	11. Patching and Provisioning 12. Managing Configurations 13. Managing Compliance 14. Using the Cloud Control Reporting Framework



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Classroom Setup



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The classroom setup (as shown in the slide) provides each student with access to the following:

- A desktop that is used to access a virtual environment set up in the Oracle University Cloud
- A virtual Linux host that has the Cloud Control installation, including the central Oracle Management Agent, the Oracle Management Service, and the Oracle Management Repository
- A second virtual Linux host that contains sample targets, Oracle databases, and a management agent

Cloud Control is accessed via a browser running on one of the virtual hosts.

Summary

In this lesson, you should have learned how to:

- Describe Enterprise Manager Cloud Control as a single point of management and explain the benefits it provides
- Describe the course structure and its relationship to other courses
- Explain the system configuration for the course practices



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Practice 1-1 Overview: Checking the Virtual Environment

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



Practice 1-2 Overview: Getting to Know Your Oracle Software Classroom Environment

In this practice, you get to know your Oracle software environment by examining your host machines.



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Cloud Control Core Concepts

ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Objectives

After completing this lesson, you should be able to:

- Confirm your understanding of the Cloud Control architecture
 - Describe the different components and subsystems of Cloud Control
 - Explain the architecture of Cloud Control, including the security model
 - List the target types managed by Cloud Control
- Explore the Enterprise Manager interface



ORACLE

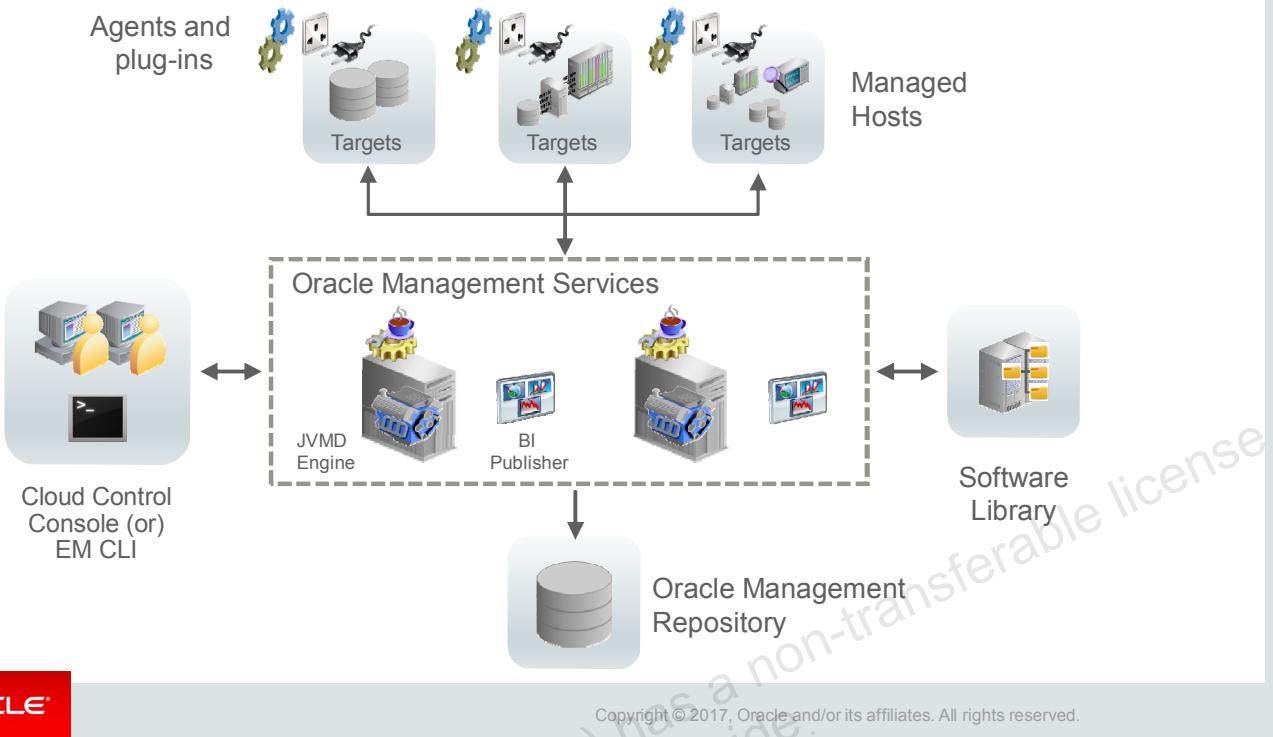
Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

This lesson is a review of the Oracle Enterprise Manager Cloud Control concepts.

Note that installation, configuration, and architecture of the Cloud Control system are covered in detail in the following courses:

- Oracle Enterprise Manager Cloud Control 13c: Install and Upgrade
- Oracle Enterprise Manager Cloud Control 13c: Advanced Configuration Workshop (focused on High Availability configuration)

Cloud Control Components



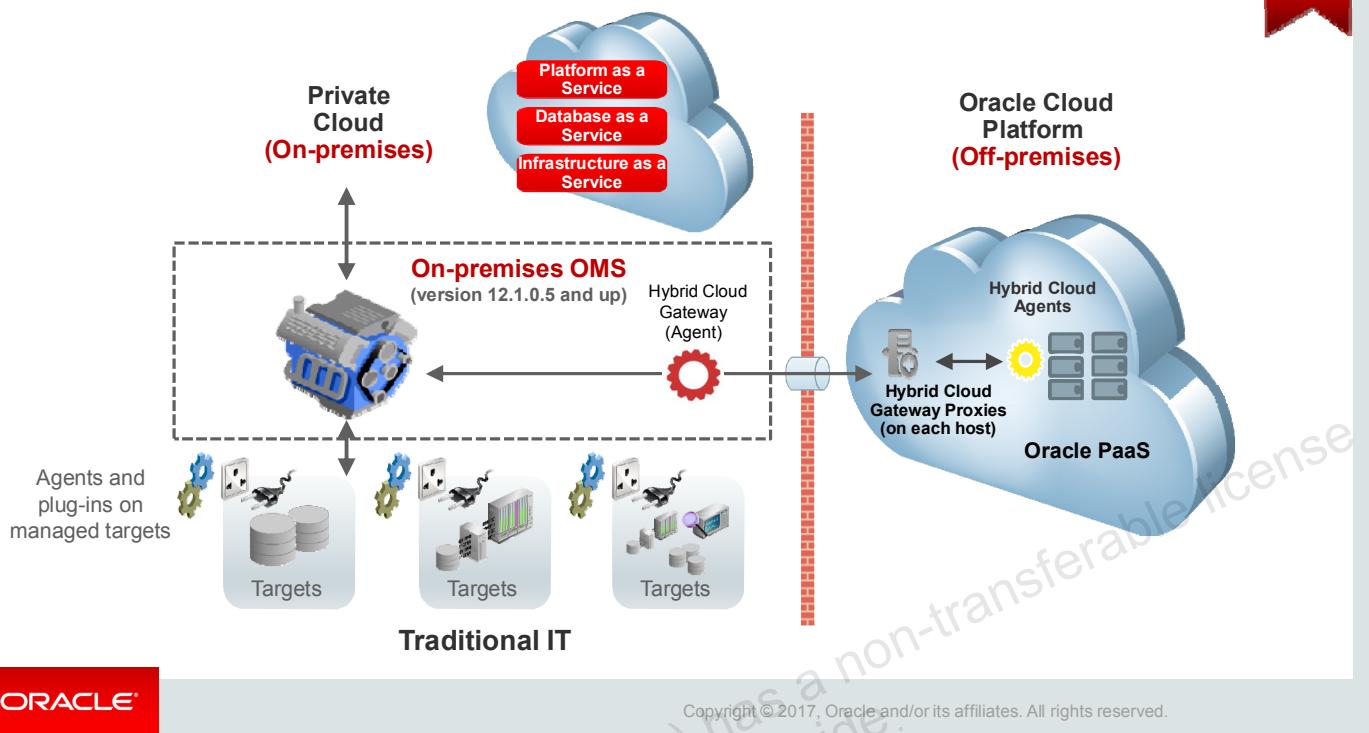
ORACLE

For traditional IT management, a Cloud Control platform includes the following main components:

- The Oracle Management Service (**OMS**), or a collection (pool) of multiple OMSs, is the central processing component of Cloud Control. Depending on the version of the OMS, this component may include a Java VM Diagnostics (**JVMD**) **Engine** and the Business Intelligence Publisher (**BIP**) for reporting. Other characteristics include:
 - J2EE applications deployed on Oracle WebLogic Server that process management and monitoring data, schedule jobs, and send notifications
 - Components called **plug-ins** that handle target management
- The Oracle Management **Repository** (**OMR**), an Oracle database that has the following characteristics:
 - A persistent store of enterprise metadata and management data
 - A schema in an Oracle database
 - Schema objects belonging to the *sysman* user

- Managed **hosts** (servers in your network) that form your IT infrastructure
- Oracle Management Agents (simply called **agents**) with target-specific **plug-ins** reside on each managed host. For Java diagnostics, Java VM (**JVM**) **agents** may exist on these hosts (not illustrated). The JVMD Engine processes the information gathered by JVM agents. Agents:
 - Are Java applications
 - Are installed in their own ORACLE_HOME (unless you are using a shared NFS-mounted agent binaries location), one agent installation per host or OS deployment
 - Use **plug-ins** to discover, monitor, and manage the targets running on a host
 - Collect monitoring and configuration data from managed **targets** and upload it to OMS
 - Execute tasks on behalf of Cloud Control users
- Managed **targets** reside on managed hosts and form your platforms, applications, and other nonhost infrastructure. Agents gather metric data as well as availability, configuration, and performance data for targets on those hosts. Targets are managed by Cloud Control using **plug-ins**. One or more targets may be running on a host and be managed by one agent. Each agent plug-in is specific to a particular target type and offers special management capabilities customized to suit that target type.
- **Software Library**, a file system for storing patches, provisioning profiles, gold images, and so on
- User interfaces:
 - Browser-based Enterprise Manager Cloud Control **Console**
 - Enterprise Manager Command Line Interface (**EM CLI**)

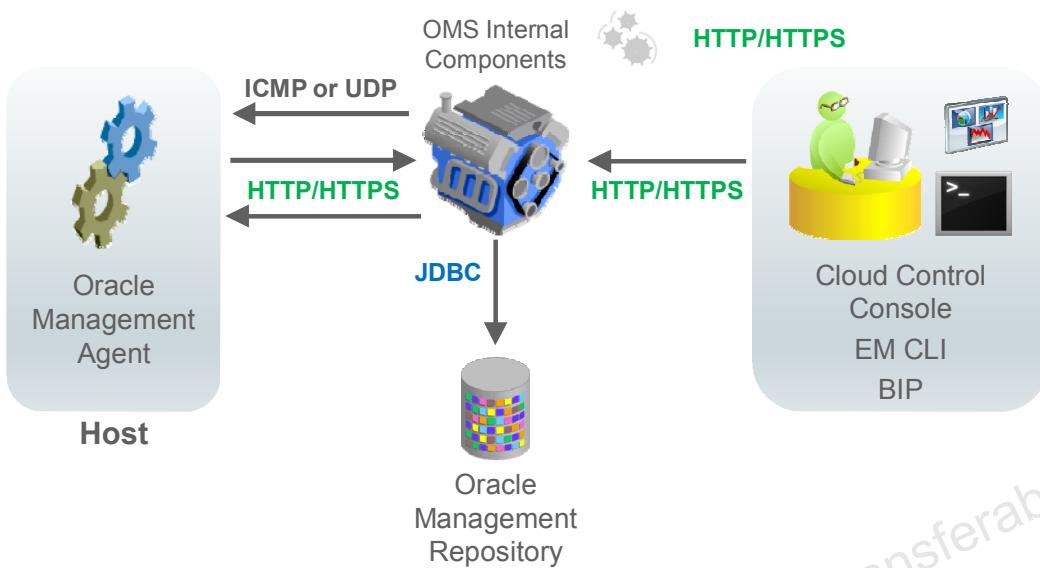
Cloud Management: Hybrid Cloud



Along with traditional IT environments, Enterprise Manager Cloud Control manages **Cloud** environments. Starting with 12.1.0.5 and up, in addition to **Private Cloud** environments, these can now be a combination of Private Cloud and the Oracle Cloud Platform (**Public Cloud**), which together form a Hybrid Cloud environment.

A Hybrid Cloud Gateway, essentially a converted cloud control agent, handles all communication between the on-premises Cloud Control and the Public Cloud. Hybrid Cloud Agents, configured on the Public Cloud, communicate to the Hybrid Cloud Gateway via local proxy processes (one on each Cloud host) and hence communicate with the on-premises OMS.

Communication Between Components



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The communication flow between the Cloud Control components is illustrated in the slide. Note that only the communication between the agent and the OMS is two-way. All the communication port values are assigned during installation, either by the installer as it searches for available ports or explicitly by you. You can also change ports after installation.

- The agent uploads data to the OMS via HTTP on a port in the range 4889 to 4898 or via HTTPS on port 1159 or a port in the range 4899 to 4908. This communication is designed to work across wide-area networks, so a low-bandwidth connection is acceptable.
- The OMS communicates with the agent via HTTP or HTTPS, depending on whether the agent is unsecured or secured respectively, on port 3872 or a port in the range 1830 to 1849.
- The OMS communicates with the OMR via JDBC on port 1521. The OMS and the OMR must be close together and have a good bandwidth, low-latency connection.
- Cloud Control Console users access the Cloud Control webpages via HTTPS on a port in the range 7799 to 7809 or via HTTP on a port in the range 7788 to 7798.
- BI Publisher communicates via HTTP by default on port 9701 or ports in the range 9701 to 49152.
- BI Publisher communicates via HTTPS by default on port 9702 or ports in the range 9701 to 49152.

Where applicable, the default and recommended protocol is HTTPS for **secure** communications between components.

Cloud Control also uses the Internet Control Message Protocol (ICMP) and User Datagram Protocol (UDP) to transfer some data between monitored components. ICMP is also used by OMS to directly communicate with a host if the agent is unavailable and validate if the host (server) is up or down.

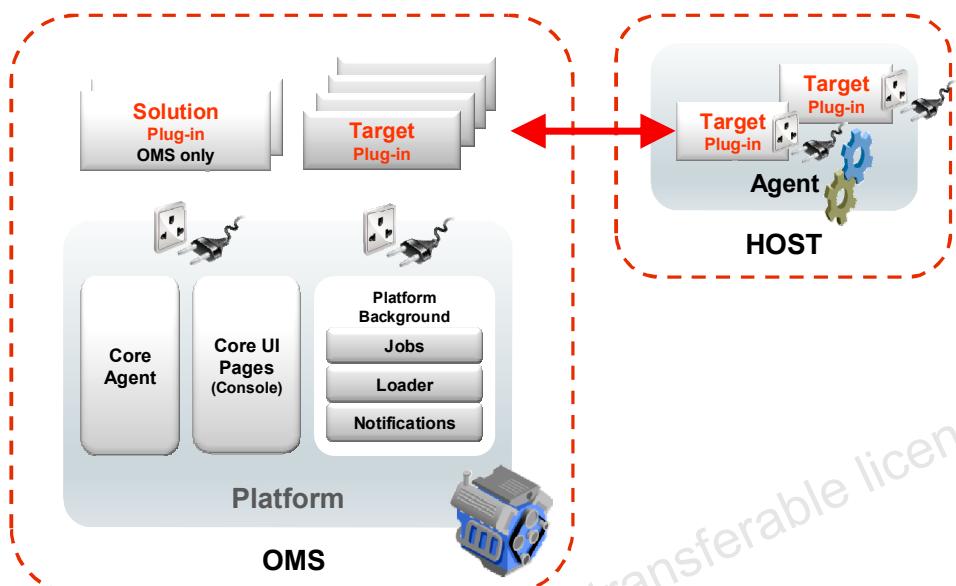
A number of other components internal to the OMS, or other optionally configured components, communicate via HTTP/HTTPS and use additional ports. Here are some examples:

- WebLogic Admin Server, default port 7101, range 71017 to 7200
- EM Domain WebLogic Managed Server HTTP, default port 7201, range 7201 to 7300
- EM Domain WebLogic Managed Server HTTPS, default port 7301, range 7301 to 7400
- Node Manager HTTPS, default port 7401, range 7401 to 7500

Knowing the ports used in your Cloud Control installation is important, especially if you are managing hosts behind firewalls or where other network restrictions apply.

Oracle Management Service

- Serves the core UI pages
- Handles jobs, notifications, and data loading
- Discovers hosts
- Contains plug-ins that provide target management and monitoring capabilities



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The **OMS** is the central component that:

- Serves the Cloud Control console webpages
- Handles jobs and notifications logic
- Discovers hosts by pushing agents to them across a network, or by cloning an agent from one host to one or multiple hosts of the same operating system
- Orchestrates the management of targets when hosts are discovered and agents are running
- Stores data collected by agents into the OMR
- Interfaces with the Oracle Harvester for uploading targets' configuration data to My Oracle Support, if configured

The OMS has two types of **plug-ins**:

1. **Solution** Plug-ins:
 - Deliver vertical Enterprise Manager functionality (for example, Cloud Application Plug-in, Capacity Planning and Chargeback Plug-in, and so on)
 - Are target agnostic
 - Reside only on the OMS
 - Can be updated independently from the OMS
2. **Target** Plug-ins:
 - Have *OMS-side* and *agent-side* components
 - OMS-side* components, residing with the OMS, determine the management options and behavior exposed through the Cloud Control console.
The *agent-side* components, residing with the agents:
 - Manage the targets as directed by the OMS
 - Gather configuration information from their managed targets
 - Monitor availability and performance of targets
 - Are installed by default in some cases (for example, the Oracle Database, listener, and so on)
 - Can be updated independently of the agent and other plug-ins

Discovery: What Is Host Discovery?

- Agent-based
 - Auto-discovery
 - Done by a dedicated agent
 - Performed via an IP scan over the network
 - Privileged hosts access required
 - Returns a list of unmanaged hosts
 - Promoted to managed hosts
- Agent-less
 - Manual, guided discovery
 - Initially, no agents exist on the hosts
 - Agents installed on host by various methods
 - Requires the host names
 - Can be performed on a single host or multiple hosts at the same time

ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

In Cloud Control, **discovery** can refer to both the discovery of *hosts* (physical or virtual servers known in your network, running supported operating systems) as well as the discovery of *targets* (software components) running on each host.

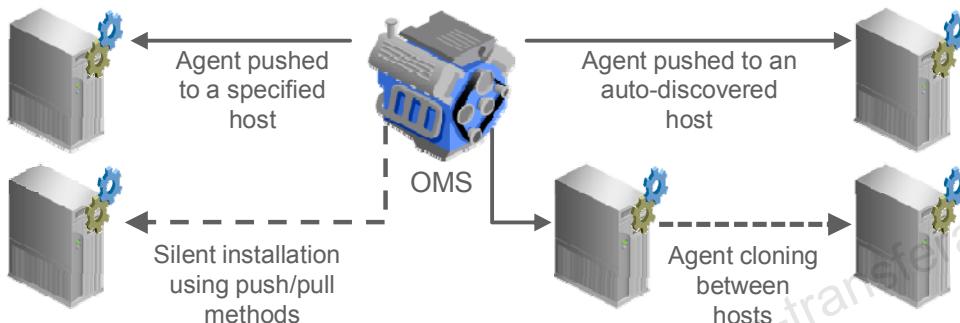
The **hosts discovery** process adds hosts to your managed enterprise. Hosts can be discovered by using a dedicated agent (typically the agent installed with the OMS called the Central Agent) or it can be agent-less.

For agent-based discovery, you specify an agent to perform IP scans and also specify the IP address ranges to be scanned. This method uses network mapper (NMAP) functionality to scan your network and discover hosts. Before hosts are discovered or known to the Cloud Control system, they are referred to as *unmanaged* hosts. Once discovered, hosts can be *promoted* to *managed* hosts.

For agent-less discovery, you need to know the host names before you can discover the products that are configured on that host. This is a manual, guided process that results in agents being installed on hosts, therefore converting those hosts from unmanaged to managed hosts.

Manual Discovery: How Do Hosts Become *Managed Hosts*?

- Hosts in an IT environment become managed hosts when agents are deployed on them: pushed or cloned.
- Sources of agent images
 - Agent software bundle from Software Library
 - Gold Agent Image built from an existing agent



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

An installed, configured, and running agent transforms a host into a Cloud Control **managed host**. Agent images used for installation can be stored and retrieved from the Software Library or, starting with Cloud Control 13c, you can create your own Gold Agent Images based on an existing agent.

The OMS can push an agent to any host that it can access across the network by using a secure shell (SSH) connection. Once connected using authentication credentials supplied through the Cloud Control console, the agent image is sent in compressed form. It is then uncompressed and installed. You nominate the installation directories in the Cloud Control console when initiating the agent push job. The agent can be pushed, using a graphical interface (Add Host Wizard), to:

- Specific hosts on the network identified by name or IP address
- Unmanaged hosts discovered automatically by Cloud Control

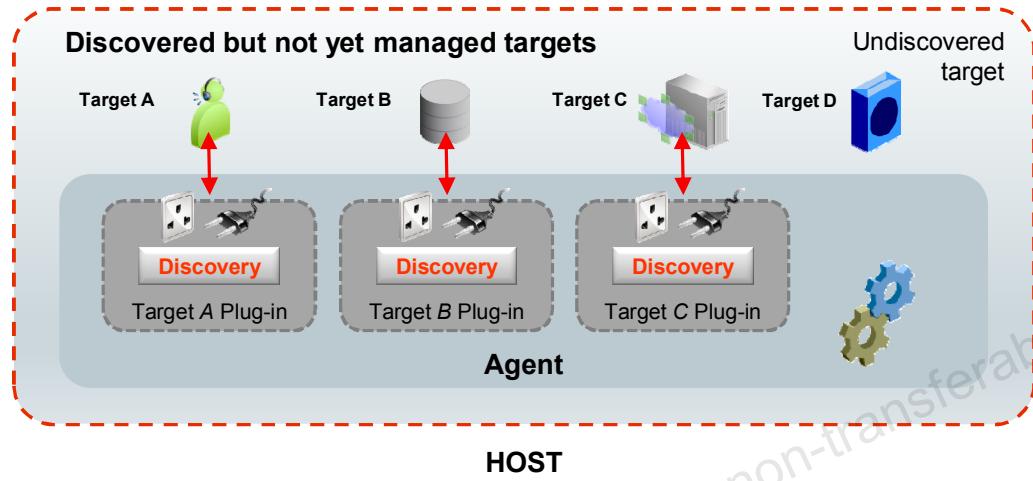
Agents can also be installed in silent mode using response files and scripts that guide the process.

The installation can be done with a “pull” method using the `AgentPull` script, a “push” method using `emcli` to generate a zip file containing the installation binaries and the `agentDeploy` script, a “push” method using `emcli` to generate an RPM file for UNIX platforms (typically used while provisioning an operating system on a bare-metal host), or a newer “push” method using the `emcli submit_add_host` verb that will allow a Gold Agent Image to be deployed.

You can also get Cloud Control to clone an agent from one host to one or more other hosts of the same operating system. This method copies not just the software but the configuration of the agent. This is typically done to define a standard agent configuration and deploy it to multiple hosts.

What Is Target Discovery?

- Done by agents running on hosts
- Based on the target plug-ins



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The agent installation process on a host automatically configures and starts up the agent. The agent then begins the process of **target discovery**. Multiple targets can exist on a host and the agent automatically looks for targets of known types. The types of targets the agent knows about depends on the **target plug-ins** it was initially installed with. An agent plug-in contains two types of components:

- A target **discovery** component
- A **management** component specific to a target that was discovered

The *discovery* content is deployed on a host:

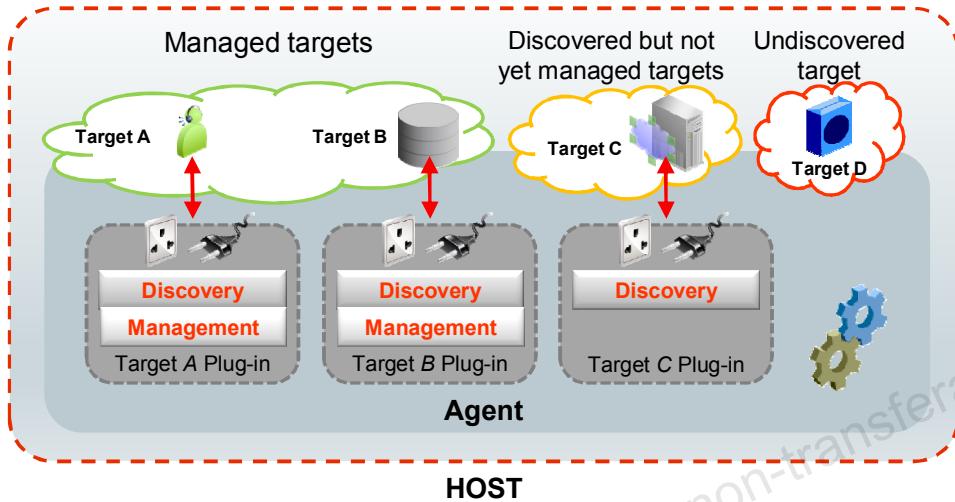
- When the agent is pushed or installed on that host (default plug-ins)
- When a new plug-in is specifically deployed to the agent from the OMS

The graphic in the slide illustrates an example of discovery of targets on a host: Targets A, B, and C are discovered because the agent includes plug-ins of that target type, while target D is not discovered because the agent does not know about that target type (plug-in for Target D is not installed with the agent).

As a Cloud Control administrator, you can guide the target discovery process from the Cloud Control console pages. Guided discovery allows you to nominate a family of target types that you want to search for and then the agents where you want that search to be executed. If any new targets are discovered, the appropriate plug-in will be pushed from the OMS if it is not already installed on the agent. You can also configure target auto-discovery to run at regular intervals on a host. The agent will then search on its own for known targets on that host. This allows you to review the results at a later stage and decide what targets to manage in Cloud Control.

How Do Targets Become *Managed* Targets?

- Discovered targets are **promoted** to managed targets.
- Not all discovered targets need to be promoted.



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Targets become **managed** targets through the process of **promotion**. The target promotion task is done through the Console user interface. The *management* components of the target plug-ins are pushed to hosts when an administrator promotes a discovered target to a managed target.

The graphic in the slide shows an example of possible categories of targets on a host:

1. Targets may be both discovered and managed on a host. In this case, the agent discovery component found the target on the host and the administrator confirmed its management (promoted it to a *managed* target).
2. A target was discovered on a host but not yet managed. This means the administrator chose to not promote it as a managed target, but it can be promoted at a later time.
3. There may be an undiscovered target on a host because no plug-in for it was installed with the agent. Therefore, this type of target is not discovered or managed by Cloud Control. A plug-in for such type of target must be explicitly deployed from the OMS to the agent in order to be first discovered and later promoted to a managed target.

Examples of Managed Target Types

- Oracle Databases
 - Instances, pluggable databases
 - Listeners
 - ASM
- Clusters and High Availability Services
- Oracle Middleware products
- Oracle Application Server
- Oracle Cloud (Hybrid Cloud, on- and off-premise)
- Oracle applications, including E-Business Suite, SOA, Siebel, and PeopleSoft
- Exadata and Exalogic
- Cloud Control components such as the OMR and the OMS
- Third-party targets



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

As you have seen, **targets** are the entities that Cloud Control manages using plug-ins specific to target types and host-specific agents.

Cloud Control can monitor, administer, maintain, and manage different types of targets, as listed in the slide. As your environment changes, you can add and remove targets from Cloud Control as needed. The commonly used Oracle targets (including Cloud Control components, such as the OMR and the OMS) are predefined as part of the base Cloud Control product, but Cloud Control has an open API that enables you to create custom targets.

The targets in the slide are just some examples of Cloud Control managed targets.

Oracle Management Repository

- Resides in an Oracle database
- Includes schema objects belonging to SYSMAN
- Must be installed in a pre-existing database
 - Use predefined database templates where available
 - Created during installation
- Installation recommended in a RAC database
- Has a dedicated database
 - Resources
 - Maintenance
 - Licensing



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Another core component of Cloud Control is the Oracle Management Repository (OMR). The OMR is installed in an Oracle database, version 12.1.0.2 or above, as a group of approximately 4,000 schema objects belonging to the SYSMAN user stored in three tablespaces:

MGMT_ECM_DEPOT_TS, MGMT_TABLESPACE, and MGMT_AD4J_TS. These schema objects contain information about Cloud Control users (administrators), targets, and applications that are monitored and managed by Cloud Control, and groups, systems, incidents, and other Cloud Control artifacts. The OMR is created during installation in a pre-existing database or a new database created just for this purpose. The OMR must be sized appropriately for the projected managed enterprise. The fastest, and recommended, way of creating a repository is by using predefined database templates. Templates allow you to create a small, medium, or large repository at installation time. Note that database templates may not be available for all certified database versions. In this case, a repository is created from the beginning during the installation process.

For high-availability and scalability options, it is recommended that the OMR be installed in a Real Application Clusters (RAC) database or configured with a stand-by database using Data Guard.

The database used to house the OMR should not be used for any other applications for the following reasons:

- Cloud Control's usage of the database should not have to compete with any other usage.
- Using the OMR database for other applications may restrict your ability to upgrade and patch the OMR schema and database as required.
- Cloud Control includes a restricted-use Oracle Database Enterprise Edition license that can be used for the OMR only. The OMR requires the Partitioning option to be included with the Enterprise Edition.

Software Library

- File system repository of various software components
- Organizes certified software entities in:
 - Oracle-owned folders, locked, shipped by default
 - User-owned folders
- Shared file system recommended
 - Sized appropriately based on your use
 - OMS reachable
 - Agent reachable
 - Referenced file system



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The Software Library is a file system-based repository that stores software entities such as software patches, virtual appliance images, reference gold images, and application software and their associated directive scripts, and allows you to organize them in logical folders. Patching and provisioning deployment procedures use these entities available in the Software Library.

This centralized media storage can be an NFS file system that is being shared between OMSs or any file system that the agents can reach. If you have multiple OMSs in your enterprise, you should create the Software Library in a location that can be accessed by all OMSs. You can also define referenced locations so that an already established centralized location of these entities, separate from the OMS, can be referenced.

The size of this central storage is based on your usage pattern.

EM Command-Line Interface

- Can be used to perform tasks from text-based consoles
- Allows automation of repetitive tasks
 - Mass-managing targets
- Is integrated with Cloud Control security and administration functions
- Interface modes include:
 - Standard
 - Interactive
 - Script



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Monitoring: Key Functionality

- Out-of-the-box monitoring as soon as Cloud Control is deployed and targets discovered
 - Predefined metrics collection
 - Includes metrics on Cloud Control itself
 - Systems Infrastructure monitoring
 - Operating systems, virtualized operating systems, servers, storage, and networks
 - Real-time data: Charts
 - Default thresholds
 - Violations produce alerts
- Customization
 - Thresholds values better suited for your environment
 - Notifications



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

One of the key functionalities of Cloud Control is the ability to monitor all its targets and aggregate and correlate all monitoring data. Enterprise Manager Cloud Control offers an out-of-the-box comprehensive set of predefined performance and health metrics that enable automated monitoring of various targets in your environment. Most **metrics** are collected by the agents deployed in your system, including data on Cloud Control itself, databases, middleware, hosts, operating systems, virtualized operating systems, and storage and network resources. Some of these metrics are real-time data displayed on predefined charts and summarized for each target.

Some metrics have associated predefined limiting parameter values called **thresholds**. When these limits are exceeded, **alerts** can be triggered. Metrics collection, threshold values, alerts, and the notifications on these alerts are all customizable.

Metrics definitions, thresholds, collection values, and collection intervals are found in the *Metric Reference Manuals*, grouped by target type, available with Enterprise Manager Cloud Control documentation at <http://docs.oracle.com>.

The monitoring setup and usage is described in detail in an upcoming lesson.

Other Monitoring and Management Functionality

- Job System
 - Automates administrative tasks with scheduled jobs
- Systems and Services monitoring
 - End user monitoring: applications or special group of targets
- Patching and Provisioning
 - Automates deployment of software and patches
- Configuration Management
 - Tracks hardware, software installation, and configuration
- Compliance Management
 - Applies and tracks standards for your organization
- Reporting System
 - Business Intelligence Publisher (BI Publisher)



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Security: Overview



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The Cloud Control security system can be divided into four components, as shown in the graphic in the slide:

- Cloud Control **Authentication** checks the validity of users accessing the Cloud Control system.
- Cloud Control **Authorization** grants privileges to managed targets.
- **Credentials** Management allows credentials to be defined for various managed targets.
- The **Target Authentication** system uses the defined target's credentials.

In addition, a security subsystem that spans all main security areas is the auditing system. Auditing capabilities are available for the purposes of tracking and validating actions performed in Cloud Control, including jobs and credentials accessed. Basic auditing is enabled by default for Cloud Control to track the use of credentials and operations such as copying or removing the encryption key, performing secure OMS operations, or changing the repository password.

More details on each of these components are provided in upcoming lessons.

Summary

In this lesson, you should have learned how to:

- Confirm your understanding of the Cloud Control architecture
 - Describe the different components and subsystems of Cloud Control
 - Explain the architecture of Cloud Control, including the security model
 - List the target types managed by Cloud Control
- Explore the Enterprise Manager interface



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Practice 2-1 Overview: Accessing Enterprise Manager Cloud Control

This practice covers the following topics:

- Accessing Enterprise Manager Cloud Control
- Customizing Cloud Control
- Navigating the Cloud Control console



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Practice 2-2 Overview: Monitoring and Managing Cloud Control

This practice covers the following topics:

- Performing the OMS and the OMR monitoring tasks
- Reviewing the Security Console



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Practice 2-3 Overview: Monitoring the Cloud Control Host

This practice covers the following topics:

- Viewing host target information (CPU, memory, and network utilization)
- Viewing related targets on this host



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Organizing Targets

Groups

ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Objectives

After completing this lesson, you should be able to:

- Define and distinguish Enterprise Manager groups
- Describe the benefits of using groups
- Explain target properties and how they relate to groups
- Create various types of groups
- Set up a monitoring hierarchy



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

ORACLE

Organizing Targets into Groups

- Cloud Control targets are units of management:
 - Hosts
 - Databases
 - Middleware, and so on
- Organizing targets is important for efficiency and ease of management.
- Organizing strategy: grouping targets:
 - By target properties
 - By monitoring style
 - By owners, and so on



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Why Use Groups?

- Streamline and simplify your management and monitoring tasks.
- Scale as your data center grows.
- Meet Service Level Agreements.
- Manage targets as one unit.
 - Targets can be organized as a single functional unit.
- Ensure consistency in your monitoring.
 - Deploy changes to your monitoring settings.
- Enforce permissions as an aggregate.



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Groups, in general, allow you to manage targets as one unit in Cloud Control. The benefits of implementing groups are to streamline and simplify your management and monitoring tasks, ensure consistency in your monitoring, and easily deploy changes to your settings. Scalability is a very important aspect in a data center: While managing ten targets manually might be possible in a consistent way, imagine doing the same for more than a thousand targets.

Groups offer advantages from a security perspective as well. You can enforce permissions as an aggregate. You only need to grant administrators access to the groups of targets that they need to manage as opposed to a large number of targets. For example, database administrators are interested only in the databases that they are responsible for, so you can create a group of databases for them. Some administrators might want to manage targets within their geographic areas, so you create groups containing those targets.

Understanding Properties of Targets

- Target types
 - Hosts, Databases, Middleware, and so on
- Lifecycle status
 - Development, Production, Test, and so on
 - Used internally by Cloud Control to prioritize workload
- Other properties
 - Version, Location, Owner, Cost Center, LOB, and so on
 - Support for custom list of values
- Assigned at discovery times
 - Can be edited later



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Cloud Control Group Types

- **Group** (Regular, Static)
 - Explicit assignment of targets
 - By search or by criteria, or both
 - Can be a **privilege propagating** group
 - Future targets inherit same privileges
- **Dynamic Group**
 - Defined by membership criteria, based on target properties
 - All criteria must be met and then targets automatically added
- **Administration Group**
 - Membership criteria based on target properties, hierarchical
 - **Privilege propagating** group
 - A target can belong to at most one Administration Group.
- **Similar to groups**
 - **System:** Targets that work together to host an application or service
 - **Service:** A set of entities that deliver a function



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

In Cloud Control, you can create a variety of groups. The following are the types of groups available:

- A **regular group** can include targets of the same type, such as all your production databases, or include targets of different types. A group can include other groups. You explicitly assign targets to a group.
- Privileges, in the context of Cloud Control, are permissions or rights granted to administrators to enable them to manage targets. A **privilege propagating group** is a regular group wherein a privilege that you grant on the group automatically extends to all its targets, including any targets added to the group in the future.
- A **Dynamic Group** is a group whose membership is determined by membership criteria. Enterprise Manager automatically adds targets that match predefined membership criteria.
- **Administration Groups** are groups that are created based on target properties that act as membership criteria. Privilege propagation is included. Cloud Control automatically adds targets to an Administration Group if that target meets your configured membership criteria. You cannot directly add targets to the Administration Group. A target can belong to at most one Administration Group.
- **Systems** are a specialized type of groups. A system includes heterogeneous targets that work together to support an application or service. When defined as a System, features such as jobs and blackouts are still available. In addition, other overview, management, and troubleshooting capabilities may be available. See the lesson “Managing Systems and Services” for more details.
- A **Service** is a container target that supplies a function (like email).

Which Groups Should I Use?

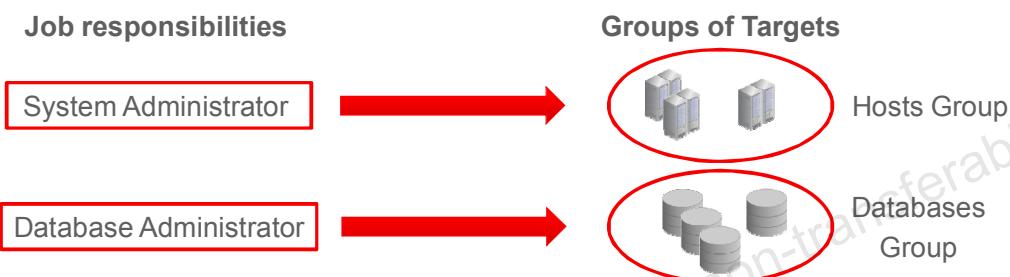
Group Type	Unique/Notable Benefits	Best Usage
Privilege propagating	Privileges granted to an administrator for a member of the group are automatically inherited by all members of the group	To allow automatic access to new targets
Dynamic	Automatic assignment to a group based on target properties	<ul style="list-style-type: none">• To group a large number of targets• To run jobs and other group operations
Administration	<ul style="list-style-type: none">• Targets belong to at most one Administration Group to avoid conflicts• One hierarchy of Administration Groups per site• Auto-deployment of monitoring settings• Privilege propagating	<ul style="list-style-type: none">• To automate the deployment of monitoring settings to targets in the group• To define collections on multiple targets



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Designing Target Groupings

- Groups are unique for each enterprise.
- Based on job responsibilities
- Typical generic groupings
 - By Lifecycle Status
 - Production, Development, and so on
 - Type
 - Databases, Hosts, and so on



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Cloud Control privileges should map to a job definition for each administrator. The job responsibilities will also determine how the managed enterprise is structured and how the targets are grouped for management.

Targets can be grouped by owners, by lifecycle status or line of business, and so on. This grouping will be unique for each enterprise. Some of the traditional roles /jobs are:

- Systems Administrator, Storage Administrator, Backup and Recovery Administrator
- Networking Administrator, Security Administrator
- Virtual Infrastructure Architect, Virtual Infrastructure Administrator
- Support

So, for example, targets may be grouped within a group called Hosts Group and a System Administrator can be the owner or have full responsibility for all those targets. Similarly, a Database Group can be assigned to be managed by a Database Administrator.

Specific fine-grained privileges can be assigned to a group owner to enable granular control over actions that can be performed by that administrator. The Enterprise Manager Cloud Control documentation describes in detail various job responsibilities and the corresponding privileges in Enterprise Manager required to support these.

Working with Dynamic Groups

- Dynamic groups are created by specifying membership criteria.
 - Based on target type properties
 - Multiple criteria
 - One time setup
- New targets are added automatically if they meet all criteria.
- You can enable or disable privilege propagation.
- The privilege that is required to create these groups is:
 - View Any Target
- The privileges required to enable privilege propagation are:
 - Full Any Target
 - Create Privilege Propagating Group
- Dynamic groups cannot contain other groups.
- They are recommended for automatically grouping a large number of targets, running jobs, or performing other group operations.

ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

A dynamic group is a group of targets created only by specifying membership criteria. Cloud Control automatically determines which members can be part of a dynamic group by evaluating the criteria. Membership criteria are based on target properties (for example, target types, lifecycle status, location, and so on). When multiple criteria are defined for a dynamic group, a target must match all criteria before it is automatically added to the group.

You can have Privilege Propagation enabled for a dynamic group. This means that the target privileges granted on the group to the administrator will be propagated to the member targets. Therefore, if this property is enabled, only targets on which the administrator has full privileges can be members of the group.

- To create these types of groups, you would require:
 - View Any Target
- To enable privilege propagation, you would require:
 - Full Any Target
 - Create Privilege Propagating Group

Dynamic groups cannot contain static groups, other dynamic groups, or Administration Groups. Again, these types of groups are recommended for managing a large number of targets, running jobs, and performing management tasks against the group as a single unit.

Working with Administration Groups: Overview

- Define group hierarchy.
 - Unique, single hierarchy
 - Group targets monitored or managed in a similar way
- Specify membership criteria.
 - Membership criteria are based on target type properties.
 - Each level in the hierarchy represents a target property.
 - Privilege propagation is included.
- Define monitoring details.
 - Create Monitoring Templates.
 - Create Template Collections.
 - Associate template collections with groups.
- Recommended for automating monitoring settings



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Administration Groups were designed to automate management settings such as:

- Monitoring settings (metrics collections and setup)
- Compliance standards (a collection of rules that are industry-accepted as best practices; to be discussed in an upcoming lesson)
- Cloud policies (a collection of rules that apply to Cloud management; beyond the scope of this course)

Administration Groups are created by first defining the group hierarchy. Each level represents a target property. You can only create one group hierarchy, based on the target properties identified. Targets should be grouped together if they are managed or monitored in a similar way. To join an Administration Group, targets must match all membership criteria defined by the levels of the hierarchy. Once defined, targets are automatically added at the leaf level based on their properties. Targets can only belong to at most one Administration Group.

Once an Administration Group is created, a typical monitoring setup follows these steps:

- Create Monitoring Templates to allow you to apply a subset of monitoring and collection settings to multiple targets. These templates allow you customize the metrics, thresholds, and collection schedules per your company policy.
- Group templates into Template Collections, which are sets of Monitoring Templates, Compliance Standards, and Cloud Policies.
- Associate Template Collections with groups.

More details on Administration Groups and compliance standards will be covered in upcoming lessons.

Comparing Group Characteristics

Group Type	Monitoring Templates Auto-Apply	Group Management Operations (Jobs, Blackouts/Brownouts, Reports, Dashboards)	Membership Criteria Based on Target Properties	# of Groups a Target Can Belong To	Privilege Propagating
Group	No	Yes	No	One or more	No
Privilege Propagating Group	No	Yes	No	One or more	Yes, by definition
Dynamic Group	No	Yes	Yes	One or more	Optional, user specified
Administration Group	Yes	Yes	Yes	At MOST one	Yes, always



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Populating Groups: Best Practices

- Set target properties once you create groups:
 - During target promotion
 - Post discovery, from the target home page
- Set target properties using Cloud Control Administrator account attributes:
 - Set attributes for a Cloud Control Administrator.
 - All targets promoted by this Administrator automatically inherit target properties.
 - This makes grouping easier.
- Use EM CLI for mass target properties setting.
- Administration Groups: Periodically check your unassigned targets.
 - Use the “Unassigned Targets” option to check for incorrectly set target properties.



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Groups are populated by setting the target properties to values that groups are organized by. Target properties can be set from the Cloud Control Console during discovery or from each target home menu.

Starting with Enterprise Manager Cloud Control 12.1.0.2, administrator account attributes such as Contact, Location, Department, Cost Center, and Line of Business can be defined. Any target added (promoted) by this administrator will automatically inherit the same values for its target properties. As a result, these targets can easily or automatically be grouped.

EM CLI is the recommended option for setting target properties in bulk.

For Administration Groups in particular, once targets are set up, you can use the “Unassigned Targets” option to check for targets that were not added to groups as designed.

Quiz



Grouping targets in Cloud Control is good practice because:

- a. Targets like to be in groups.
- b. Groups can simplify management of targets by enforcing consistent privilege assignments and monitoring settings.
- c. You want to create more work for yourself.



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Quiz



Administration Groups are privilege propagating groups.

- a. True
- b. False



Answer: a

Summary

In this lesson, you should have learned how to:

- Define and distinguish Cloud Control groups
- Describe the benefits of using groups
- Explain target properties and how they relate to groups
- Determine what groups to use
- Set up a monitoring hierarchy



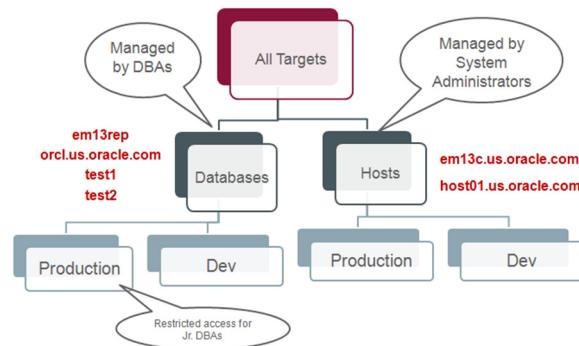
ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Practice 3-1 Overview: Organizing Your Targets: Administrative Groups

This practice covers the following topics:

- Assigning target properties
- Creating an Administrative group hierarchy
- Exploring the new group



Practice 3-2 Overview: Organizing Your Targets: Non-Privilege-Propagating Groups

This practice covers the following topics:

- Creating a group that does *not* propagate privileges
- Exploring the new group



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Practice 3-3 Overview: Discovering Additional Targets

This practice covers the following topics:

- Discovering additional targets in your environment
- Noting the groups these targets get assigned to



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Unauthorized reproduction or distribution prohibited. Copyright© 2019, Oracle and/or its affiliates.

GANG LIU (gangl@baylorhealth.edu) has a non-transferable license
to use this Student Guide.

Oracle Cloud in Your IT Ecosystem

ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Objectives

After completing this lesson, you should be able to:

- Identify the Oracle Cloud services that can be managed by Enterprise Manager Cloud Control
- Describe how Enterprise Manager Cloud Control manages Oracle Cloud services
- List the operations that Enterprise Manager Cloud Control enables between on-premises targets and Oracle Cloud services



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Oracle Cloud as Part of Your IT Ecosystem

- Oracle Cloud gives you many benefits:
 - Rapid scalability
 - Ability to lift and shift workload from your data center to the cloud
 - Delegation of hardware and platform maintenance to Oracle
- You can monitor and manage Oracle Cloud services with on-premises Cloud Control.
 - Referred to as Hybrid Cloud



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Oracle Cloud Has a Silver Lining

If you choose to take advantage of the benefits that Oracle Cloud offers, you can use your Enterprise Manager Cloud Control 13c to manage and monitor your cloud services and deployments, just as you would the hosts and applications in your own data centers. Cloud Control agents can be deployed to the virtual machines that underpin some of the Oracle Cloud services. The same plug-ins that manage and monitor your local targets can be used with the targets that are running on the Oracle Cloud virtual machines too.

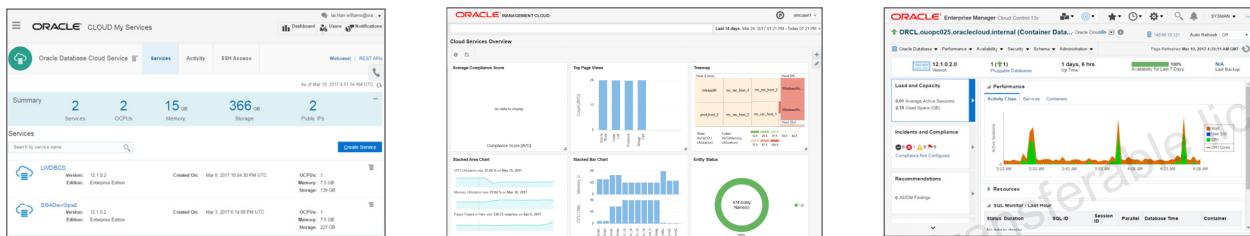
At the time of writing this course, the following services were supported by Hybrid Cloud:

- Oracle Database Cloud Services (DBCS)
- Oracle Java Cloud Services (JCS)
- Oracle Compute Cloud Services

This means that you can install the Enterprise Manager Cloud Control management agent on the virtual machines that are deployed for you as part of the service. In the case of Compute Cloud Service, you have the potential to use standard Cloud Control plug-ins to manage and monitor whatever applications you deploy on the Compute Cloud Service VMs.

Tools for Monitoring and Managing Oracle Cloud Services

- Oracle Cloud service webpages
 - Provisioning, configuration, patching, user maintenance, network configuration
- Oracle Management Cloud
 - Monitoring Oracle Cloud compute and PaaS instances
- Enterprise Manager Cloud Control
 - Monitoring and managing service instances with standard agents and plug-ins



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Tools for Every Need

After you subscribe to Oracle Cloud, there different ways of monitoring and managing your services:

- **Oracle Cloud service webpages:** Serving as your primary entry point to provisioning instances in your Oracle Cloud service, you can also use these pages to manage users and their access, configure and patch your service instances, configure network access, and decommission service instances.
- **Oracle Management Cloud:** If you subscribe to Oracle Management Cloud, you can use it to monitor your Compute, Database, and Java Cloud Services.
- **Enterprise Manager Cloud Control:** Exercise the same level of monitoring and management on your Oracle Cloud service instances that you enjoy with your on-premises targets by using the same agents, plug-ins, and user interface.

Why Use Cloud Control to Manage Oracle Cloud Services?

- Single pane of glass
 - Same interface for on-premises and Oracle Cloud instances
 - Same administrator authentication and authorization mechanism
 - Management of all incidents in one place
- Fine-grained control of service instances
- Lifting and shifting of load
 - From on-premises to Oracle Cloud
 - From Oracle Cloud to on-premises



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

If You Could Only Choose One Management Tool

If you could only choose one tool from the tools that are available to manage your Oracle Cloud services, Enterprise Manager Cloud Control would be the logical choice.

Primary among the reasons for using Cloud Control is one of the central design tenets of Enterprise Manager Cloud Control 13c: the single pane of glass. In an on-premises-only IT ecosystem, the single pane of glass design refers to the ability to monitor and manage a variety of target types with a single tool and to provide access to users of different roles. When Oracle Cloud is added to your IT ecosystem, the single pane of glass philosophy is truly showcased because the reach of Cloud Control extends beyond your on-premises targets to the cloud.

Because Cloud Control monitors and manages your Oracle Cloud targets with the same agent and plug-in software that is used for your on-premises targets, you can exercise the same level of control over the Oracle Cloud targets that you have over your on-premises targets.

Cloud Control's awareness of targets on-premises and in Oracle Cloud enables you to clone database and middleware targets between both domains, effectively lifting and shifting load from your data centers to Oracle Cloud or vice versa.

How Cloud Control Monitors and Manages Oracle Cloud Services

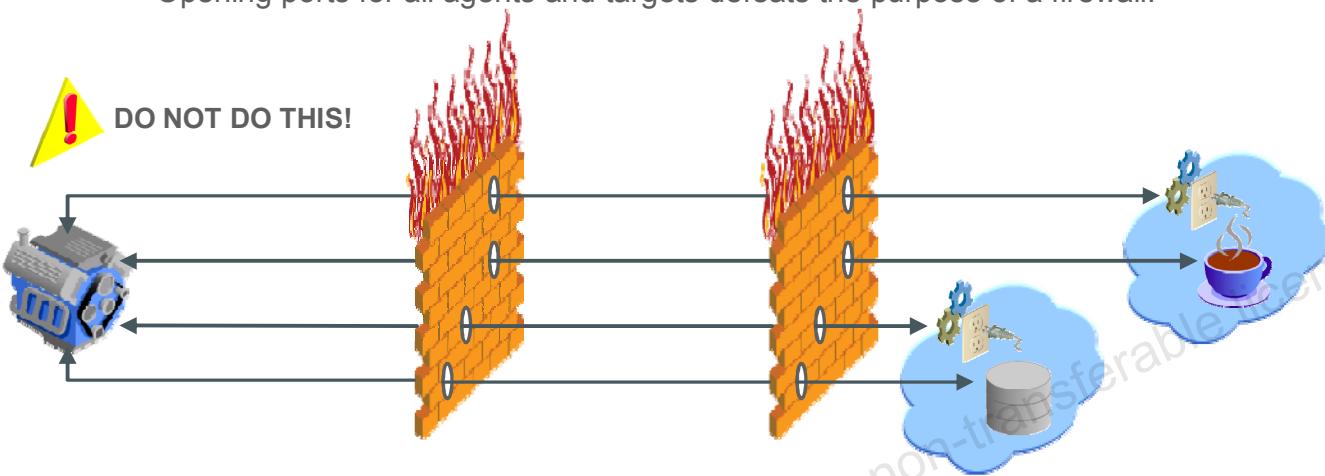
- Deploy the standard agent to your Oracle Cloud service instance virtual machine.
- Discover targets in your Oracle Cloud service instance.
- Treat the Oracle Cloud targets like any other.
 - Set up credentials.
 - Add to groups.
 - Monitor, manage, and report.
 - Patch (caveat applies).
- Discover and manage Oracle Cloud services through the Cloud REST APIs.
 - NEW in Enterprise Manager Cloud Control 13.2 Plug-ins Update 1
 - Mimics the Oracle Cloud console functionality



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

How to Get Past the Firewalls That Protect You

- How do you communicate with Oracle Cloud hosts without compromising firewall security?
 - Firewalls are prescriptive.
 - Opening ports for all agents and targets defeats the purpose of a firewall.

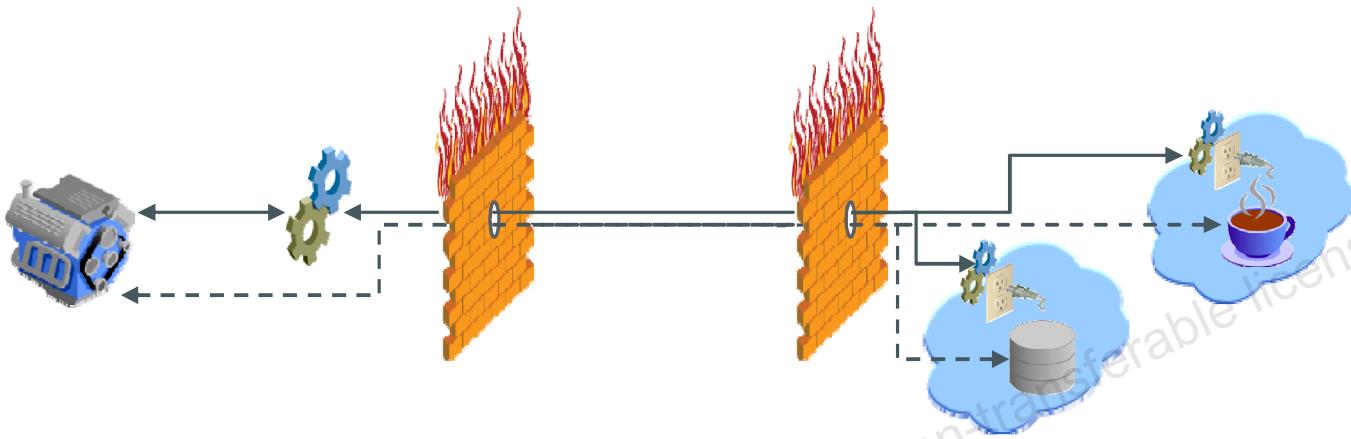


ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The Hybrid Cloud Agent: An Elegant Solution

- Tunnels communication with Oracle Cloud over SSH
 - Via an on-premises “gateway” agent for OMS-to-agent communication
 - Via the SSH tunnel for OMS-to-target communication



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

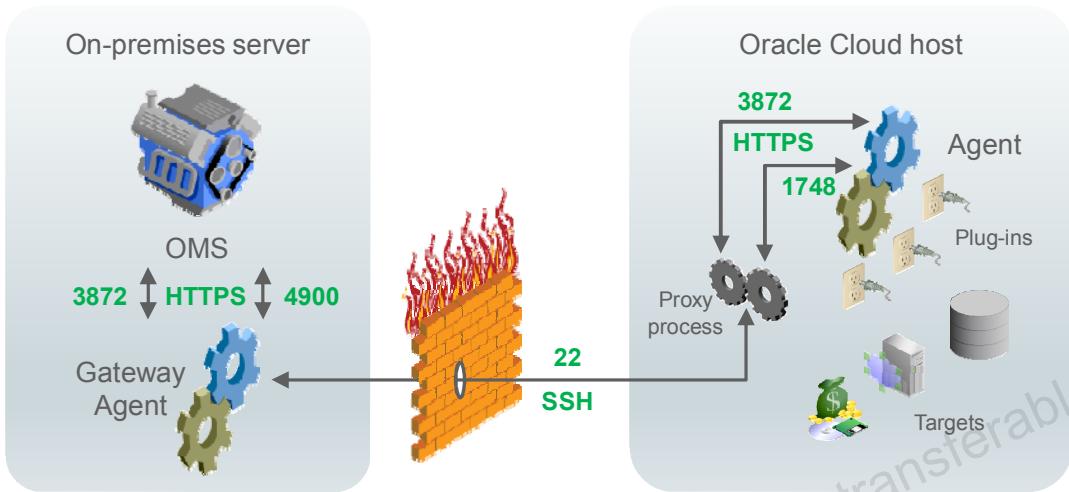
One Tunnel for All Traffic

The Hybrid Cloud Agent elegantly resolves the topological dilemma for accessing hosts and targets in the Oracle Cloud in several ways:

- A Secure Shell (SSH) tunnel is configured in the OMS by providing named SSH credentials for the Oracle Cloud.
- One or more on-premises agents are configured as gateway agents.
- The agents on the Oracle Cloud hosts are installed via a gateway agent.
- Agent-based communications are made over the SSH tunnel via a gateway agent.
- OMS-to-target communications are made directly over the SSH tunnel.

Under the Covers of the Hybrid Cloud Agent

- OMS and cloud agents are protected from direct communication.



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Protected by a Gateway and a Proxy

Aspects of the hybrid cloud agent topology have been specifically designed to ensure that both the OMS and the hybrid cloud agent are protected from any illegitimate traffic:

- When the OMS initiates communication with an agent in Oracle Cloud, it does so via the SSH tunnel by using an EMCTL dispatcher on the Oracle Cloud host.
- When the agent initiates communication with OMS, it does so via a local proxy process which, in turn, communicates via the SSH tunnel with an on-premises agent that is configured as a *gateway agent*.
- When the OMS initiates direct communication with any of the targets on the Oracle Cloud managed host, such as a database, it does so via the SSH tunnel.

For more information about enabling hybrid cloud agents, see the *Enterprise Manager Cloud Control Administrator's Guide*.

What the Hybrid Cloud Agent Enables

- Lift and shift for DB
 - Clone an on-premises DB to a Compute Cloud instance.
 - Clone an on-premises DB to a DBCS instance.
 - Refresh data from an on-premises test master DB to DBCS instances.
- Lift and shift for MW
 - Clone on-premises apps and composites to JCS instances.
 - Clone on-premises WebLogic Domain partitions to JCS or Compute Cloud instances.
 - Clone a WebLogic Domain to JCS.



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Summary

In this lesson, you should have learned how to:

- Identify the Oracle Cloud services that can be managed by Enterprise Manager Cloud Control
- Describe how Enterprise Manager Cloud Control manages Oracle Cloud services
- List the operations that Enterprise Manager Cloud Control enables between on-premises targets and Oracle Cloud services



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Unauthorized reproduction or distribution prohibited. Copyright© 2019, Oracle and/or its affiliates.

GANG LIU (gangl@baylorhealth.edu) has a non-transferable license
to use this Student Guide.

Cloud Control Access

Roles, Privileges, and Credentials

ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Objectives

After completing this lesson, you should be able to:

- Identify how access to Cloud Control targets is controlled
- Define roles and privileges and how they relate to groups
- Distinguish between various types of roles
- Describe target credentials and their types

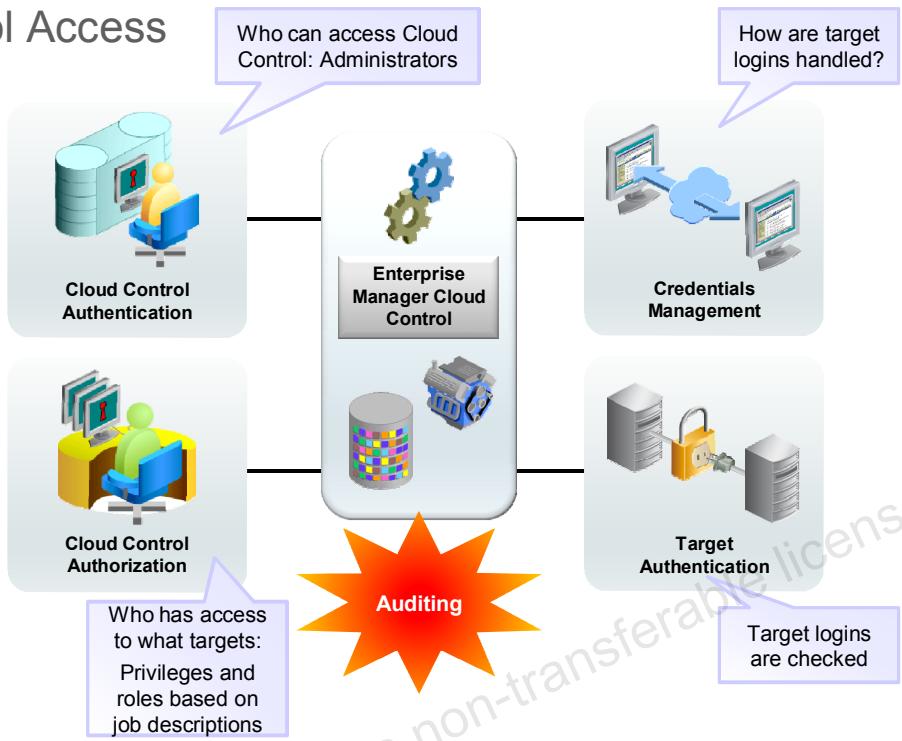


Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

ORACLE

Designing Cloud Control Access

- Based on job responsibilities
- Spans all security subsystems
- Job responsibilities map to privileges
 - Basic unit of access



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

How Authentication Works in Cloud Control

- Authentication: Login credentials provided are compared to those on file.
- Support for different classes of login users:
 - Super Administrators
 - Administrators
 - Repository Owner: SYSMAN
- User credentials on file are preconfigured, typically at install time.
 - Database authentication
 - Other authentication methods supported:
 - SSO, LDAP, and so on



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Authentication is the process of comparing a set of login credentials provided to those on file for that system. A Cloud Control user logs in as a pre-created user, created by a Super Administrator (SYSMAN at first). The classes of users supported are as follows:

- **Super Administrators are assigned highest privileges:** They can manage all the resources in the system with the exception of Named Credentials created by other users, therefore limiting access to jobs and deployment procedures created by other users.
- Regular Administrators are assigned specific tasks.
- Repository owner, SYSMAN, which should not be deleted or altered in any way

With Cloud Control, the on-file credentials can be stored in a database (by default, the database authentication is configured) or other authentication servers such as Single Sign-on (SSO) or Lightweight Directory Access Protocol (LDAP) based systems.

Authentication is built into both access interfaces, the Cloud Control console and the Enterprise Manager Command Line Interface (EM CLI).

Cloud Control Administrators

- Login access to Cloud Control
- Created by Super Administrators
- Given required and optional attributes
- Assigned target privileges, resource privileges, and associated roles
 - Provides separation of duties among administrators
 - Requires these privileges to be explicitly granted to allow administrators to perform any task in Cloud Control



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

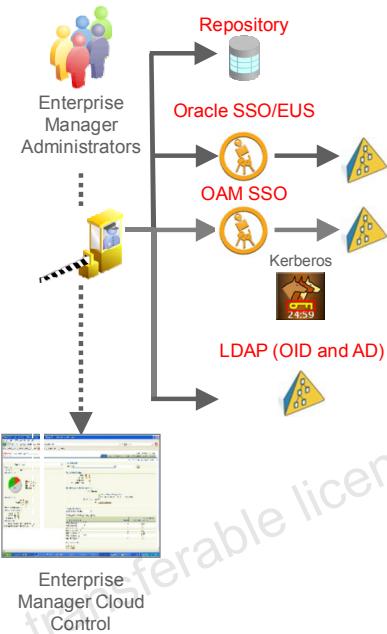
Cloud Control Authentication Options

Repository-based (default)

- Cloud Control Administrator accounts are database users.
- Database-controlled password management

External Authentication

- Oracle Access Manager (OAM) Single Sign-on
 - Including Kerberos
- Application Server Single Sign-on
- Enterprise User Security (EUS)
- Oracle Internet Directory (OID)
- Active Directory (AD)



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Repository-Based Authentication is the default authentication option. An Enterprise Manager administrator is also a repository (database) user. By using this option, you can take advantage of all the benefits that this authentication method provides, such as password control via password profile, enforced password complexity, password life time, and number of failed attempts allowed.

In addition, Enterprise Manager Cloud Control supports other types of authentication methods for logging in to the Enterprise Manager Cloud Control console:

- **Oracle Access Manager (OAM)** is the Oracle Fusion Middleware single sign-on solution, supporting various protocols (for example, Kerberos). This is commonly configured for sites that use OAM as a standard solution.
- **Application Server SSO-based authentication** is another supported authentication method that provides centralized user identity management across the enterprise.
- **Enterprise User Security (EUS)-based authentication** enables you to create and store enterprise users and roles for the Oracle database in an LDAP-compliant directory server.
- **Oracle Internet Directory (OID)-based authentication:** When using an authentication scheme based on Oracle Internet Directory as the identity store, you can plug in the OID-based authentication schema to have your applications authenticate users against the OID.
- **Microsoft Active Directory-based authentication:** When using Microsoft Active Directory as an identity store, you can plug in this schema to have your applications authenticate users against Microsoft Active Directory.

Configuring authentication using these supported methods is specific to the authentication solution. In most cases, OMS will need to be configured for that authentication application and restarted.

How Authorization Works in Cloud Control

- Authorization is the process of checking a user's privileges and access to resources.
- It is managed with privileges and roles.
 - Privileges define access to the managed targets.
 - Roles are sets of privileges.
 - Roles can contain other roles.
- Administrators are assigned privileges and/or roles by Super Administrators.



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

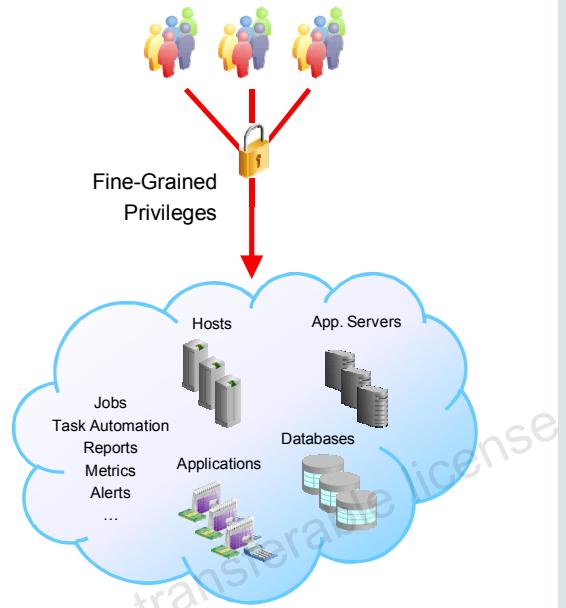
If the login credentials match, the authentication process is completed and a user (here, an Administrator) is **authorized** access to the system. **Authorization** is the process of checking a user's privileges and access to resources to ensure integrity, confidentiality, and availability.

After it is authenticated, Cloud Control users are given access to a number of targets and resources via the concept of Privileges and Roles. Privileges define the access level to the targets or resources in the managed system. Similar to the database Roles concept, Cloud Control roles are collections of privileges. Roles simplify access to thousands of targets and resources.

The privileges granted to the authorized Administrator depend on the selections done by the initial administrator, a Super Administrator.

Privileges

- Administrators acquire privileges upon successful authorization.
- Target Privileges
 - Target operations
 - FULL, OPERATOR, and VIEW levels
 - Applicable to all targets or specific targets
- Resource Privileges
 - Access to specific functionality
 - FULL, EDIT, or VIEW levels



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Privileges are the basic layer of access control for Administrators in Cloud Control. There are various privileges defined in Cloud Control and they fall into two categories:

- **Target privileges** allow the user to perform activities on a specific target. Target privileges can apply to all targets. They can range from the privilege to perform all operations and edit properties on a target (FULL) and perform operations only (OPERATOR), to simply looking at a target's information without being able to make any changes (VIEW).
There are also target privileges that can be applied only to a single target. When assigning these, a Super Administrator must indicate the specific target.
- **Resource privileges**, on the other hand, allow the administrator to perform operations against a resource or a specific feature or function of Cloud Control. Access can vary again from full privileges (FULL) and editing of that resource's properties (EDIT) to view only (VIEW). For example, there are a series of privileges that allow users to work with the Job System or Patching System. If granted, Job System privileges may include full job privileges, edit job privileges (which do not allow a job to be deleted), view jobs, and so on. These privileges refer to subsystems of Cloud Control rather than access to a specific managed target.

Roles

- Contain resource or target privileges
 - Can contain other roles
- Designed for easy privilege assignment
- A more secure way of managing privileges
 - Allows implementation of the Principle of Least Privileges
- Can be defined on group criteria
 - Geographical location, line of business, and so on
 - Groups of targets by same criteria get these roles
- Types
 - System Roles
 - Private Roles, to protect powerful privileges
 - External, can map to groups defined externally (for example, LDAP)
 - Out-of-the-box or Custom
 - Default Public Role, no privileges initially



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

A role is a collection of Cloud Control resource privileges and/or target privileges granted to administrators or to other roles. Roles are advantageous because administrators only need to assign a role to a new user and automatically all appropriate privileges are assigned to that user. To change a set of privileges for an administrator, you just need to update the role. When new administrators are added, you only need to grant them the appropriate role(s) instead of granting them individual privileges. Roles also facilitate the implementation of the Principle of Least Privileges, which dictates that users should be granted the least amount of privileges needed to perform their job.

Regular groupings of privileges are called System Roles. Private Roles were introduced starting with Cloud Control 12.1.0.4 to help manage more powerful privileges that allow access to credentials or the Job System.

Roles can be custom-defined or you can take advantage of a number of predefined roles that are packaged out-of-the-box with Cloud Control. A special Role called Public is defined by default; however, no privileges are assigned to it initially. This role is automatically assigned to all new non-super administrators at creation time. If you decide to use this role, you must decide what roles can automatically get assigned to newly created regular administrators.

Administrators, by default, do not have any Software Library privileges. The Super Administrator must explicitly grant privileges to an administrator to access the Software Library.

Private Roles Versus System Roles

- Special privileges
 - **EDIT_CREDENTIAL**: Edit a credential, except deleting it
 - **FULL_CREDENTIAL**: Full access to a credential, including deleting it
 - **GET_CREDENTIAL**: View-only access to a credential
 - **FULL_JOB**: Perform all valid operations on the job, library job, deployment procedure configuration, and deployment procedure instance
 - **FULL_DP**: Perform launch, create like, edit structure, and delete operations on a deployment procedure
 - **LAUNCH_DP**: Perform launch and create like operations on a deployment procedure
- Private Roles **can** include special privileges.
- System Roles **cannot** include special privileges.



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Sensitive privileges are handled in a special way in Cloud Control. These privileges can only be part of Private Roles. These special privileges are:

- **EDIT_CREDENTIAL**: Edit a credential, except deleting it. For example, change the password for a database user set as a preferred credential for all database types
- **FULL_CREDENTIAL**: Full access to a credential, including deleting it
- **GET_CREDENTIAL**: View-only access to a credential
- **FULL_JOB**: Perform all valid operations on the job, library job, deployment procedure configuration, and deployment procedure instance
- **FULL_DP**: Perform launch, create like, edit structure, and delete operations on a deployment procedure
- **LAUNCH_DP**: Perform launch and create like operations on a deployment procedure

System Roles cannot include special privileges. Private Roles, on the other hand, can include all other privileges.

Note that jobs and deployment procedures will be explained in more detail in an upcoming lesson.

Who Can Create Roles?

Administrator Type	Can create System Role	Can create Private Role with or without ADMIN option
Regular Administrator	X	X
Administrator with the MANAGE_SYSTEM_ROLE resource privilege	✓	X
Administrator with the CREATE_ROLE resource privilege	X	✓
Super Administrator	✓	✓



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Privileges and Roles: Best Practices

- Implement the Principle of Least Privileges.
- Simplify and centralize roles across the enterprise.
 - Use out-of-the-box roles.
 - Create roles that aggregate the out-of-the-box roles.
- Use privilege propagating groups.
 - Automatic access privileges to new targets
- Use read-only privileges where applicable.
 - Critical development systems
- Leverage the authorization management to external authorization tools.
 - Use External Roles
 - Auto-provisioning bonus: automatic creation of user accounts



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Cloud Control Initial Access: Best Practices

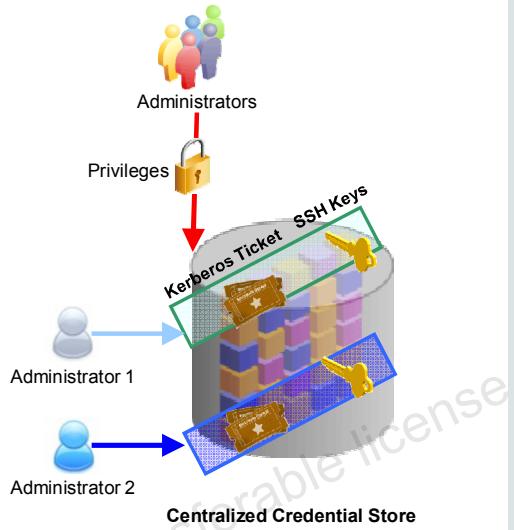
- Create Administrators:
 - Use out-of-the-box roles such as EM_ALL_VIEWER, EM_ALL_OPERATOR, EM_ALL_DESIGNER, and EM_ALL_ADMINISTRATOR.
 - Map to job roles.
- Administrators access:
 - Restrict access to SYSMAN.
 - Create new Super Administrator.
 - Change initial SYSMAN password.
 - Adjust logout period per company policy.



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Managing Securely with Credentials

- Centralized credential store for ease of management
- Support for managing password-less and strong authentication credentials (Kerberos tickets and SSH keys)
- Support for SUDO/PowerBroker
- Reuse and sharing among users (without disclosing the sensitive content of credentials)
- Controlled and protected access



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

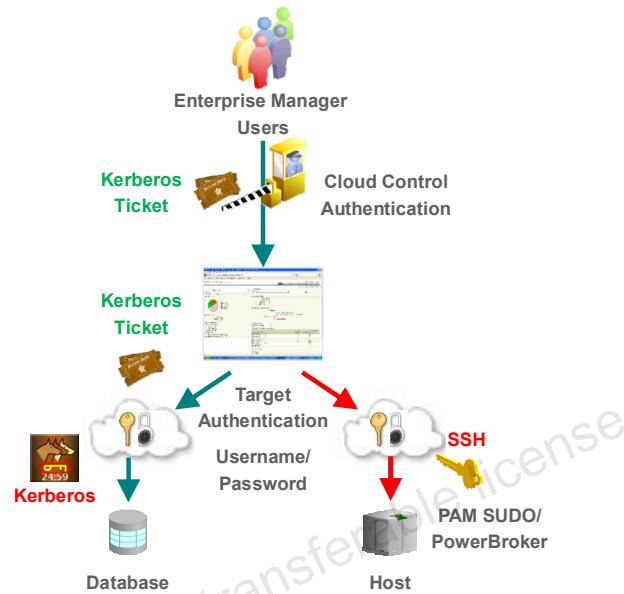
Because Cloud Control can perform a wide range of management tasks, managing credentials for hosts, databases, and many other target objects can be a real challenge.

Cloud Control controls access to targets via the Credentials subsystem. A centralized credential store keeps all credentials, saved by name. These named credentials support password-less and strong authentication schemes such as Kerberos tickets, SSH key pairs, and Public Key Infrastructure (PKI), and can be shared among many different users. Cloud Control also supports SUDO/PowerBroker-based impersonation.

Access to the credentials is controlled and protected by privileges.

Target Authentication

- Authentication schemes
 - Traditional username/password
 - SSH key pairs for hosts
 - PAM host authentication option
 - Kerberos tickets for database
- Seamlessly traverse between Cloud Control and database targets
 - Same credentials used for Cloud Control authentication and database target authentication



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Cloud Control supports strong authentication for host and database targets. You can use SSH key pairs for host authentication, as well as Kerberos tickets for database authentication.

The Cloud Control agent running on the managed hosts can authenticate that host by using traditional password file authentication or by using a Pluggable Authentication Module (PAM). PAM is a framework that allows administrators to specify other authentication mechanisms (such as LDAP, Kerberos, and RADIUS) to be used.

If you are using Kerberos tickets for both Cloud Control authentication and database authentication, you can seamlessly traverse between Cloud Control and the database targets without being prompted for database authentication. The same credential that is used for Cloud Control authentication is automatically used for database as well.

Target Access Using Credentials

- Various access types to targets
 - Monitoring
 - For collecting metrics on targets
 - Management tasks
 - Run jobs
 - Start/stop targets
 - Privileged tasks use hosts privilege delegation
- Named Credentials
 - Saved username/password, public key-private key pairs, or security certificates
- Secure access control to credentials
 - Controlled and protected by privileges
 - CREATE_CREDENTIAL privilege needed to create credential
 - VIEW, EDIT, and FULL privilege levels can be granted



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Targets are accessed in Cloud Control via the credentials subsystem, either for performing management tasks, such as running jobs, or for monitoring and collection of metrics. Monitoring credentials are unique because they are not directly used by the administrators, but the data collected using these credentials is organized and available to administrators based on their privileges. Monitoring credentials are specified at the time a target is discovered.

To perform operations like running jobs, patching, and other system management tasks, you can define and store credentials (username/password, a public key-private key pair, or security certificates such as an X509v3 certificate) as **Named** credentials. Named credentials are “placeholders” designed to simplify password management. Password input fields for credentials always use masking characters.

The ability to set privilege delegation for hosts was designed to allow privileged operations to be run as another privileged user without knowing sensitive information such as passwords. Cloud Control supports *SUDO* and *PowerBroker* to enable password-less and far more secure modes of running specific powerful jobs. Privilege delegation settings can also be saved as templates and applied enterprise-wide for standardization.

The access level to credentials varies and is determined by the owner of the credential, who must have the CREATE_CREDENTIAL privilege to create it. The following levels can be assigned to other administrators for a particular credential:

- **VIEW:** Grantee administrators can view nonsensitive details about the credential and use it in running jobs and other operations.
- **EDIT:** Grantee administrators can change sensitive information such as passwords and public-private key pairs.
- **FULL:** Grantee administrators have full privileges to a credential, including the ability to delete it.

Preferred Credentials

- Named credentials can be set as preferred credentials.
- Benefits include the simplified use of credentials for multiple administrators and targets of various types.

Who has access?	What is the access for?	Name of the Credential
Specific administrator	Specific target	Preferred Credential
Specific administrator	Multiple targets of the same type	Default Preferred Credential
Multiple administrators	Specific target	Global Preferred Credential
Multiple administrators	Multiple targets of the same type	Default Global Preferred Credential



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Global Preferred Credentials

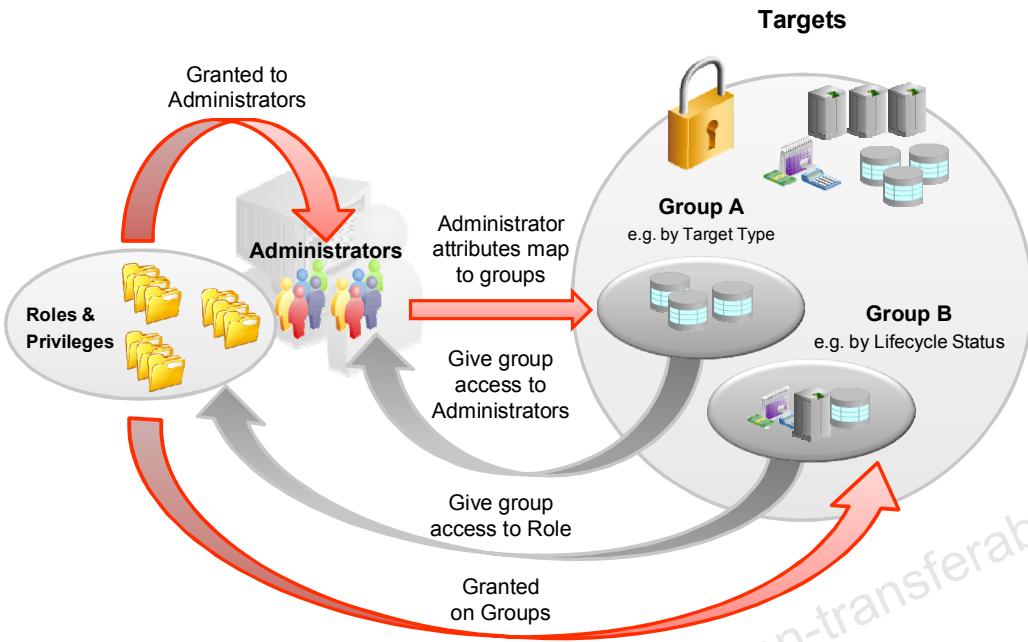
- Ideal for large managed systems with many administrators and many targets
- Automatic access to new targets

Task	Privilege needed
Set Global Preferred Credentials for a specific target	FULL_TARGET
Set Global Preferred Credentials for a specific target type	FULL_ANY_TARGET
Use Global Preferred Credentials	OPERATOR_TARGET



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Correlating Administrators, Roles, and Groups



ORACLE

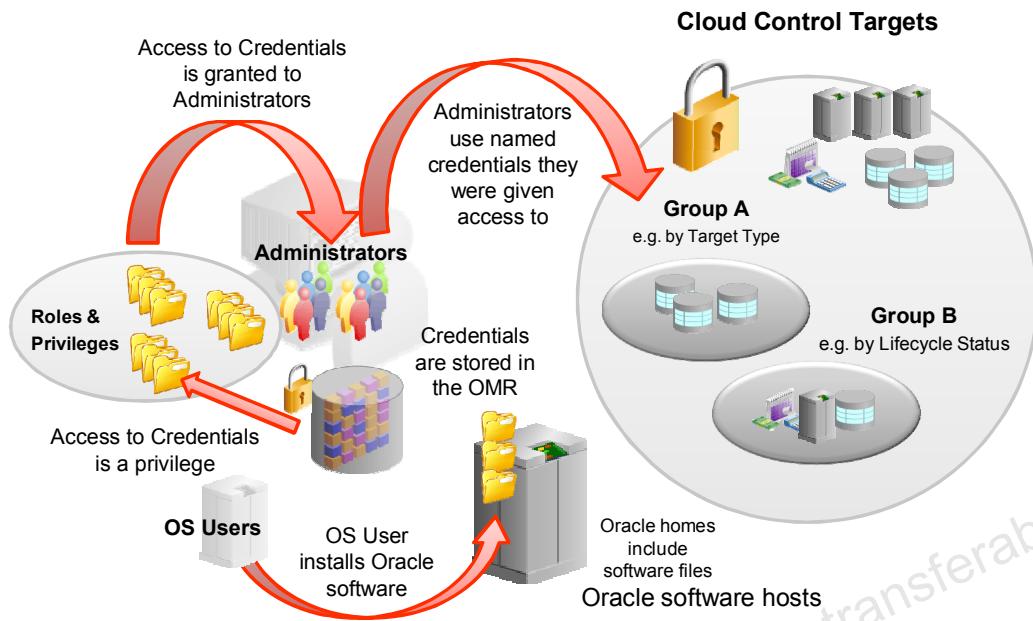
Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Bringing It All Together

Note in the slide how all the elements of authentication and permission within Cloud Control, namely administrators, roles, privileges, and groups, are interrelated:

- **Administrators** are the end-users of the Cloud Control console (users you log in as). These accounts are, by default, created within the Cloud Control repository but can also be linked to external technologies such as LDAP. Any administrator account links to login accounts via Privileges (individual grants of permissions) or **Roles** (aggregates of permissions and other roles).
- **Roles** (sets of privileges, to be used as best practice) or individual privileges can be granted to Cloud Control Administrators.
- Privileges and Roles provide permissions to individual targets or **groups** of targets, which means that any administrator with those roles will be given those privileges to that group of targets.
- Conversely, as a full-privileged group administrator, you can give access to your group to a specific role. This means that anyone with that role will have access to your group.
- Also as a full-privileged group administrator, you can give access to your group directly to individual Administrators.
- Administrators are defined with **attributes** such as Department, Line of Business, or any custom attribute and its corresponding list of values to choose from. Access to groups can be based on these attributes. So, for example, Administrators marked as part of a Department named *Development* are automatically given access to the targets that are also marked *Development*.

Correlating Administrators and Target Credentials



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

In the slide, note how administrators relate to access to various targets using credentials.

Administrators, again, are the end-users of the Cloud Control console. Privileges and Roles provide permissions to individual targets, groups of targets, or even to all targets. However, these permissions do not give administrators login access to targets. Login access to targets is provided using **Credentials**. Credentials required and used by Cloud Control are as follows:

- Credentials used to **install, upgrade, and patch** the Cloud Control system itself are not stored with Cloud Control; they are operating user credentials. The installation of Cloud Control components (repository, the OMS, and Software Library) uses a nonroot user account and group on the OS. The installation uses a directory that has full read/write permissions for that user/group combination. A privileged user account or privilege delegation tool (such as SUDO or PowerBroker) is required to execute the finish script, and may be required to apply some patches or upgrades. The OS-level repository database user account would be used when executing database scripts (SQL Plus, for example). The OS-level OMS user account would be used when running scripts (using EM CLI or emctl). Privileged permissions are typically not required to apply patch content for the OMS or its associated software. The directory associated with a Software Library requires full read/write/execute permissions for the user and group used to install and manage the OMS, and provides read/execute permissions to other user accounts.

- Target credentials are used to **perform management operations** on targets. Depending on the target type, some of these credentials may be OS-level user credentials. Target credentials are stored in a credentials store in the OMR and enable users to perform actions such as collecting metrics in the background or real-time, performing jobs such as backup, patching, and cloning, performing real-time target administration such as start and stop, or connecting to My Oracle Support. Administrators can only use credentials they were given access to or those credentials they own.

Quiz



System Roles can include special privileges (for example, the GET_CREDENTIAL privilege to view a credential).

- a. True
- b. False



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Quiz



You can give **group access** to a **role**.

- a. True
- b. False



Answer: a

Summary

In this lesson, you should have learned how to:

- Identify how access to Cloud Control targets is controlled
- Define roles and privileges and how they relate to groups
- Distinguish between various types of roles
- Describe target credentials and their types



Practice 5-1 Overview: Creating Roles and Administrators

This practice covers the following topics:

- Creating new roles for the following types of jobs:
 - DBA
 - Jr. DBA
- Creating new administrators and granting them the newly created roles
- Creating Named Credentials to be used by the new administrators



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Practice 5-2 Overview: Creating Named and Default Credentials

This practice covers the following topics:

- Creating or reviewing named credentials used by the following types of jobs:
 - DBA
 - Jr. DBA



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

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

This practice covers the following topics:

- Logging in as a new DBA role administrator
- Performing DBA-type tasks
 - Set up Backup and Recovery
 - Back up a tablespace



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

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

This practice covers the following topics:

- Logging in as a new Jr. DBA role administrator
- Performing Jr. DBA type of tasks
 - View targets access



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Unauthorized reproduction or distribution prohibited. Copyright© 2019, Oracle and/or its affiliates.

GANG LIU (gangl@baylorhealth.edu) has a non-transferable license
to use this Student Guide.

Monitoring

Design and Setup

ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Objectives

After completing this lesson, you should be able to:

- Explain the monitoring infrastructure and the process of creating standards for monitoring your enterprise
- Identify out-of-the-box monitoring settings
- Customize metric settings
- Create and apply monitoring templates and template collections, and relate them to Administration Groups
- Describe metric extensions



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

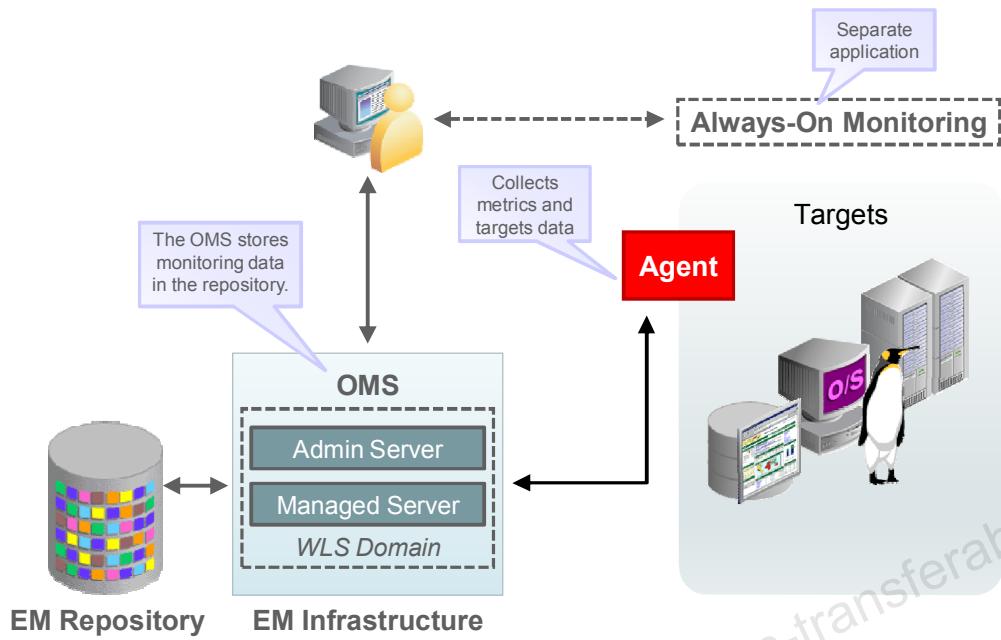
Cloud Control Monitoring: Overview

- Cloud Control monitoring functionality
 - In-depth monitoring with Oracle-provided metrics and suggested thresholds
 - Access to real-time performance charts
 - Collection, storage, and aggregation of metric data in the management repository to perform tasks such as trend analysis and reporting
- Monitoring and management for many target types
 - Generic and target-specific tasks
 - For example, database
 - Out-of-the-box monitoring for many target types



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Enterprise Monitoring with Cloud Control



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Because of the size, complexity, and criticality of today's enterprise IT operations, the challenge for IT professionals is to be able to maintain high levels of component availability and performance for applications and all components that make up the application's technology stack. Monitoring the performance of these components and quickly correcting problems before they can impact business operations is crucial.

The management agent on each monitored host monitors the status, health, and performance of all managed targets (such as database, application server, operating system, and hardware) on that host. If a target goes down, or if the performance metric crosses a warning or critical threshold, an event is generated and sent to the Oracle Management Service (OMS). By using the Cloud Control console, you can view the status of all the monitored targets.

Starting with Cloud Control 13c, you can also set up a separate instance for monitoring, called Always-On Monitoring, to continue monitoring mission-critical targets while the OMS is unavailable (for example, under maintenance).

Always-On Monitoring

- New service for core monitoring capabilities
 - Ensures continuous monitoring of critical targets
 - Handles target availability metrics and alerts
 - Sends notifications: email
- Separate Java application
 - Self-Updatable
 - Off by default
 - Recommended use: running at all times with notifications off
- One-time configuration
 - Dedicated repository
 - Upload URL to synchronize with the OMR
 - Targets information
 - Notification information: email addresses



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

For the highest availability solutions, a new monitoring capability is available with Cloud Control 13c and above: Always-On Monitoring. This service ensures that critical targets are continuously monitored even when the OMS is not available by sending notifications in the form of emails to administrators on call.

Always-On Monitoring is available as a separate Java application, updatable via Self-Update and configured as OFF by default. However, to keep the application in sync with Cloud Control at all times, it is recommended that you set it up running in the background and turn off only the notifications.

A one-time configuration process sets up its repository, connects to the Cloud Control repository via an upload URL, and automatically synchronizes information about targets and email addresses with the OMR.

For more details about Always-On Monitoring, be sure to watch the OLL demonstration titled “*System Broadcast and Always-on Monitoring with Oracle Enterprise Manager*.”

Defining Monitoring Standards

- Determine business requirements:
 - SLAs
- Determine the type of monitoring needed:
 - Performance
 - Availability
- Define monitoring elements:
 - Metrics to be collected
 - How often to collect metrics
 - Thresholds that metrics can reach before alerts are triggered
 - Corrective actions when alerts are triggered
- Group targets by monitoring types.

ORACLE

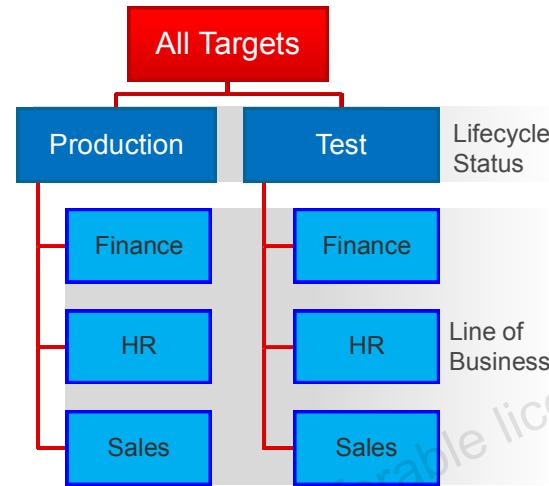
Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

How Do You Go About Setting Up Your Monitoring?

You must first determine your business requirements based on Service Level Agreements (SLAs) in order to decide what type of monitoring you need for your enterprise. Typically, you monitor for both performance and availability. This will decide the metrics to be collected and their collection cycle, metric thresholds, and any corrective actions needed should any alerts be triggered. Monitoring is best applied to groups of targets, so you may consider grouping also by the way targets need to be monitored.

Using Administration Groups for Monitoring

- Automatic and unique deployment of monitoring settings
 - One hierarchy per enterprise
- Automatic assignment of targets to groups based on membership criteria
 - Membership criteria are based on target properties.
 - Targets can only belong to one group in the hierarchy.
 - Users *cannot* directly add targets to the groups.
- Propagating privileges



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Administration groups are specifically designed to automatically deploy your management settings to a target as the target joins the group. You can only define one hierarchy of groups per enterprise, to ensure uniqueness, and privileges to the group automatically propagate to the group members.

You define the membership criteria first, based on predefined target properties such as contact, department, location, line of business, lifecycle status, target, type, target version, cost center, and customer support identifier. Then, Cloud Control will take the targets that match that membership criteria and assign them to the right groups. You indirectly control how targets are assigned to administration groups but you do not directly assign their group membership.

The example in the slide shows that all targets are first grouped by lifecycle status (Production and Test) and then by line of business, such as Finance, HR, and Sales.

Concept: Metrics and Metric Thresholds

- Metrics: Measurements of various properties of a managed entity
- Metric thresholds: Boundary values against which monitored metric values are compared
- Metric threshold values can be set for two levels of metric alert severity:
 - **Warning:** Attention is required in a particular area, but the area is still functional.
 - **Critical:** Immediate action is required in a particular area. The area is either not functional or indicative of imminent problems.



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Customizing Metric Settings

Must have the Manage Any Target Metric privilege

Task	Description
Customize metric threshold values.	Threshold values can be set to reflect the operational norms of your environment accurately. Advanced options include setting time-based or adaptive thresholds.
Set/modify metric collection schedules.	The collection schedule of a metric can be enabled or disabled. If enabled, you can define the schedule frequency and, for some metrics, a start time.
Set the number of occurrences that triggers the alert.	Define the consecutive number of evaluation cycles for which a metric has to cross its warning or critical threshold before a warning/critical metric alert is sent.
Customize alert message.	Modify an alert text message to apply to your environment.



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Some metric thresholds come predefined out-of-the-box for each target being monitored. Although these values are acceptable for most monitoring conditions, your environment may require customized threshold values to reflect the operational norms of your environment accurately. Advanced options include setting different fixed thresholds for specific time windows (time-based) or allowing the system to calculate thresholds automatically and set them dynamically (adaptive thresholds).

Metrics are collected for each managed target at predefined collection schedules. The upload interval determines how often a metric value is uploaded to the management repository. For example, if a metric value is collected every five minutes and the upload interval is set to six (every sixth collection), the metric value is uploaded every 30 minutes. It is recommended that you use the Oracle default values for the collection schedule of a metric. If you do need to change it, be careful when changing the collection schedule to intervals of less than five minutes. If the metric value does not change too frequently, this will cause unnecessary work for the agent. Changing the collection schedule may also affect data collection for other related metrics and/or compliance rules. Before changing the collection schedule, check the Affected Metrics list to determine the impact of changing the collection settings.

In addition to setting warning and critical thresholds, you can set the number of occurrences when monitoring a single object. This parameter allows you to define the alert sensitivity by permitting metric data sampling over a period of time. This prevents sporadic spikes in collected data from triggering an alert.

Specifically, the metric has to cross its warning or critical threshold for a consecutive number of evaluation cycles (equivalent to the number of occurrences) before a warning/critical alert is sent.

Number of occurrences determines the period of time a collected metric value must remain above the threshold value before an alert is triggered. For example, if a metric value is collected every five minutes and the number of occurrences is set to six, the metric values (collected successively) must stay above the threshold value for 30 minutes before an alert is triggered.

An alert message comes with a predefined text message, but it can also be customized for your specific environment.

You must have the “Manage Any Target Metric” privilege on the target to make changes. Without this privilege, the content of the Metric Threshold table will be read-only.

Concept: Monitoring Templates and Template Collections

- Monitoring Templates
 - Collections of monitoring settings for specific target types
 - Can be used individually
 - Recommended use: grouped
- Template Collections
 - Set of Monitoring Templates
 - Include one monitoring template per target type
 - Are associated with an administration group
 - Management settings automatically propagate to targets
 - Inherited by new targets as well



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Using Monitoring Templates and Template Collections

- Create Monitoring Templates:
 - Define the target type to which the template applies:
 - Use the Create-Like functionality.
 - Include applicable metrics, thresholds, and metric collection schedules.
 - Add metrics extensions, if used.
 - Add corrective actions.
- Create Template Collections:
 - Add existing templates and save.
- Make use of Template Collections:
 - Apply a template collection to an administration group:
 - Ensures that any changes are applied to the monitored targets
 - Set or confirm the global synchronization schedule.
 - Targets are automatically synchronized with the selected items.



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

You can start creating and using templates once your target properties have been defined and you have designed your administration group hierarchy by grouping together targets that are monitored in the same way.

Templates define the target type to which the template applies and list the metrics of interest, metrics extensions, metrics thresholds, metric collection schedules, and corrective actions. You may be using the Create-Like functionality and create templates based on Oracle's predefined templates.

At this point, you can use templates individually (ad hoc) across one or more targets or groups. However, the recommended next step is to create Template Collections.

When using templates ad hoc, if a change is made to a template, you need to manually reapply the template across affected targets in order to propagate the new changes. For any target, you can preserve custom monitoring settings by specifying metric settings that can never be overwritten by a template. When a template is applied to a target, any monitoring settings not specified in the template remain unaffected on the target.

When templates are added to a template collection, on the other hand, you are guaranteed that settings are applied to their target type in the administration group hierarchy. You can only have one monitoring template of a particular target type in the template collection. When you associate a template collection with administration groups, you set or confirm a global synchronization schedule and Cloud Control automatically performs the synchronization of the targets with the selected items.

Additional Information on Working with Individual Templates

Enterprise Manager Cloud Control includes templates for monitoring Oracle target types, such as Oracle WebLogic Domain, Oracle home, Oracle Fusion Middleware Farm, Metadata Repository, Listener, Database Instance, Application Deployment, Oracle WebLogic Server, Host, and Agent.

You can view these templates and any others that your organization might have on the Monitoring Templates page. This page provides the starting point for your tasks, which include working with the monitoring templates. Note that the correct privilege level is required.

You can use predefined templates as a starting point (with Create Like) or create a new monitoring template. Templates can be edited and, if no longer needed, they can be deleted.

Compare and *Apply* operations are needed only when you work with individual templates. When a monitoring template is used as part of a template collection, these operations occur automatically based on their assignment to an administration group.

When you have an individual template version that you want to use, it is recommended that the template is compared with the targets before applying the template to the targets.

The **Compare Settings** functionality provides details about how metric settings defined in a template differ from those defined at the destination target. The Compare functionality is especially useful when working with aggregate targets, such as groups and systems. For example, after you apply a monitoring template to a group, you want to verify that the group members now have the same monitoring settings as the template. Compare Settings makes checking simple. You can also schedule this as a report, allowing you to check periodically if the group members still follow the template settings.

Monitoring templates are independent of the targets to which they are applied. After a template is applied, if you make subsequent changes to the template, you must reapply the template to any of the applicable targets in order for the changes to be propagated to these targets. Conversely, any monitoring settings changes made to individual targets will not appear in the template. The most common use case is to apply a monitoring template to a group.

Two template *Apply* options are available:

- **Template will completely replace all metric settings in the target:** All metrics defined in the template are applied to the target. Pre-existing target monitoring settings are disabled. Metric thresholds will be set to NULL or blank. This effectively eliminates alerts from these metrics by clearing current severities and violations.
- **Template will only override metrics that are common to both template and target:** Only metrics common to both the template and target are updated. Existing target metrics that do not exist in the template remain unaffected. When this option is selected, additional template apply options are made available for metrics with key value settings.

When an individual template is applied, the *Apply* operation is performed asynchronously, one for each target to which the template is applied.

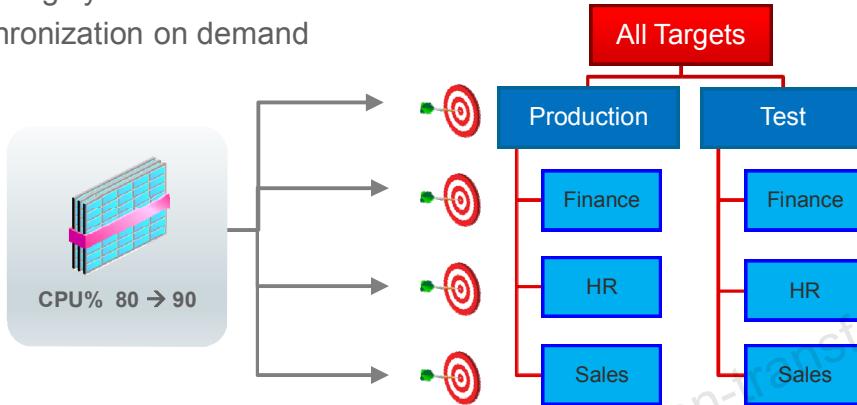
You can select any existing monitoring template and export it to an XML file by clicking Export. For any monitoring template that has been exported to an XML file, you can add it back as an active template by clicking Import. You can only export/import metric templates between the same Cloud Control versions.

Cloud Control allows you to set default monitoring templates that are automatically applied to newly added targets, thus allowing you to apply monitoring settings that are appropriate for your monitored environment.

Note: Super administrator privileges are required to define default monitoring templates.

Example of Template Modifications

- Underlying monitoring template is edited
- Automatic synchronization of target with the change
- Performed by Cloud Control in one of the following ways:
 - Recurring synchronization schedule
 - Synchronization on demand



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

What happens if templates that are part of a template collection need to be modified?

For example, you determined that a threshold in one of the templates needs to be adjusted. How do you do it?

First, edit the underlying monitoring template that contains those settings (for example, the CPU threshold must be changed to 90% instead of 80%).

Cloud Control ensures that the change is deployed across the targets through the process of “synchronization.” Synchronization can be done as part of regular maintenance work (you can specify the schedule, such as every midnight) or on demand.

Keeping Targets and Templates Synchronized

- Applied Template Collections are a “source of truth” for metrics settings.
- Cloud Control maintains settings integrity:
 - Cannot delete a template that is part of a template collection
 - Cannot apply ad hoc templates to administration groups or targets in administration groups
 - Informational message about affected template collections and targets when editing a monitoring template
- Cloud Control allows settings exceptions:
 - Warning while editing a target’s metric settings
 - Can enable “Prevent Template Override”
 - Keep target-specific settings
 - Can disable “Prevent Template Override”
 - Synchronize targets according to schedule



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

When a target joins an administration group, it is synchronized with the applicable template(s) in the associated Template Collections, according to the synchronization schedule. These templates become the “source of truth” for the defined monitoring settings, unless exceptions are defined.

Cloud Control maintains the integrity of the monitoring settings by:

- Preventing the deletion of a template that is part of a template collection
- Disallowing ad hoc template apply operations on administration groups or targets that are part of administration groups
- Displaying a message about affected template collections and targets if a monitoring template is being edited

In some cases, metrics for specific targets may need to be different from the template settings. These exceptions can be handled by manually editing the metric settings. Cloud Control will then:

- Present a warning message and allow you to override settings for a specific target.
- Give you the option to:
 - Enable “Prevent Template Override,” in which case the target will NOT be scheduled for synchronization, thereby preserving the manual settings.
 - Disable “Prevent Template Override,” in which case the target will be scheduled for synchronization and allow the old setting to override the manual setting.

The Administration Group home page has a Synchronization section that specifies the current synchronization status of your targets. Administrators should review this periodically.

Administration Groups and Template Tasks Prerequisite Privileges

Task	Cloud Control Privilege
Create administration group hierarchy.	Full Any Target Create Privilege Propagating Group
Create a monitoring template.	None
Use a specific monitoring template.	View on the target
Create template collections.	Create Template Collection resource privilege
Use template collections.	View or Full (on a specific template collection) or View Any Template Collection
Associate Template Collection with Administration Group.	Operator on the group View Any Template Collection



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Extending Your Monitoring Scope

- Metric extensions (MEs):
 - Allow you to extend Enterprise Manager's monitoring scope to meet your data center needs
 - Can be defined for any target type
 - Can be used in any feature that uses metrics
 - Are mechanisms for collecting metric data: SQL script, OS script, SNMP, and JMX
- Scripts can generate multiple metric values.



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

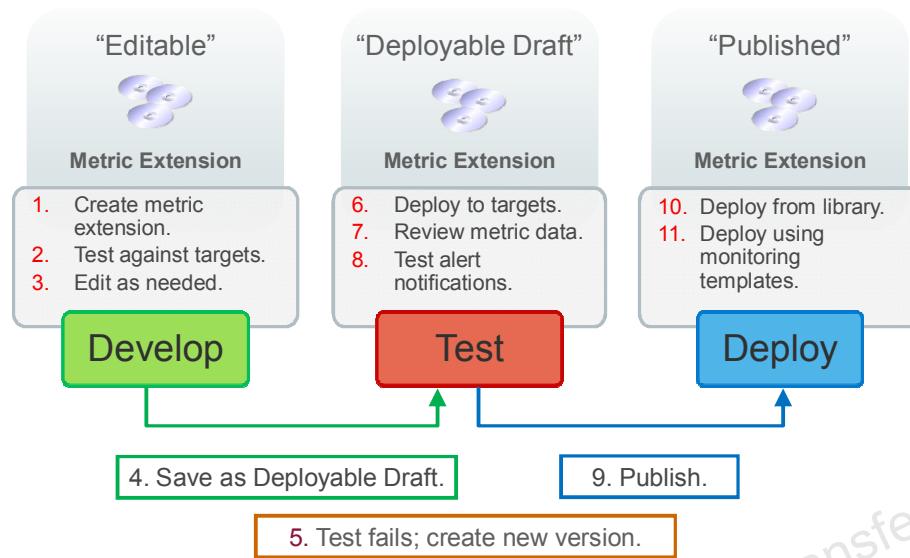
If the predefined (out-of-the-box) metrics do not cover all of your monitoring needs, then you can define extensions to Enterprise Manager's monitoring scope, so that you can meet your data center needs.

A metric extension (ME) can be defined for any target type in Enterprise Manager. A wizard guides you through the workflow. When you have defined a metric extension, it can be used in any feature in Enterprise Manager that uses metrics.

Mechanisms for collecting metric data include SQL script, OS script, SNMP, and JMX. Multiple metric values can be returned to your script in a metric extension.

Note: All the mechanisms that Oracle's own developers use to collect metric data are exposed to you as well.

Developing and Deploying Metric Extensions



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The graphic in the slide shows (from left to right) the development and deployment life cycle of a metric extension. The first phase is the development, during which the ME is “editable.” It can be changed, tested, and so on.

When the metric is ready for testing by others, you save it as a “deployable draft.” It can now be deployed against a target and start collecting metric data, thresholds can be placed on it, and alerts generated, as it would when the metric extension is ultimately deployed in a production environment. If you find problems at this stage, you create a new version of the metric extension and edit it as needed.

When the metric extension meets your requirements, you can publish it. Then, it is available for general use. You can deploy MEs from the metric extension library or through monitoring templates. (The numbered activities in the graphic might not all occur. The numbers merely indicate a likely workflow.)

Two demonstrations cover this topic. Even though they may be older demonstrations, the basic flow still applies.

- **Using Metric Extensions - Part I:** Shows you how to create and test a metric extension for a host target type
- **Using Metric Extensions - Part II:** Shows you how to deploy the previously created metric extension and view the results

Securely Dividing Metric Extension Tasks

User Roles	Role Tasks	Privileges
Metric Designer	<ul style="list-style-type: none">Designs and creates new metric extensionsTests and publishes metric extensionsDevelops new versions of metric extensions	<ul style="list-style-type: none">Create Metric ExtensionManage Target Metrics (per target)Full Metric Extension (per metric extension)Edit Metric Extension (per metric extension)
Target Administrator (DBAs, middleware administrators, system administrators, and so on)	<ul style="list-style-type: none">Consumer of the metric extension(s)Deploys metric extensions to targetsUses metric extension functionality	<ul style="list-style-type: none">Manage Target Metrics (per target)



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Typically, there are two users involved in the use and creation of metric extensions. The first of these is the **metric designer**, who is responsible for the design and creation of new metric extensions, as well as testing and publishing MEs and developing new versions as needed. The second user is the **target administrator**, who uses MEs. This may be a DBA, middleware administrator, system administrator, and so on. The target administrator is responsible for deploying the ME to its targets.

To support these operations, a metric designer typically needs:

- The Create Metric Extension resource privilege
- The per-target Manage Target Metrics privilege to deploy the metric extension to a target
- The Full Metric Extension and Edit Metric Extension privileges on a per-metric extension basis to work on other authors' metric extensions

The target administrator needs the Manage Target Metrics privilege to deploy metric extensions.

Quiz



Using monitoring templates, you can:

- a. Apply standardized monitoring settings
- b. Specify monitoring settings once and apply them as often as needed
- c. Save, edit, and apply these templates
- d. Apply the template only to targets of the same type
- e. All of the above



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Quiz



You can apply monitoring templates on:

- a. Targets
- b. Groups
- c. Both



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Summary

In this lesson, you should have learned how to:

- Explain the monitoring infrastructure and the process of creating standards for monitoring your enterprise
- Identify out-of-the-box monitoring settings
- Customize metric settings
- Create and apply monitoring templates and template collections, and relate them to Administration Groups
- Describe metric extensions



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Practice 6-1 Overview: Reviewing the Oracle-Provided Monitoring Templates

This practice covers the following topics:

- Reviewing host metrics
- Changing thresholds



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The Cloud Control 12c demonstrations that are still relevant for this lesson include:

- **Monitor a Target:** Shows you how to view metrics, thresholds, and collection settings (where they are defined), and host target values (your current monitoring information). The demonstration also shows context-sensitive help for metrics, pointing to additional information to help you evaluate the monitoring data.
- **Administer Monitoring Templates:** Shows you how to view Oracle-provided templates, how to create a new template, compare its settings to a target, and how to apply the template

For advanced use:

- **Using Metric Extensions - Part I:** Shows you how to create and test a metric extension for a host target type
- **Using Metric Extensions - Part II:** Shows you how to create and deploy the previously created metric extension and view the results

Practice 6-2 Overview: Creating a Monitoring Template

This practice covers the following topics:

- Creating a monitoring template
- Comparing and applying a monitoring template
- Comparing metric settings



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The demonstrations relevant for this lesson include:

- **Monitor a Target:** Shows you how to view metrics, thresholds, and collection settings (where they are defined), and host target values (your current monitoring information). The demonstration also shows context-sensitive help for metrics, pointing to additional information to help you evaluate the monitoring data.
- **Administer Monitoring Templates:** Shows you how to view Oracle-provided templates, how to create a new template, compare its settings to a target, and how to apply the template

For advanced use:

- **Using Metric Extensions - Part I:** Shows you how to create and test a metric extension for a host target type
- **Using Metric Extensions - Part II:** Shows you how to create and deploy the previously created metric extension and view the results

Practice 6-3 Overview: Applying a Monitoring Template Using a Template Collection

This practice covers the following topics:

- Creating a template collection
- Reviewing privileges required to work with templates
- Associating a template collection with an Administration Group
 - As a user with a defined role



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The demonstrations relevant for this lesson include:

- **Monitor a Target:** Shows you how to view metrics, thresholds, and collection settings (where they are defined), and host target values (your current monitoring information). The demonstration also shows context-sensitive help for metrics, pointing to additional information to help you evaluate the monitoring data.
- **Administer Monitoring Templates:** Shows you how to view Oracle-provided templates, how to create a new template, compare its settings to a target, and how to apply the template

For advanced use:

- **Using Metric Extensions - Part I:** Shows you how to create and test a metric extension for a host target type
- **Using Metric Extensions - Part II:** Shows you how to create and deploy the previously created metric extension and view the results

Unauthorized reproduction or distribution prohibited. Copyright© 2019, Oracle and/or its affiliates.

GANG LIU (gangl@baylorhealth.edu) has a non-transferable license
to use this Student Guide.

Managing Events and Incidents

ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Objectives

After completing this lesson, you should be able to:

- Describe the use of events, incidents, and problems in Enterprise Manager Cloud Control
- Access Incident Manager to manage events, incidents, and problems
- Perform incident lifecycle operations



Goals of Incident Management

- Monitor and resolve service disruptions quickly and efficiently:
 - Manage fewer disruptions
 - Intelligent associations based on root cause analysis
 - Manage in a more meaningful manner
 - By business priority
 - Across life cycles
- Provide a centralized evaluation and resolution console:
 - Manage **events, incidents, and problems.**
 - Identify, resolve, and eliminate root causes of disruptions.
 - Integrate Oracle expertise to accelerate incident and problem diagnosis, and resolution.
 - Assign, acknowledge, prioritize, track status of, escalate, suppress, or open a helpdesk ticket.



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The goal of incident management is to enable you to monitor and resolve service disruptions that may be occurring in your data center as quickly and efficiently as possible. Instead of managing the numerous discrete occurrences that may be raised as the result of service disruptions, you can manage a smaller number of problems with the same root cause, or in a more meaningful manner, based on business priority and across their life cycle.

Cloud Control's Incident Management subsystem is aimed at providing a single centralized console that will enable you to track, diagnose, and resolve these issues.

The **Incident Manager** interface gathers data from the underlining monitoring system and reports on:

- **Events:** Any significant occurrence indicating problematic behavior for one or more managed entities (for example, a metric alert or a violation of a set rule)
- **Incidents:** A significant single event or a set of related events that are found to represent the same issue
- **Problems:** The root cause of incidents that correlate to issues with the Oracle software and logged into a special repository called Advanced Diagnostic Repository (ADR)

Incident Manager includes features to tie in to Oracle expertise via relevant My Oracle Support knowledge base articles and documentation to enable administrators to accelerate the process of diagnosing and resolving incidents and problems. Incident Manager also offers the ability to perform lifecycle operations for incidents, so you can assign ownership of an incident to a specific user, acknowledge an incident, set priority for an incident, track an incident's status, escalate or suppress it, or even raise notifications and open a helpdesk ticket via the helpdesk connectors.

Understanding Events

- Significant occurrences related to a managed entity
- Attributes:
 - Type
 - Raising entity
 - Message
 - Timestamp
 - Category
 - Severity

Fatal	
Critical	
Warning	
Advisory	
Informational	

Examples of event types:

- Target Availability
- Metric Alert
- Job Status Change
- Compliance Standard Violation Event
- Metric Evaluation Error
- Service Level Agreement (SLA) Alert
- High Availability
- JVM Diagnostics Threshold Violation
- User-reported event

ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

An event is a significant occurrence detected by Cloud Control related to one or more managed entities (such as a target or a job) at a particular point in time, which can indicate normal or problematic behavior. Each event has a set of attributes: the event type, the severity, the object or the entity on which the event is raised (typically a target but it can also be a job or some other object), the message associated with the event, the timestamp (when the event occurred), as well as the functional category (such as availability or security).

Event severities could be:

- **Fatal:** Specifically associated with the target availability event type, triggered when a target is down
- **Critical and Warning:** Can occur when metric thresholds exceed set values
- **Advisory:** Typically associated with compliance standard violation events
- **Informational:** Indicate simply that an event has occurred, but there is no need to do anything about it

Cloud Control supports a number of event types. Some examples are shown in the slide.

Understanding Incidents

- Significant occurrences related to a managed target
- Created automatically based on rules or defined manually
 - Can be based on one significant event
 - Example: A Target Down event produces an incident based on a system-generated rule.
 - Can include a group of events related to the same underlying issue
- Incident attributes help manage incidents:
 - **Summary:** Based on event details
 - **Owner:** Existing Cloud Control administrator
 - **Status:** New, work in progress, or resolved
 - **Priority:** Set usually by the owner
 - **Escalation level:** The priority within your organization
 - **Comment:** Additional information



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Incidents are significant occurrences related to a managed target in Cloud Control. Incidents can be based on one significant event or on a combination of events that are related, and may be automatically or manually created.

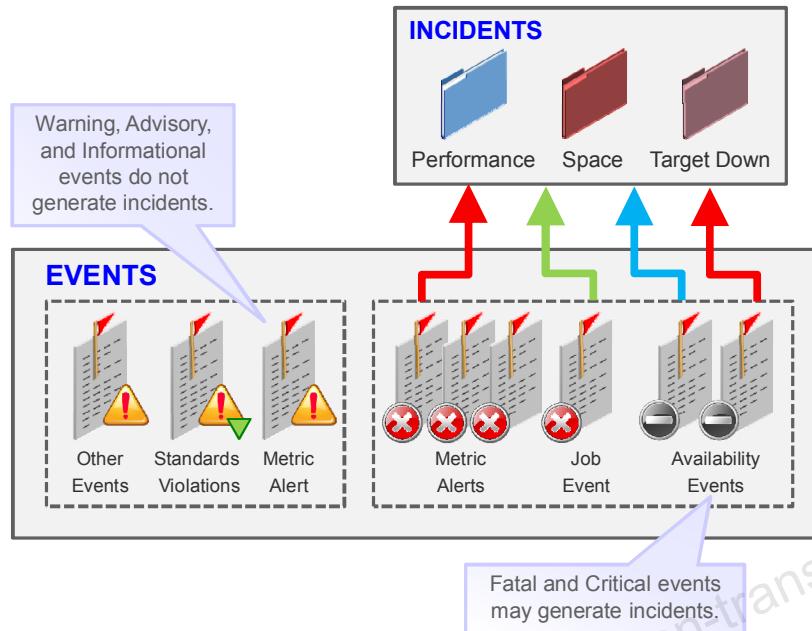
For example, a Target Down event automatically produces an incident based on a system-generated rule (built into Cloud Control; to be discussed later). This is an example of an incident based on a single event.

Cloud Control determines which events are significant and which ones are related to the same underlying issue, and presents this information in the Incident Manager.

Incidents can be managed from the Incident Manager interface by setting their attributes based on an adopted company-wide incident management policy. Incidents can have the following attributes:

- **Summary:** Based on event details
- **Owner:** An existing Cloud Control administrator, initially the target owner that can later be assigned to the administrator on duty
- **Status:** *New, Work in Progress, or Resolved*
- **Priority:** Set usually by the owner to values such as *Urgent, Very High, High, Medium, or Low*
- **Escalation level:** Used to set a priority for that issue within your organization, predefined values *Level 1* through *Level 5*
- **Comment:** A field for any additional information the administrator may find important

Distinguishing Between Incidents and Events



ORACLE

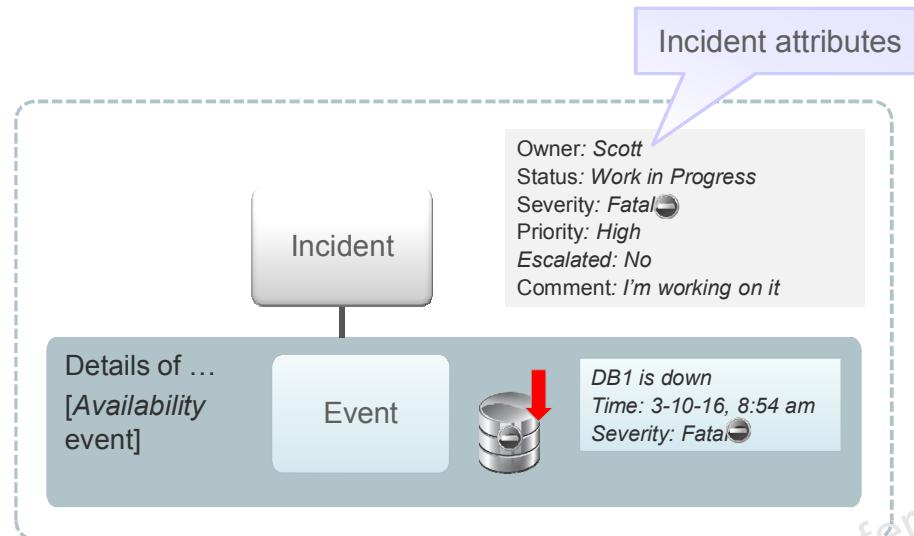
Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Cloud Control monitors the entire software stack from applications and databases to hosts and the operating system. When Cloud Control detects issues in any of this infrastructure, it raises events. Example of events (as shown in the graphic in the slide) include the following:

- Target availability, an event raised when a target is down or an agent is unreachable
- Metric alerts, raised when a metric crosses its threshold (for example, CPU utilization or tablespace usage alerts)
- Job status change event, raised, for example, when a job fails
- Compliance standard violation event, raised when there is a violation of a compliance standard
- Other events, such as SLA alerts and user-reported events

An incident is based on one or more events. For example, “running out of space” events raised from database, host, and storage can all be part of one incident. Note that Warning, Informational, or Advisory type of events will not generate incidents, while Fatal and Critical events may generate incidents.

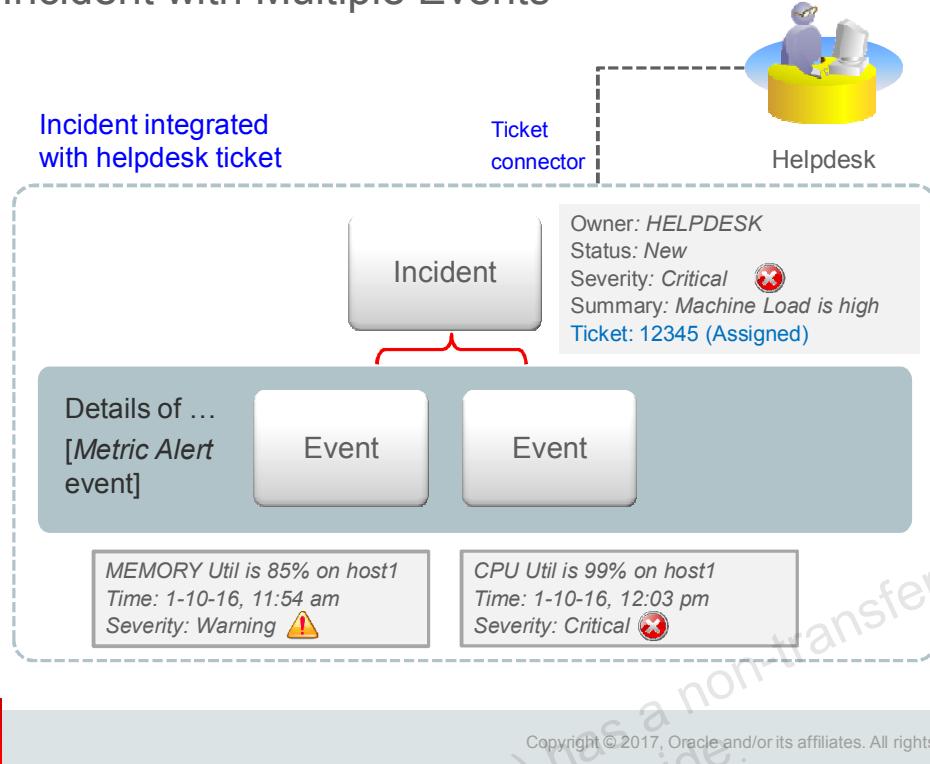
Example: Incident with One Event



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Example: Incident with Multiple Events



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The graphic in the slide shows an example of an incident (large rectangle) that contains two events (in the small rectangle).

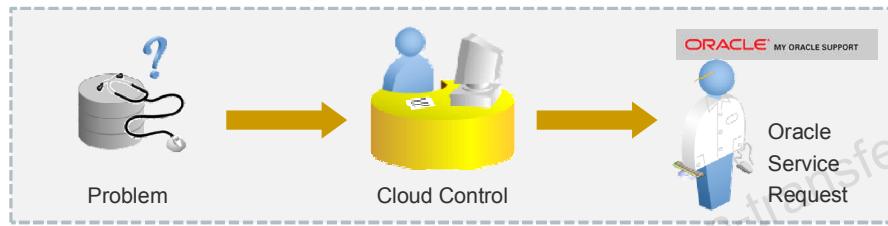
The events are related and point to the same underlying cause. They are two metric alert events on a host target—a memory utilization metric alert event and a CPU utilization metric alert event—because the host experiences a heavy load. In the example, you see a warning severity memory utilization metric alert event, and a short time later, a critical severity CPU utilization metric alert event.

An incident (large rectangle) is manually created by an administrator based on these two events to help manage, track, and resolve the issue. The incident attributes in the example include Owner, Status, Severity, Summary, and optionally, Ticket.

- Cloud Control automatically assigns the incident severity based on the worst case event severity of all the events contained in the incident (in this example, Critical).
- The incident has a summary, which is a short description of the incident. The individual events indicate that the machine load is high. You can write your own summary or let it default to the message of the last event in the incident.
- If you are using one of the helpdesk connectors to interface to a helpdesk system, an incident can result in a helpdesk ticket. Within Cloud Control, you can track both the ticket number and the status of that particular ticket.

Understanding Problems

- **Problem:** Underlying root cause of one or more incidents
 - Oracle software errors
 - Logged in to the Automatic Diagnostic Repository (ADR)
- Cloud Control functionality to facilitate error resolution:
 - Auto-creation of problems based on ADR errors
 - Packaging of diagnostic data
 - Ability to open Oracle service requests (SRs)



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Monitoring Oracle Software Problems

- Automatic problem generation functionality:
 - An ADR incident generates one Cloud Control problem per occurrence.
 - Flood control applies
 - Multiple ADR incidents with the same problem signature (for example, same root cause) generate one problem.
- Managing software problems in Incident Manager:
 - Track status (assign ownership and so on)
 - View diagnostic information (via Support Workbench)
 - Open Oracle SR (via Support Workbench)
 - Note the status of diagnostic activity visible in the UI:
 - Diagnostic data packaged (yes/no)
 - SR and Bug numbers

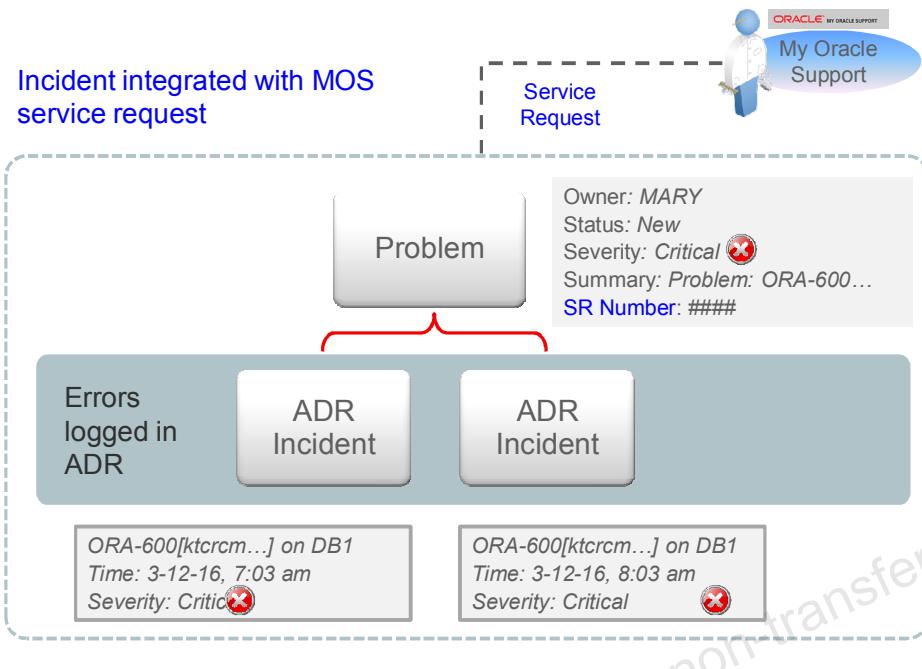


Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

When an ADR incident is raised, Cloud Control automatically generates a problem. All the ADR incidents that have the same problem signature (that is, the same root cause) are linked into a single problem object. To prevent potential flooding of the Incident Manager with hundreds of messages due to the same problem, starting with Cloud Control 12.1.0.4, the diagnostic incidents are, by default, limited to 5 records per hour and 25 records per day, for any given target and problem key combination. All incidents, however, continue to be recorded in the ADR.

You can manage problems in the Incident Manager in the same way as you would manage an incident, so you can assign an owner to the problem, track the resolution, and so on. In addition, there are in-context links to the Support Workbench functionality. This allows the administrator to package the diagnostic material, open a service request, and view the status of diagnostic activity, such as the SR number and ultimately bug number (if one is generated), within the user interface.

Example: ADR Incidents and Cloud Control Problems



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

When an ADR incident occurs, ADR sends a diagnostic alert to Cloud Control. The graphic in the slide shows an example of one Problem, or critical error (large rectangle), created for two separate ADR incidents (in the small rectangle).

Two ADR errors occurred in the example with two ORA-600 errors in the DB1 database. Both of these incidents are of critical severity. Cloud Control automatically creates a problem containing those ADR incidents. Within the Incident Manager user interface, you can link to the Support Workbench to open a service request (SR) with My Oracle Support (MOS). SRs can then be tracked directly from Incident Manager.

Enterprise View of Incident Manager

- Central location for all incidents
 - Ease of management
 - Ability to search and filter
 - Consolidated view helps correlate incidents
- Can perform common incident and problem tasks
 - Respond to an incident or problem
 - Manage and automate
 - Suppress
 - Filter Incidents, Problems, and Events using views
- Incident Dashboard
 - Summaries of open incidents and problems
 - Real-time data, auto-refresh option
 - Customizable views



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The Incident Manager is the central location for managing incidents. You can search, view, edit, and resolve incidents and problems affecting your environment. Use Incident Manager to perform the following tasks:

- Respond to an incident or problem
- Manage and automate
- Suppress
- Filter Incidents, Problems, and Events using views

The Incident Dashboard is designed to provide summaries of open incidents or problems, highlighting key areas such as incidents of fatal severity, escalated incidents, and unassigned incidents. This filtered view of incidents can be set up to refresh automatically providing real-time updates, and can be customized to display data and charts that are relevant to your business.

Performing Incident Lifecycle Operations

What you can do with Incident Manager:

- Update the status of an incident or problem.
- Identify the owner working on an incident or problem.
- Change priority of an incident or problem.
- Escalate an incident or problem.
- Add comments.
- Acknowledge an incident or problem.
- Edit the summary of an incident or problem.
- Suppress an incident or problem.
- Perform Root Cause Analysis on Target Down events.



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Using the General tab in the Details section of the Incident Manager page, you can perform the following tasks:

- **Update the status of an incident or problem:** Click Manage and change Status field.
- **Identify the owner working on an incident or problem:** Click Manage and add the name of owner in the Owner field.
- **Change the priority of an incident or problem:** Click Manage and change the Priority field.
- **Escalate an incident or problem:** Click Manage and choose the appropriate Escalation.
- **Add comments:** Either click Add Comment and type the comment or click Manage and type the Comment.
- **Acknowledge an incident or problem:** Click Acknowledge.
- **Edit the summary of an incident or problem:** Click More and select Edit Summary.
- **Suppress an incident or problem:** Click More and select Suppress.

Starting with Cloud Control 12.1.0.3, you can view Root Cause Analysis (RCA) on Target Down events (Target Availability type of events). This is automatically performed by the incident management framework to determine if a target down event is a root cause or a symptom.

Who Can Use Incident Manager?

- Access privileges based on the object of origin.
 - Event based on original target
 - Incident based on original event
 - Problem based on original ADR incident
- Levels
 - **VIEW** privileges on a target: View and add a comment to an event
 - **MANAGE_TARGET_ALERTS**: Full access to events
 - **OPERATOR_TARGET**: Includes **MANAGE_TARGET_ALERTS**

ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Quiz



Incident Manager provides:

- a. Wizards for setting up target credentials
- b. Interfaces to create groups
- c. Context-sensitive guided resolutions for incidents and Oracle software problems



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Quiz



Problems reported in Incident Manager are based on:

- a. Events
- b. ADR incidents
- c. Cloud Control incidents
- d. Nothing; no problems are ever reported in Incident Manager



Answer: b

Summary

In this lesson, you should have learned how to:

- Describe the use of events, incidents, and problems in Enterprise Manager Cloud Control
- Access Incident Manager to manage events, incidents, and problems
- Perform incident lifecycle operations



Practice 7-1 Overview: Preparing an Incident

This practice covers the following topics:

- Introducing a problem to trigger an incident
- Overview of the Incidents Dashboard



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Practice 7-2 Overview: Finding and Resolving an Incident

This practice covers the following topics:

- Finding an incident
- Resolving an incident



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Unauthorized reproduction or distribution prohibited. Copyright© 2019, Oracle and/or its affiliates.

GANG LIU (gangl@baylorhealth.edu) has a non-transferable license
to use this Student Guide.

Responding to Events, Incidents, and Problems

ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Objectives

After completing this lesson, you should be able to:

- Define incident rules
- Describe notifications and their options
- Define corrective actions in response to incidents and problems
- Distinguish between blackouts and notification blackouts

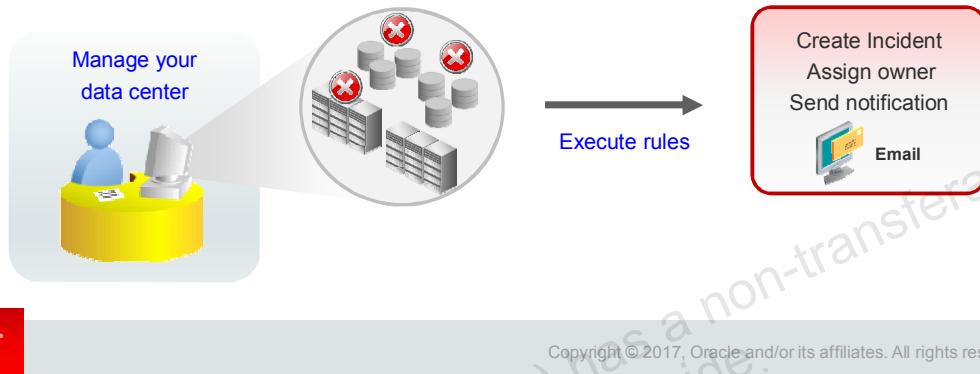


ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Why Do You Need Incident Rules?

- Designed to automate actions related to events, incidents, and problems
 - Can be grouped into sets
- Common uses:
 - Automatic creation of an incident based on an event
 - Notification actions (including ticketing)
 - Operations to manage incident workflow



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Incident rules enable you to manage the automation of business processes relating to incidents, problems, and events. They are instructions for an action to be performed in case of an event, an incident, or a problem.

Some of the common scenarios or use cases for incident rules include creating an incident based on an event, sending notifications such as email messages or pages as well as opening helpdesk tickets, or automating incident workflow actions, such as automatically assigning the owner of an incident or escalating an incident after it has been open for some time.

What Is an Incident Rule?

- Instruction that automates response actions
- Predefined rules provided out-of-the-box
- Operating on incoming events, incidents, or problems
- Consisting of:
 - Selection criteria (*for whom*)
 - Condition (*when*)
 - Response or rule action (*what*)

RULE CRITERIA	RULE CONDITION	RULE ACTION
CPU Util (%), Tablespace Used (%) metric alert events of warning or critical severity	--	Create Incident
Incidents of warning or critical severity	If severity = critical If severity = warning	Notify by page Notify by email
Incidents open for more than seven days		Set escalation level to 1

ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

An **incident rule** (simply called **rule** in this context) is an instruction to Enterprise Manager Cloud Control on how to automate actions when an event, incident, or problem occurs. Rules do not operate retroactively, so a rule only operates on events, incidents, or problems that occur after the rule is created. Several predefined rules are provided out-of-the-box.

A rule consists of the selection criteria (to identify the events, incidents, or problems for which they apply), the conditions (when the rule should be applied, for example, if an incident priority is changed to P1), and the actions. EM-supported actions include notifications, changing of the appropriate resolution management attributes, and ticket creation.

Examples

1. If the rule criteria is a specific metric alert (for example, CPU utilization or tablespace percent used crosses a certain threshold of either warning or critical severity), the intended action is to create an incident.
2. Another rule can operate on incidents that are of either warning or critical severity, and the action is to send a notification. In this case, there could be an additional condition that if the rule condition is severity=critical, the action is to notify by page, while if the rule condition is severity=warning, the action is to notify by email.
3. Another example of a rule could be for incidents that have been open for longer than seven days, where the rule action is to set the escalation level to one.

Defining Rules

Common tasks for which you can define rules include the following:

- Creating an incident in response to an event:
 - Intelligent Incident Compression allows multiple events to be automatically grouped into a single incident.
- Creating helpdesk tickets for incidents
- Sending events to third-party systems
- Sending notifications to different users
 - Notifying different administrators for different classes of events, problems, and incidents
- Managing workflow of incidents and problems



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Use rules on events:

- To create incidents for the events managed in Cloud Control
 - Starting with Cloud Control 13c, the Intelligent Incident Compression functionality allows multiple events to be automatically grouped into a single incident. This is built into the out-of-the-box rules and can be used during custom rules definition.
- To create helpdesk tickets for incidents managed by a helpdesk analyst
 - Create incidents based on an event, and then create a ticket for the incident.
- To send events to third-party management systems
- To send notifications on events
 - No incident is created

Use rules on incidents:

- To automate the management of the incident's workflow
 - Assign owner, set priority, escalation levels, and so on, and send notifications
- To create tickets based on incident conditions
 - For example, create a ticket if an incident is escalated to level two.

Use rules on problems:

- To automate the management of the problem's workflow (assign owner, set priority, escalation levels) and send notifications

Rule Sets

- Rules grouped together to operate on the same object
- Two types of rule sets:
 - Enterprise
 - For operational practices of the data center to manage events and incidents
 - EM-supported actions
 - Requires the CREATE_BUSINESS_RULESET resource privilege
 - Visible to all administrators
 - Collaborative: multiple co-authors
 - Private
 - Sending email to yourself
- Notifications on enterprise rules or rule sets:
 - Administrators can subscribe to notifications when rule sets are applied.
 - Rule owners can assign notification recipients.



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Rule sets are rules grouped together to operate on the same object (for example, a target group). There are two types of rule sets in Enterprise Manager: an **enterprise** rule set and a **private** rule set.

Use an **enterprise rule set** to implement your operational practices for events and incidents. All the previously mentioned actions are possible. Because these are actions that affect all types of incidents and problems, the administrator that creates these rule sets requires the CREATE_BUSINESS_RULESET resource privilege. After an enterprise type rule set is created, it is visible to all Cloud Control administrators. Further development of that rule set can be done in a collaborative manner by multiple co-authors (that is, multiple users who can edit a particular rule set).

A **private rule set**, on the other hand, is designed only to send email notifications to yourself for events, incidents, and problems of interest. As a result, no special privileges are required to create a private rule set.

As an administrator, you may be interested in knowing when a rule or a rule set is applied as a response to an event, incident, or problem. You can subscribe to **notifications** for any existing enterprise rules or rule sets. Alternatively, when rules or rule sets are defined, they can include information on where notifications can be sent.

Setup of Notifications

- Notification preferences setup
 - Incoming and outgoing (SMTP) email server
 - Customized email formats
 - Schedules
 - Notifications repeating cycle and maximum number
- Third-party tools notifications setup
 - Configured connectors, ticketing systems, or other advanced notifications
 - Examples: SNMP traps, custom notification methods via OS scripts or PL/SQL procedures
- Appropriate target privileges
 - `MANAGE_TARGET_ALERTS`: Full access to events
 - `OPERATOR_TARGET`: Includes `MANAGE_TARGET_ALERTS`



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Whether you have a subscription to an incident rule or rule set, or the rule creator made you the recipient of a notification, you must first perform the following tasks:

- Set up your administrator account notification preferences, which includes setup of:
 - An email incoming and outgoing (SMTP) server
 - Email addresses for notifications to be sent to
 - The schedule emails are to be sent on
 - Any customization to the email format
 - Repeat notification frequency; if repeat notifications are enabled and you would like to be notified repeatedly about the same events, incidents, or problems, up to a defined maximum number of times
- If you are using connectors, ticketing systems, or advanced notifications, configure them.
- Grant appropriate privileges to your Cloud Control administrator account to manage incidents from the managed target system, as discussed in the previous lesson.

For example, Cloud Control also supports third-party notifications via SNMP traps, including SNMP v3. Other custom notification methods can be set up via OS scripts or custom PL/SQL procedures.

You must have Super Administrator privileges to set up a notification method. Many of these setup tasks should be performed ideally by a Cloud Control Super Administrator as part of the installation and configuration.

Prioritization of Rules and Notifications

Under heavy load, processing priority is based on the:

- Lifecycle status of the target
 1. Mission Critical (highest priority)
 2. Production
 3. Stage
 4. Test
 5. Development (lowest priority)
- Type of event or incident
 - Availability events and incidents (highest priority)
 - All events and incidents of warning and critical severities
 - All informational events (lowest priority)



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

If Cloud Control experiences a very heavy load, it is important that the more important events and incidents are processed ahead of others. Two factors determine the processing priority.

- The first factor is the lifecycle status of the target, with the priority based on the order shown in the slide, where Mission Critical targets have the highest priority and Development targets have the lowest. As an EM administrator, one of your responsibilities is to set the lifecycle status of each target appropriately.
- The second factor is the type of event or incident. Any availability event or incident, such as target down, always has the highest priority. Next, any events or incidents that are of critical or warning severities are handled, and finally informational events are treated as the lowest priority.

This prioritization is taken into account only when the system is under heavy load. When the system is under normal load, events and incidents are handled as they arrive.

Best Practices for Using Incident Rule Sets

- Combine rules into a manageable unit:
 - Use groups as rule set targets.
 - Place all the rules for the members of that group in the same rule set.
 - Control the execution order.
- Incidents and problems:
 - Automate your routine operations.
- Oracle predefined rule sets:
 - Use for incident creation, event deletion
 - Cannot be edited
 - Can be disabled
 - Create custom copies of out-of-the-box rule sets.
 - Subscribe to this rule set.



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Summary of Using Rules and Rule Sets: Best Practices

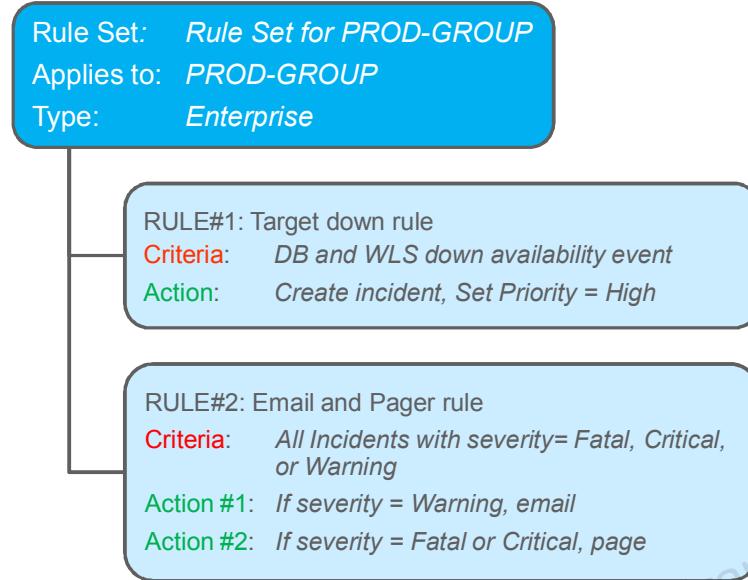
A rule set enables you to logically combine different rules that relate to the same object into a single manageable unit. A common set of objects can be targets, groups (also of heterogeneous types), or jobs.

Rule sets, as well as the rules within a rule set, are executed in a specific order: either by default in their creation order or as you specify it. Make sure you define the order correctly.

Use rule sets for automating responses on incidents and problems.

A variety of predefined rule sets are provided with Enterprise Manager Cloud Control. They automatically create incidents for what Oracle believes are meaningful events, as well as automate event deletion. You can use these out-of-the-box rule sets as is, but you cannot edit them. It is recommended that you create your own versions by using the Create Like functionality, and subscribe to this new rule set. The originals can then be disabled.

Rule Set: Example



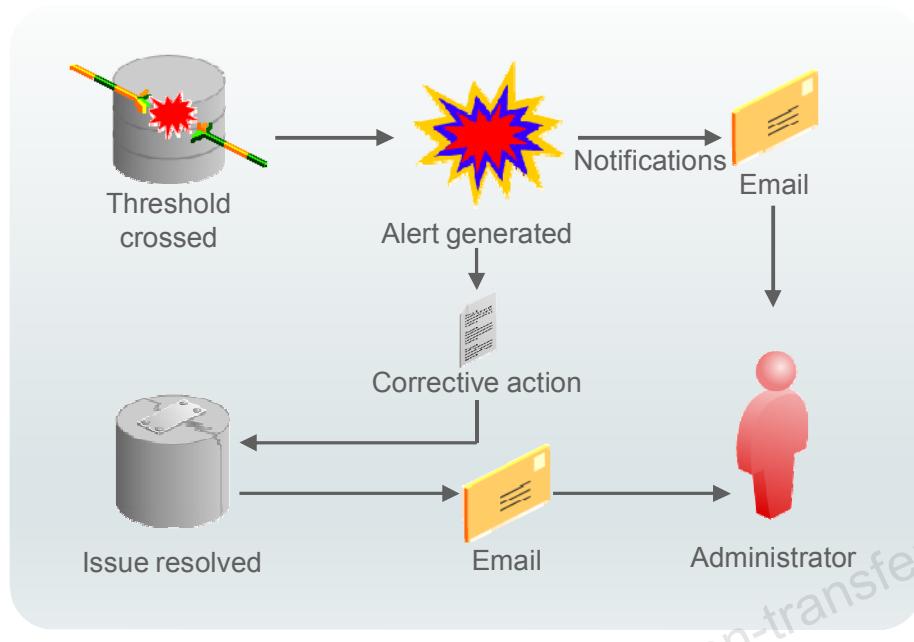
ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The graphic in the slide shows an enterprise rule set that applies to the PROD-GROUP group. This heterogeneous group consists of targets that include hosts, databases, and WebLogic servers. Two rules are included:

1. If any database or WebLogic servers are down, the action is to automatically create an incident and set its priority to high.
2. For any Fatal, Critical, or Warning incidents within the PROD-GROUP group, Cloud Control should send an email if the severity is set to Warning, and a page if the severity is set to either Fatal or Critical.

Corrective Actions



Corrective actions allow you to specify automated responses to alerts. They ensure that routine responses to alerts are automatically executed, thereby saving administrator time and ensuring that problems are dealt with before they noticeably impact users. For example, if Cloud Control detects that a component such as the listener is down, a corrective action can be specified to automatically start it back up. A corrective action is thus any task you specify that will be executed when a metric triggers a warning or critical alert severity. By default, the corrective action runs on the target on which the alert has been triggered. Administrators can also receive notifications for the success or failure of corrective actions.

A corrective action can also consist of multiple tasks, with each task running on a different target. For example, if an application server triggers a warning alert indicating that it is approaching its limit on the number of requests it can handle, a corrective action can be defined to automatically start up additional service instances on another host, thereby sharing application load among different service instances.

Corrective actions are implemented in Cloud Control using the Job System, described in an upcoming lesson.

Defining and Using Corrective Actions

- To add a corrective action to a metric on a specific target or in a monitoring template:
 - Create a new corrective action as part of the metric definition.
 - Reuse a corrective action already defined for a metric on the same target or in the monitoring template.
 - Apply one from the corrective actions library (at the enterprise level).
- Define a library corrective action for a corrective action that you plan to use repeatedly.
- Prerequisite privileges:
 - `MANAGE_TARGET_METRICS`
 - An `OPERATOR` subprivilege



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Corrective actions are stored in a **Corrective Actions Library**. Defining corrective actions at the enterprise level enables you to associate corrective actions with events, incidents, or other changes in your environment. You can add a corrective action as a response to various events on a specific target or you can add it in a monitoring template in any of the following ways:

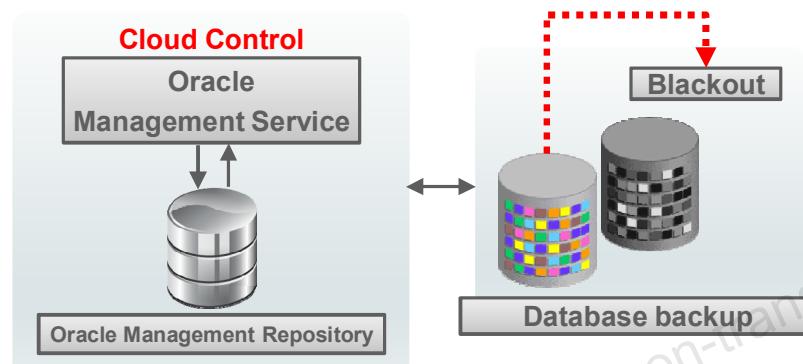
- Create a new corrective action as part of a metric definition or response to other alerts and status changes.
- Specify the name of a corrective action that has already been defined on another metric for that target. If you are adding the corrective action to a metric in a monitoring template, you can also reuse corrective actions that have been previously defined in the monitoring template.
- Specify the name of a corrective action that has been previously defined in the corrective actions library.

When you define a corrective action, you choose from a list of corrective action job types. The list of available job types will vary depending on the target type.

Corrective actions for a target can be defined by all Cloud Control administrators who have been granted the “`MANAGE_TARGET_METRICS`” (or greater) privilege on the target. The “`MANAGE_TARGET_METRICS`” privilege is an `OPERATOR` subprivilege.

Using Blackouts

- Designed to suspend collection of monitoring data during maintenance activities
 - More accurate target availability data
- Can be scheduled one-time or periodic
- Can also be set using EM CLI
- Require the `BLACKOUT_TARGET` privilege



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Blackouts allow you to suspend the collection of metrics on a target when performing scheduled maintenance on the target. Blacking out a target suspends monitoring on the target for the duration of the blackout.

A blackout can be defined for individual targets, a group of multiple targets that reside on different hosts, or for all targets on a host. Blackouts can be scheduled to run immediately or in the future, and to run indefinitely or stop after a specific duration. Blackouts can be created on an as-needed basis, or scheduled to run at regular intervals. During the maintenance period, if you discover that you need more (or less) time to complete a maintenance task, you can easily extend (or stop) the blackout that is currently in effect. The blackout functionality is available from both the Cloud Control console as well as via the command line interface (EM CLI). EM CLI is often useful for administrators who need to incorporate the blacking out of a target in their maintenance scripts.

Blackouts allow you to collect accurate monitoring data. For example, you can stop data collections during periods where a managed target is undergoing routine maintenance, such as a database backup (as shown in the slide) or hardware upgrade. If you continue monitoring during these periods, the collected data shows trends and other monitoring information that are not the result of normal day-to-day operations.

Blackouts occur simultaneously across all targets, regardless of the time zone. To black out a target, you need at least the `BLACKOUT_TARGET` privilege on the target, which is an `OPERATOR` subprivilege.

Using Notification Blackouts

- Designed to allow suspending *only* incidents and notifications for events:
 - During regular maintenance activities
 - When a known target is down
- Still allow visibility into the status and health of the targets
- Similar interface to the blackouts
 - Can be defined for targets or groups
 - Maintenance or nonmaintenance types
 - EM CLI option
- Require the `BLACKOUT_TARGET` privilege



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Notification Blackouts allow administrators to suspend incidents and notifications for events while targets are undergoing planned maintenance activities or simply when a target is down and administrators are already aware of the problem. Monitoring data is still collected and targets' status and health data is available to administrators. While targets are brought down for maintenance, the brownout time is excluded from target availability (%) calculations. At the end of the notification blackout, all events that occurred during the brownout are processed and notifications are sent.

Creating the notification blackout interface is very similar to the blackouts interface. The one exception is that you can specify if the target is:

- Under maintenance, in which case the target down time is excluded from Availability (%) calculations
- Nonmaintenance, in which case the target down time is taken into account during Availability (%) calculations

To place a target under a notification blackout, you need at least the `BLACKOUT_TARGET` privilege on the target, which is an `OPERATOR` subprivilege.

For more details on notification blackouts, be sure to watch the OLL demonstration titled “*Notification Blackout with Oracle Enterprise Manager*.”

Quiz



By enabling repeat notifications, you:

- a. Repeatedly send email notifications about the same metric event, incident, or problem
- b. Send email notifications based on the repeat frequency
- c. Send email notifications based on the maximum repeat notifications
- d. All of the above



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Quiz



A corrective action is:

- a. A user-defined job stored in a library
- b. A series of steps that performs a task
- c. An automatic response to an event, incident, or other status change
- d. All of the above



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Summary

In this lesson, you should have learned how to:

- Define incident rules
- Describe notifications and their options
- Define corrective actions in response to incidents and problems
- Distinguish between blackouts and notification blackouts



Practice 8-1 Overview: Creating a Corrective Action

This practice covers the following topics:

- Creating corrective actions for alerts or events
- Reviewing actions saved in the library



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Practice 8-2 Overview: Creating a Rule Set

This practice covers the following topics:

- Creating a rule set
- Adding rules to the rule set



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Practice 8-3 Overview: Observing How a Rule Set Is Applied

This practice covers the following topics:

- Causing an incident to occur
- Observing how a rule set is applied to resolve the incident



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Using the Job System

ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Objectives

After completing this lesson, you should be able to:

- Define and describe jobs and related terms
- Explain the difference between job steps, executions, and job runs
- Distinguish predefined jobs from customizable jobs
- Create and manage jobs of different types
 - Multitask jobs
- View job activity
- Use the job library



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

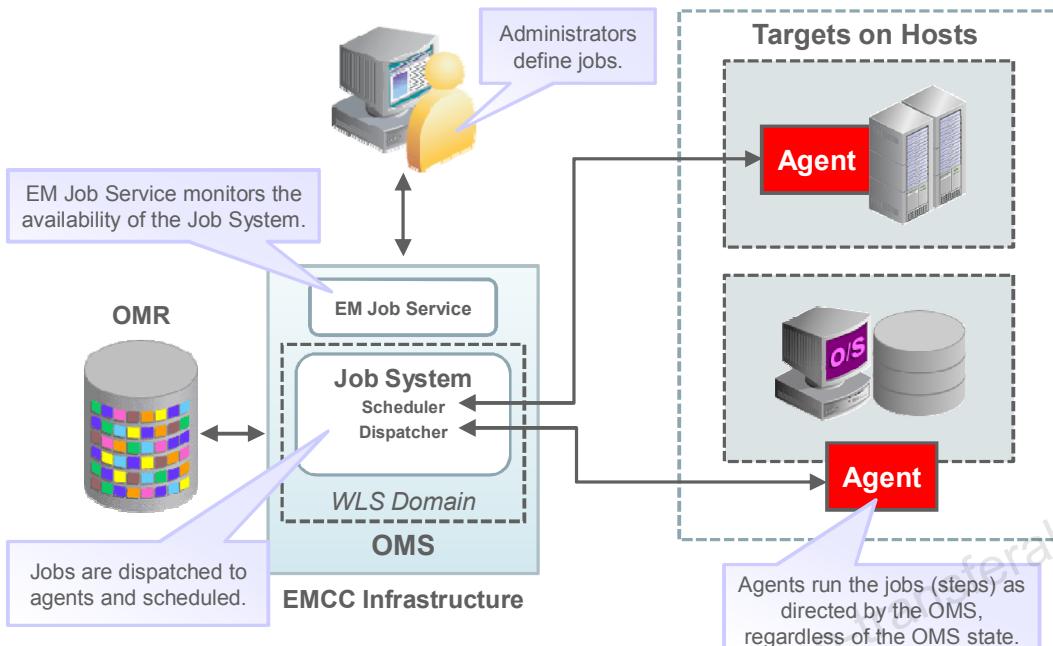
What Is a Job?

- Work that you define and schedule to automate commonly performed tasks
- Defined by parameters, schedules, targets, and so on
- Can have predefined elements
- Can execute immediately or at a specified date and time
- Can execute once or repeatedly
- Runs on multiple targets at the same time
 - Thousands of targets

ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

How Do Jobs Work in Cloud Control?



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The Cloud Control Job System has several subcomponents that handle various aspects of creating, scheduling, and running jobs.

The graphical interface allows administrators to create jobs by selecting the type of job and entering the required parameters and destinations (targets to run on).

The **scheduler** within the OMS determines the job steps and schedules them in the system. Note that the Cloud Control job scheduler is different from the scheduling functionality within the database. The database built-in scheduler is used by the management repository to run its database jobs when needed, but it is independent of the Cloud Control job system.

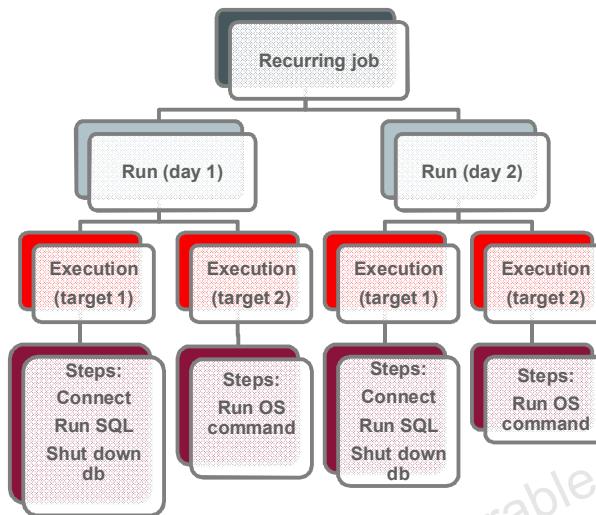
The **dispatcher** is a component of the job system that uses several preconfigured worker threads to dispatch a job step. Short command threads dispatch asynchronous steps and short synchronous steps, while long command threads dispatch steps that have long-running commands.

The agents on the targets actually run the steps on the remote targets as directed by the OMS. Once the job steps reach the agents, the agents handle the jobs independently of the OMS (even if the OMS is down). When jobs complete, job status is reported back to the OMS.

A predefined **EM Job Service**, a special kind of target in Cloud Control, monitors the availability of the Job System. Services will be discussed in an upcoming lesson.

Job Elements

- Job **steps**:
 - Executable units of work
 - Ordered commands
- Job **executions**:
 - Steps per target
- Job **runs**:
 - “Parents” of job executions
 - Multiple runs for repeating jobs



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

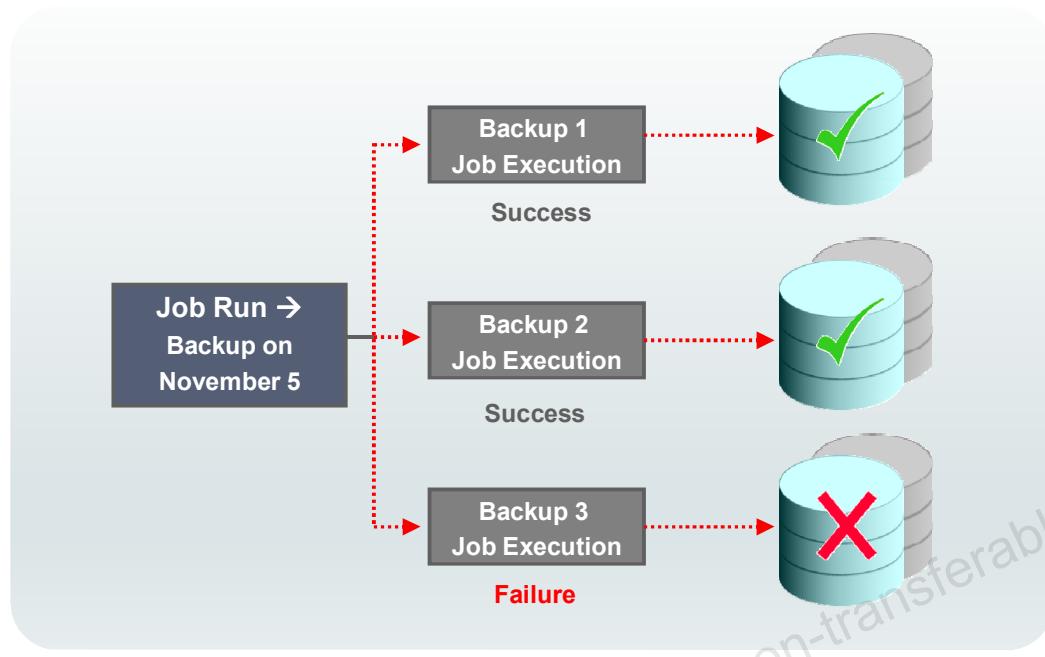
A job **step** is an executable unit of work. Agents perform job steps on the managed targets.

Most jobs typically execute their job logic in parallel with multiple targets. For such jobs, each job run consists of multiple job **executions**, one job execution per target.

A job **run** is an instance of a specific job on its scheduled start date. Recurring jobs will have one job run per scheduled occurrence.

The graphic in the slide shows the hierarchy of the job steps, executions, and runs. This is an example of a recurring job that runs on two targets and executes identical steps on each target.

Job Executions and Job Runs



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Job **executions** are usually associated with one target (for example, a backup job on a particular database). When a job is run against multiple targets, each execution may execute on one target. Job executions are not always a one-to-one mapping to a target. Some executions have multiple targets (for example, comparing the software configuration on multiple hosts). Other executions have no targets (for example, a predefined job that updates the information on available patches for all your products, called the Refresh From My Oracle Support job).

When you submit a job to many targets, it is tedious to examine the status of each execution of the job against each target (for example, you run a backup job against hundreds of databases). In this scenario, you may ask questions such as: Were all the backups successful? If not, which backups failed? If this backup job runs every week, you would want to know each week which backups were successful and which ones failed. With the Job System, you can easily get these answers by viewing the job **run**. A job run is the sum of all job executions of a job that ran on a particular scheduled date. Using the backup example, if you have a backup job against one hundred databases on November 5, you will have one November 5 job run. The job runs once on one hundred databases. This results in one hundred executions of the job. The job table that shows the job run will provide a rollup of the statuses of these executions.

Defining Jobs

There are two categories of jobs within Cloud Control:

- Predefined jobs for:
 - Database (such as backup, export, and import)
 - Middleware (such as start, stop, or restart components)
 - Deployment (such as patching and cloning)
- Customizable jobs that can:
 - Use custom OS or SQL scripts
 - Reference target properties, such as:
 - %TargetName%
 - %OracleHome%
 - %SID%



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Cloud Control provides predefined job tasks for known targets such as database or middleware targets, or deployment type of jobs that handle software bits (installations or patches). A job task contains predefined, unchangeable logic (for example, patch an agent, back up a database, and so on). Examples of predefined database jobs include backup, export, and import. The predefined jobs associated with deployments include patching, cloning Oracle homes, and cloning databases.

In addition to predefined jobs, you can define other jobs that are more customizable for your environment. For example, these jobs could involve writing code to be run by your targets' operating systems (OS) or against a database target (SQL scripts). These scripts can reference variables that are known to Cloud Control, such as Target Names, Oracle Name, or Database SID. These variables are encapsulated by the “%” sign and Cloud Control provides full descriptions of their exact names so that they can be interpreted correctly at run time.

Using Predefined Jobs

- Large number of predefined jobs provided
- Available for specific targets
- Examples of database instance jobs:
 - Shutdown Database
 - RMAN Script
 - Startup Database
- Collection of jobs: Deployment Procedures
 - Used for provisioning and patching
 - Collections of predefined jobs and additional logic
 - Examples of Deployment Procedures:
 - Clone and Patch Oracle Database
 - Upgrade Database



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Cloud Control provides various predefined jobs that are available from the Job Library or from target-specific pages such as a Database Instance home page.

Many jobs are target-specific so you must define the targets they will run on. Some jobs are targetless jobs, which means that they apply to the enterprise and do not have any specific targets, such as the Refresh From My Oracle Support or Opatch Update jobs (which you will use as part of patching activities in the lesson titled “Patching and Provisioning”).

You can use the Create Like functionality as a starting point for your own jobs.

Deployment Procedures are best practices provided by Oracle for various Provisioning and Patching tasks (provisioning databases, middleware components, applications, and so on). These include a series of jobs as well. Procedures supplied by Oracle cannot be edited, but can be extended using the “Create Like” functionality. This enables you to customize them to fit your environment.

Note: Deployment Procedures will be discussed in an upcoming lesson.

Job System Chef-Solo Support



- Chef Recipe: New Job System interface
 - New job type
- Chef uses recipes and cookbooks:
 - Stored in the Software Library
- Cloud Control supports the stand-alone version of Chef-Solo:
 - Recipes and cookbooks can be stored on the hosts.
 - Cloud Control can execute Chef recipes that exist on managed hosts.
- Add and delete cookbooks using EM CLI.
- Deployment Procedures can include Chef recipes.

ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Job Interfaces in Cloud Control

- Job Activity page:
 - Displays 24-hour history by default
 - Highlights Problems, Runs, Jobs Scheduled, and My Jobs
 - Customizable information tiles
 - Used to:
 - Manage search for jobs
 - Ability to save searches and add them to the top information tiles
 - Create ad hoc jobs
 - View, edit, create like, suspend, resume, stop, or delete job runs or executions
 - Save jobs for reuse
- Job Library page:
 - Provides access to stored job definitions
 - Used to view, create (like), and modify library jobs



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

There are two pages within Cloud Control that provide interfaces to jobs:

- **Job Activity page:** This is the hub of the Job System within Cloud Control. The top of this page highlights, by default, Jobs with Problems, Job Runs, Jobs Scheduled, and My Jobs, all for the last 24-hour period. These information tiles are customizable. From this page, you can create new custom jobs as well as manage existing jobs. For creating new jobs, there is a drop-down list from which you can choose the type of job (for example, OS Command or SQL Script) and continue with the rest of the job definition. A rich search mechanism enables you to easily find the jobs that fit various criteria, for example, search by name, owner, status, scheduled start, job type, target type, and target name. These searches can also be saved at the top as one of the information tiles.
- **Job Library page:** The Job Library stores the basic definition of jobs that can be customized to run against specific targets, or that can be stored with the specific target information. If a particular job is going to be used over and over again, you may want to save that job in the Job Library. This enables you to reference this job whenever required, as well as grant other administrators access to it.

For all jobs, you can specify email notifications depending on the job status. A job owner may choose to receive email notifications based on the job severity status. Emails will then be sent based on the Owner's notification schedule. In addition, more advanced options can be enabled, such as generating events for job status or creating corrective actions.

Creating Jobs

- Job selection by Job Type
- Job attributes
 - Name
 - Parameters
 - Credentials, if required
 - Schedule
 - One time, repeating
 - Access
 - Grant access to this job to other administrators
- Privileges
 - Typically, regular administrator privileges are required to *create* a job.
 - Must have appropriate target privileges to *run* the job.

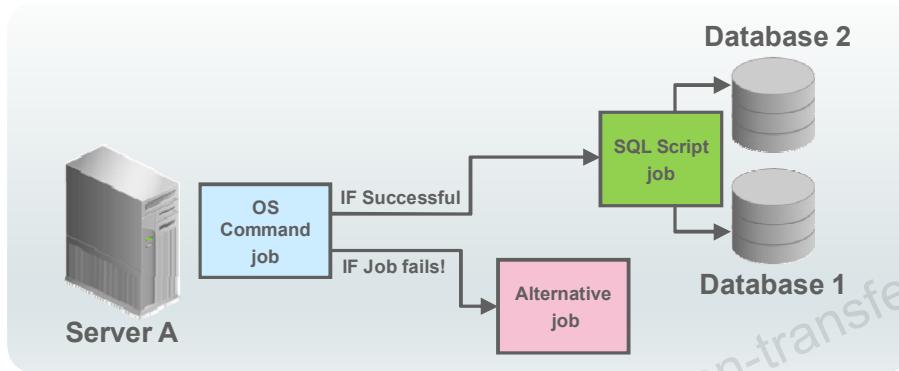
ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Creating a Multitask Job

Multitask jobs:

- Are complex jobs consisting of one or more distinct tasks
- Can run against targets of the same type or different types
- Allow you to specify dependencies between the different tasks



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

A multitask job is a complex job made up of one or more distinct tasks. It can run against targets of the same or different types.

You can create a multi-task job consisting of two tasks, each a different job type and each operating on two separate (and different) target types.

Example:

- Task 1 (OS Command job type) performs an operation on Server A.
 - If Task 1 is successful, run Task 2 (SQL Script job type) against both Database 1 and Database 2.
 - If Task 1 fails, you can set it to run an alternative job, indicating that the first task failed.

This multitask functionality makes it easy to create extremely complex operations.

You create a multitask job by selecting the job type **Multi-Task** from the list of available jobs.

Details of a Multitask Job

- Define the job name.
- Specify where all tasks run:
 - On same targets
 - Different targets
- Enter the tasks to be run in sequence:
 - At least two tasks
- Set the **Condition** and **Depends On** options.
- Create the initialization error handler task.
- Define the schedule:
 - One-time, repeating
- Specify access:
 - Grant access to this job to other administrators.



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

A multitask job requires general parameters just like other job types, such as Name. Next, for this job type, you define whether the task will run on the same target or different targets. On the Tasks page, enter the tasks accordingly. The tasks entered are run in sequence. If you choose to have your job run against different targets for different tasks, you have to enter the target information for the tasks also. If you choose the option to run the job against the same targets for all tasks, it uses the target information entered on the General page.

If you have at least two tasks entered, you can set the **Condition** and **Depends On** options. Task conditions define states in which the task will be executed. These condition options include:

- **Always:** Task is executed each time the job is run.
- **On Success:** Task execution **Depends On** the successful execution of another task.
- **On Failure:** Task execution **Depends On** the execution failure of another task.

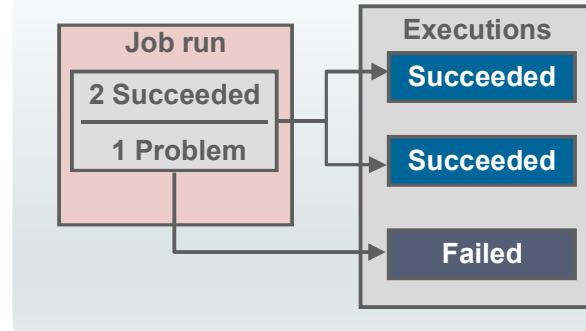
You can also create an initialization error handler task. This task executes if any task of the multi-task job (except Always tasks) causes an initialization error. The initialization error handler task does not affect the job execution status.

The remaining information, such as schedule and access information, is similar to that of simple jobs.

Reviewing Job Execution Results

Job status values:

- Scheduled
- Running
- Suspended
- Succeeded
- Problems



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

When a job is submitted and run, you receive a status for each execution. If a job runs against more than one target, each target receives a status for its execution. The job status values are as follows:

- **Scheduled:** The job has been scheduled to run at a later date.
- **Running:** The job is defined to be in this state if at least one of its steps is currently running.
- **Suspended:** The job is in this state for the following reasons:
 - It has been manually suspended by the user.
 - It has been scheduled during a blackout window defined on any one of its targets with the “Run jobs” option set to Disabled (when creating a blackout, users can choose to run jobs or not). Jobs in this state go to “Scheduled” after the blackout period ends and eventually execute.
 - A resource is unavailable. For example, the job is blocked from running because it is waiting on a lock held by another process. It automatically resumes after the lock becomes available.
 - The management agent is down or unreachable due to network problems between the Oracle Management Service (OMS) and the management agent.
 - It is waiting for the completion of an external event. For example, this status currently applies to patch jobs. For the patch job, the execution is suspended until the agent restarts, performs some required post-patch tasks, and sends a notification to the management service to indicate that it has completed these tasks. At this point, the management service resumes the execution of the job.
- **Succeeded:** The job has completed successfully.

- **Problems:** The job could be in this state for the following reasons:
 - **Error:** The job or step could not be run for some reason (for example, the execution of a remote command failed because incorrect credentials were specified or the job includes an invalid path to a script). If a step in a job fails initialization, the job status is Error.
 - **Failed:** It executed, but did not accomplish its task. For example, the wrong password for the database user was entered so the database backup could not complete.
 - **Stopped:** The job was canceled.
 - **Inactive:** The job target or the job owner was deleted. If the job owner is deleted, that job is in an inactive state. Jobs are deleted in the background after their administrators are deleted.
 - **Reassigned:** The owner of the job had been removed. Ownership of the job has been assigned to a new administrator.
 - **Skipped:** The job could not be executed at the specified time. This could be because a grace period has expired, execution from a current or previous job run has not finished, the user chose to skip the job execution, or OMS problems prevented the job from running.
 - **Credentials Missing:** The job or step could not be run because the credentials were missing.

Performing Job Operations

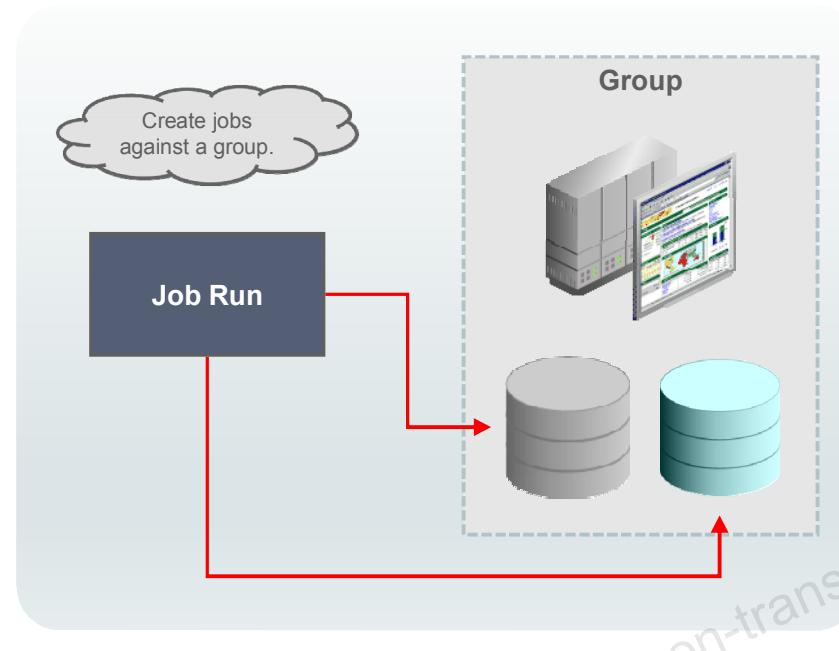
- Suspending a job: Halts execution until you explicitly resume it
- Resuming a job: Restarts the execution of a job with the next step (after fixing problems at a previous step)
- Stopping a job: Stops the execution altogether
- Deleting a job depends on:
 - Job status at that time
 - Running or Suspended
 - Completed
 - Scheduled
 - Type of job
 - Recurring
 - One-time



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

- Deleting a job has the following effects:
 - For running and suspended jobs, deleting a job stops the job and removes it from the system, including the job history and logs for the execution. Currently running steps may complete execution before the job stops.
 - For completed jobs, deleting a job removes all job information for that execution, but does not affect other executions.
 - For scheduled jobs, deleting a job cancels all executions scheduled for the future, but does not delete executions that have already run.
 - For repeating jobs, deleting a running or scheduled execution cancels all future executions of the job. Deleting a completed execution removes only that execution. Users may choose a job and select the option to delete all runs to remove all executions of that job.

Jobs and Groups



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Job Events

- Job **status changes** are treated as **events**.
- Can create incidents based on these events
 - Managed as any other incident
- Can create rules/rule sets for these incidents
- Out-of-the-box events generated for job status:
 - Action Required
 - Problems
- Privileges
 - Super Administrator: Determines the job status that generates events
 - Administrators with target access: Specifies targets that should generate events



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

In Cloud Control, job status changes are treated as events. This implies the following:

- Administrators can create incidents based on these events.
- They can be managed as any other incident:
 - Including creating rules/rule sets for these incidents

Out-of-the-box behavior:

- Events are automatically generated for job status:
 - Action Required
 - Problems

Super Administrators can change the job status that generates events for your system. All other administrators with target access can add those targets to the list of targets that generate events based on the job status defined by the Super Administrators.

Jobs Privileges

Operation	View access	Full access	Owner	Super Administrator
View submitted job	✓	✓	✓	✓
Edit description, schedule, targets, credentials, and parameters	X	✓	✓	✓
Edit access	X	X	✓	✓
Grant job view access	X	X	✓	✓
Create Like	✓ *	✓ *	✓	✓ *
Copy to Library	✓	✓	✓	✓
Retry/Suspend/Resume/Stop	X	✓	✓	✓ *
Delete job	X	✓	✓	✓
Enable events for job status	X	X	X	✓

ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Enterprise Level: Monitoring Jobs and Job System Status

- Jobs summary status
 - Enterprise Summary page
- Job-related incidents
 - Enterprise Summary page
 - Incident Manager
- Job System status
 - Tracked on the Management Services and Repository page
 - Step scheduler status
 - Jobs backlog
 - Broken System jobs
 - All Metrics
 - Predefined job metrics
 - Examples: Job step backlog, overall job steps per second



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Jobs can be monitored from a few locations in Cloud Control:

- Enterprise Summary page: For a rolled-up status of all the jobs running in your enterprise as well as job-related incidents
- Incident Manager: Specifically for incidents related to jobs, if any were set up

The Job System itself is a self-managing entity. Depending on how you use the job system, you may want to periodically analyze how the jobs run and tune up the Job System for your needs. The Job System internal monitoring is tracked on the Management Services and Repository pages of Cloud Control and includes statistics such as Step scheduler status, Jobs backlog, Broken System jobs, or metrics that are specific to jobs and available under All Metrics. Job System parameters and metric thresholds can be adjusted based on these findings but this is only recommended for advanced users.

Quiz



To save and reuse jobs for the future, use:

- a. Job Library
- b. Job Activity
- c. Corrective Action Library



Answer: a, c

Quiz



Predefined, target-specific job logic can be modified.

- a. True
- b. False



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Summary

In this lesson, you should have learned how to:

- Describe and define jobs and related terms
- Explain the difference between job steps, executions, and job runs
- Distinguish predefined jobs from customizable jobs
- Create and manage jobs of different types
- View job activity
- Use the job library
- Enable job notifications



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Practice 9-1 Overview: Creating and Executing a Simple SQL Job

This practice covers the following topics:

- Creating a SQL job that runs immediately
 - Setting appropriate credentials
 - Saving the job to the library for future use



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

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

This practice covers the following topics:

- Creating an OS job that runs immediately
 - Setting appropriate credentials
 - Selecting multiple targets
 - Saving the job as a repeating job
 - Saving the job to the library for future use



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Practice 9-3 Overview: Creating a Multitask Job (Optional)

This practice covers the following topics:

- Creating a job that includes multiple tasks against different types of targets
- Creating job dependencies
- Running the job



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Unauthorized reproduction or distribution prohibited. Copyright© 2019, Oracle and/or its affiliates.

GANG LIU (gangl@baylorhealth.edu) has a non-transferable license
to use this Student Guide.

Managing Systems and Services

ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Objectives

After completing this lesson, you should be able to:

- Describe systems and services
- Create a service based on a system
- Define and monitor the availability of a service
- Discuss the use of beacons
- Define and monitor service levels
- Explain Root Cause Analysis



Systems and Services

Why would you use Systems and Services?

- **Systems**

- Collection of assets available: Targets
 - Out-of-the-box systems are provided for Oracle-packaged applications and database targets.
 - Simplify management and monitoring tasks.
 - Manage targets as one unit.

- **Services**

- Business representation of systems.
- Measure performance and availability as one unit.
- Report on service-level agreements.



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Systems are *logical* groupings of entities, which are assets represented in Cloud Control as targets (for example, database instances, WebLogic Servers, and so on), that provide a special function or form a particular application. Out-of-the-box systems are provided for Oracle applications such as Siebel, PeopleSoft, and E-Business Suite. In addition, systems are provided for database targets that include the database, listener, host, and Automatic Storage Management components for that database so that you can manage the components collectively.

Similar to groups, the benefits of using systems include simplified management and monitoring because all targets are managed as a single unit.

Services, on the other hand, are the *business* representation of various targets, grouped as systems, which have the ability to measure performance and service availability levels as a single unit, as well as being able to create customized reports based on service-level agreements.

Example: System and Service

- **System:** Cloud Control target comprising a logical set of targets
- Email system targets:
 - The database
 - Listener
 - Application server
 - Host targets on which the email application runs



Email system

- **Service:** Cloud Control target based on a system, models an application
- Email service:
 - Based on the Email System
 - Monitors availability and performance of the email application



Email service

ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Creating a Generic System

- Define system attributes and properties.
- Select the privilege propagating options:
 - Enabled
 - Disabled
- Select the targets that are part of the system.
- Define associations.
 - Connections or interactions
- Specify the availability criteria:
 - Based on key members
- Specify the charts to be displayed:
 - Based on metrics collected for targets
 - Oracle-suggested or custom



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Cloud Control includes wizards for various system types. To create a generic system, select **Systems** from the **Targets** menu, and then select **Add**. To define a new generic system:

- **General:** Use this page to specify a name and additional system properties for a new system, and to add target members for a new system or remove target members for an existing system. If you choose to include dependent targets, then these will automatically be included in your system even if the actual list of dependent targets may change. You also select the time zone that is used for scheduling operations on the system.
You can enable Privilege Propagation for a generic system, which means the target privileges granted on the generic system to the administrator will be propagated to the member targets. This automatically implies that only those targets on which you have "Full Target" privileges can be members of a Privilege Propagating generic system.
- **Define Associations:** Lists associations between members detected automatically. You can also define additional associations on this page. If you know of relevant relationships between the targets in the system, you can enter, for example, the "Stores on database" association between an application deployment target and a database system target.
- **Availability Criteria:** On this page, specify which targets (or key members) need to be up for the system to be considered up. You can choose from "Any of the Key Members" and "All of the Key Members."
- **Charts:** This page allows you to determine which charts should be displayed on the System Charts page. You can include any or all Oracle-suggested charts and add other charts for selected metrics.

Using the System Home Page

- View
 - Summary status of the targets within the system
 - Overview of issues (incidents and problems)
 - Compliance information
 - Job information for jobs within the last seven days
 - Blackouts
 - Configuration and relationship changes within the last seven days
 - Dependent targets
 - Services, if defined
- Manage
 - Set new target properties.
 - Grant access to the system.
 - Add the system to a group.
 - Create/end blackouts or brownouts.
 - Operations: Compare monitoring settings.

ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Other System Views

- Topology
 - Targets of the systems and the associations between them
 - Status of the targets in your system and the overall status of the system
 - Drill down to detail pages for targets to get information about their incidents
 - Icons indicate:
 - Status of the system members
 - Type of incidents for the system member
- Dashboard
 - Incidents, problems, compliance violations

ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The System Topology page provides a graphical representation of the components of your systems as modeled in Cloud Control. This page shows all targets, represented as icons, as well as the associations between them, represented as links between targets.

The status indicators enable you to quickly assess which targets are down or have open incidents. The screenshot shows a black icon for a fatal incident. By clicking any of the targets, you can see additional information about the status of the member.

The Topology page is used to identify the dependencies between services and the systems on which they run. From the View drop-down list, you can select services to review which of them depend on this system. The page shows the relationship between the service and its dependencies on service tests, key components, and so on. It also displays an overall view of the status of all the dependent subservices and key components as already discussed for systems. You can also use this page to perform Root Cause Analysis (discussed later in this lesson).

The Dashboard color-coded interface view helps monitor the status, incidents, and compliance violations of the system by highlighting problem areas.

Defining Services

- **Service:** In an enterprise, an entity that provides a useful function to its users.
- Define one or more *service models* that represent the business functions or applications that run in your enterprise to assess availability and performance of the services.



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

In an enterprise, a **service** is an entity that provides a useful function to the end users. Some other examples of services include customer relationship management (CRM) applications or online banking. As an administrator, you need to monitor and manage the availability of these services. However, service failures and performance degradation are a few of the problems that you may have in an enterprise. Because these services form an important type of business delivery, monitoring these services and quickly correcting problems before they can impact business operations are crucial in any enterprise.

Service level agreements are used to evaluate service availability, performance, and usage. By constantly monitoring the service levels, you can identify problems and their potential impact, diagnose root causes of service failure, and fix these in compliance with the service level agreements. Cloud Control monitors not only individual components in the IT infrastructure, but also the applications hosted by those components, allowing you to model and monitor business functions using a top-down approach, or from an end-user perspective. In Cloud Control, you can create a new target, a service, to model and monitor your business applications from within Cloud Control. When creating a service, you can define the availability, performance, and usage parameters, and service level rules.

Understanding Service Types

Select from the following types when defining a service:

Service Type	Description
Aggregate	Consists of two or more services called subservices
Generic	Used to model and monitor any business process and/or application. A generic service can be: <ul style="list-style-type: none">• Test-based• System-based



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Defining the Availability of a Generic Service

Availability of a generic service can be determined by:

Service Availability	Description
Service Tests	Availability of the service is defined in terms of availability of the service test(s) or successful execution of the test(s). A service is considered available if the key tests can be executed successfully.
System	Availability of the service is based on the underlying system that hosts the service.



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Defining a Service Test

- Service availability can be based on a single test that you specify when you create the service.
- Additional tests can be defined for the service.
- Tests are used to:
 - Monitor the service remotely.
 - Determine the availability and performance of the service.
- **Beacons** are used to execute the service tests from different geographical locations.

ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Using Beacons

- A *beacon* is used to execute service tests.
- Beacons are typically defined in geographical locations representative of your key user communities.
- Run service tests from your beacon locations.



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Defining a Web Transaction Service Test

- Web application availability can be defined in terms of the availability of the web transactions that are being monitored.
- Web transactions represent the service tests.
- Create a web transaction service test in one of the following ways:
 - Use the Transaction Recorder to automatically record user actions and navigation paths.
 - Define the steps manually.



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Defining Service Performance

Service performance can be based on the following:

- *Response metrics* collected by beacons executing the service tests
 - Response metrics help you determine how well the service test is performing for each of the remote beacons.
 - Critical and warning thresholds can be set.
 - Maximum, minimum, and average response data across two or more key beacons can be calculated.
- *Performance metrics* of the underlying system components hosting the service
 - Maximum, minimum, and average value across all components



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Performance of the service refers to the response time experienced by end users. You can define service performance based on the following:

- **Response metrics:** These are collected by the beacons that execute the service tests. You can set critical and warning thresholds for the metrics. The maximum, minimum, and average response time across two or more key beacons can be calculated. By reviewing this information, you can determine whether there are beacon locations with slow performance when compared with others.
- **Performance metrics:** These are the metrics of the system components that host the service. The maximum, minimum, and average values across all components can be calculated.

Defining and Monitoring Usage Metrics

- *Usage metrics* are used to measure the user demand or workload for the service.
- They are collected based on the usage of the underlying system components on which the service is hosted.
- The monitor usage metrics are as follows:
 - Monitor the usage of a specific component.
 - Statistically calculate the average, minimum, and maximum value from a set of components.



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Viewing Additional Service Information

Service Page Tabs	Description
Charts	Displays performance and usage graphs
Test Performance	Shows performance data for service tests
System	Displays component summary and provides for editing of the component list
Monitoring Configuration	Used to configure the service: availability, performance, usage metrics, and root cause analysis. Used to add/edit service tests
Topology	Identifies dependencies between the service and the system on which it runs Shows the relationship between the service and its dependencies on service tests, key components, and so on Displays an overall view of the status of all the dependent subservices and key components



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Defining Service Level Rules

- Service level is:
 - A measure of the quality of the service
 - Calculated as a percentage of time the service meets the specified availability and performance criteria during business hours
- Service level rules enable you to:
 - Define an assessment criteria to determine the quality of the service.
 - Specify the availability and performance criteria that the service should meet during business hours.
- Privileges required to define or update service level rules:
 - Owner of the service
 - Super administrator or Cloud Control administrator with the OPERATOR target privilege



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Services are used to model business functions or applications within your enterprise and provide an accurate measure of the availability, performance, and usage of the function or application they are modeling.

For each service, you can define a service level rule. A service level rule defines the assessment criteria used to measure service quality. It enables you to specify availability and performance criteria that your service must meet during business hours, as defined in your service level agreement. For example, an email service must be 99.99% available between 8 AM and 8 PM, Monday through Friday.

You can define only one service level rule for each service. This service level rule will be used to evaluate the actual service level over a time period and compare the actual service level against the expected service level.

You can view service level information directly from the Cloud Control console or as a generated report. From any service home page, you can click the Actual Service Level link to drill down to the Service Level Details page. This page displays what actual service level is achieved by the service over the last 24 hours, 7 days, or 31 days, compared to the expected service level.

Any super administrator, owner of the service, or Cloud Control administrator with the OPERATOR target privilege can define or update the service level rule.

Specifying Service Level Rule Elements

A service level rule is based on the following:

- **Expected service level percentage:** Percentage of time during business hours that you expect your service to meet the specified availability and performance criteria. The default is 85%.
- **Actual service:** Availability and performance criteria that an expected service level percentage is based on:
 - **Business days, hours:** Applicable days and times
 - **Availability criteria:** Availability states for which the service will be considered to be up
 - **Performance criteria:** Performance metrics that will be evaluated when computing the service level



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

A default service level rule is automatically applied when you create a service. The default expected service level is 85%. You can edit the service level rule to specify the assessment criteria that is suitable for your service. You can have only one service level rule for each service.

A service level rule is based on the following elements:

- **Expected service level:** Minimum acceptable service level that the service must meet over any applicable assessment period
- **Business days, hours:** Period during which the service level is calculated
- **Availability criteria:** When the service should be considered available. You can choose from the following states for a service:
 - **Up:** The service is considered up and available. You cannot change this state.
 - **Under Blackout:** You can specify the service blackout time also as available service time.
 - **Unknown:** You can choose this to specify the time a service is not monitored if an agent is down, as available service time.
- **Performance criteria:** Defined performance metric criteria that determine service availability. For any performance criteria used here, if the critical threshold has been met, it is considered a service level violation.

Using Root Cause Analysis (RCA)

- Benefits of Root Cause Analysis:
 - Provides the capability to analyze service failures
 - Returns a list of possible causes when a service fails
 - Evaluates the availability status of subservices and key components to determine the root cause of a service failure
 - Enables administrators to quickly identify problem areas
 - Enables administrators to assess the impact of service failures
- Configured from the Service Administration page
 - Runs in automatic mode by default
- View results by using the service topology viewer or from the Incident Manager.



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The Root Cause Analysis (RCA) feature provides you with the ability to analyze service failures, filtering the availability, performance, and configuration data of the system components used by the affected service.

RCA provides administrators with a focused assessment of service problems and allows them to quickly identify the cause and corrective action for the problem. You can use RCA to identify problems in complex aggregate services, including component failure.

By default, RCA is configured to run automatically whenever a service fails.

RCA processing is triggered by the occurrence of a service failure event. RCA monitors the status of a service and any defined component tests. The component test tests an aspect of a key component on which the service depends. Add a component test by choosing a metric and setting a threshold on a metric key. When RCA runs, it evaluates the status of the key component and component tests, and reports violations as possible root causes. RCA also provides the ability to include the details associated with the analysis with notifications sent for service failure alerts.

You can view the RCA feature by using the service topology viewer that enables you to see a graphical representation of the service and its relationship to other services, systems, and infrastructure components, with the causes identified by RCA highlighted in the display. The Incident Manager also provides access to the RCA topology.

Creating a Generic Service: Sample Wizard

Defining a generic test-based service

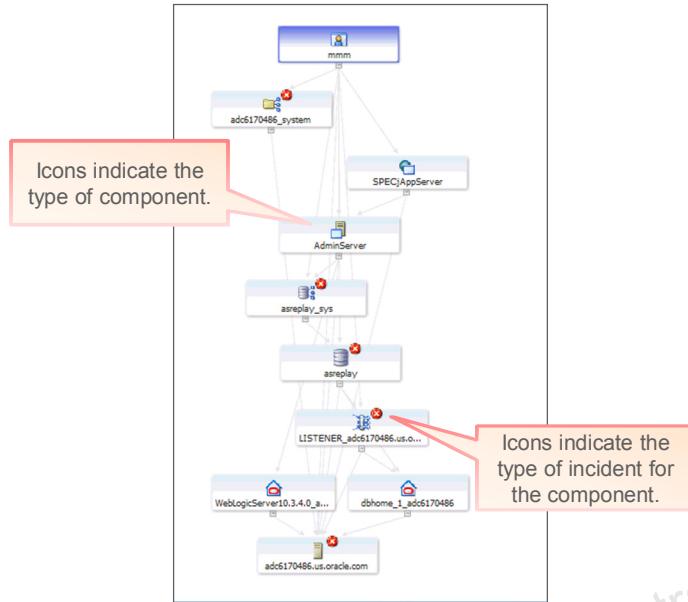
Additional pages enable you to specify a particular service test, beacons for the service test, and metrics that provide performance and usage information.

Define a service test and its key components.

ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Viewing the Service Topology



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Example: Implementing Systems and Services

1. Install the Oracle agents on the hosts where the components of your service reside.
2. Discover all the components for your service so they can be listed as Cloud Control targets.
3. Define a *system* these targets will be part of.
4. Create a *service* based on this system.
5. Specify the *availability* for the service, based on a service test or the availability of its system.
6. For service tests, create one or more *beacons* to monitor these service tests.
7. When the service is not available, identify the root cause of failure directly from Incident Manager.
8. Specify service level rules and track service levels by using Service Level Reports.



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Quiz



You can define service availability based on service tests or system components.

- a. True
- b. False



Answer: a

Quiz



Root Cause Analysis evaluates:

- a. The ability to log in as a root user on a Linux system
- b. The availability status of subservices and key components to determine the root cause of a service failure
- c. The likelihood of a corrective action being run
- d. Failed jobs



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Summary

In this lesson, you should have learned how to:

- Define systems and services
- Create a service based on a system
- Define and monitor the availability of a service
- Discuss the use of beacons
- Define and monitor service levels
- Explain Root Cause Analysis



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Practice 10-1 Overview: Reviewing Existing Systems and Services

This practice covers the following topics:

- Reviewing the definition of Systems and Services
- Exploring the Management Services and Repository System
- Exploring the EM Console Service



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Practice 10-2 Overview: Creating a System

This practice covers the following topics:

- Creating a generic system
- Evaluating the system's availability



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Practice 10-3 Overview: Creating a Generic Service

This practice covers the following topics:

- Creating a system-based generic service
- Reviewing the new service home page



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Practice 10-4 Overview: Monitoring the Availability of a Web Application

This practice covers the following topics:

- Adding a test-based service
- Creating a new key beacon to monitor your service



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Practice 10-5 Overview: Creating and Testing a Web Transaction

This practice covers the following topics:

- Creating a web transaction
- Testing your web transaction



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Patching and Provisioning

ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Objectives

After completing this lesson, you should be able to:

- Define software lifecycle management
- Describe the different roles and responsibilities
- Define provisioning, patching, and the Software Library
- Review configuration of the Software Library
- Use deployment procedures for provisioning and patching automation
- Patch software
- Define bare metal provisioning



Software Lifecycle Management

- Software provisioning
- Software patch management
- Software upgrades
- MyOracle Support integration



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

As the enterprise grows, as an administrator, you are constantly required to acquire new software and hardware. At the same time, you need to decommission the old or unused hardware and software. You are also required to upgrade the existing software and apply patches as required.

The provisioning and patching features of Cloud Control automate the deployment of software, applications, and patches. They make critical data center operations easy, efficient, and scalable, resulting in lower operational risk and cost of ownership.

- Software provisioning allows you to deploy database and middleware software enterprise-wide.
- Software patch management allows you to perform the complete end-to-end patch process.
- Software upgrades can be automated (configured, tested, and deployed) en masse.
- MyOracle Support (MOS) integration allows for automatic updates and facilitates context-sensitive access to information. (MOS also provides integrated incident management.)

The modular nature of Cloud Control facilitates performing lifecycle management tasks, because you can, for example, update a plug-in without updating the entire EM infrastructure.

Software Lifecycle Management Requirements

- Configured Software Library
 - Recommended at installation time
- Defined software lifecycle roles
 - Site administrator: Managing access
 - Designer: Creating the workflow and its procedures
 - Operator: Using published procedures



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Access to the software lifecycle framework and to the Software Library that stores all its required entities can be implemented with the following roles:

- The site administrator, a **Super Administrator**, is responsible for creating users, granting them appropriate roles, and maintaining the Cloud Control infrastructure.
- A **Designer** is someone who creates the workflow and its procedures:
 - Define profile or use an Oracle predefined profile (for known configurations, such as Exadata database provisioning).
 - Use profile to create deployment procedures, which are tested and published.
 - Create patching workflows.
 - Lock procedures for use by the operators.
- **Operators** consume the published procedures to deploy or patch software, without necessarily understanding all the nuances of more complex environments.
 - Execute the published procedures on EM targets.
 - Monitor the progress of the executions.
 - Debug any issues that may come up in the executions.

Typically, Designers are assigned the predefined EM_ALL_DESIGNER role and Operators are assigned the EM_ALL_OPERATOR role. These roles include roles for both provisioning and patching tasks, but finer role assignment can be defined as well.

Configuring the Software Library: Review

- Storing certified software entities in:
 - Oracle-owned folders, locked, shipped by default
 - User-owned folders
- Configuring the Software Library:
 - Allocate sufficient space for software binaries and scripts.
 - Storage types:
 - NFS file system
 - Any agent-reachable file system:
 - The OMS Shared File System (recommended for UNIX)
 - The OMS Agent File System (recommended for Windows)
 - Referenced locations (separate from the OMS)



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

A short review from the **Enterprise Manager Cloud Control Installation and Upgrade** course:

The Software Library has two types of folders: Oracle-owned folders (marked by a lock symbol, shipped with the product by default) and user-owned folders.

The storage type can be an NFS file system that is being shared between OMSs or any file system that the agents can reach. You can define referenced locations. So, if you have a centralized location for serving these entities that is separate from the OMS, you can reference them via HTTP, NFS, and so forth. In this case, the OMS stores the metadata about where this referenced location is, and the software bits are stored externally.

If you have multiple OMSs (for High Availability) in your enterprise, create the Software Library in a location that can be accessed by all OMSs.

Super Administrators, who have, by default, complete privileges on all entities present in Software Library, create the additional administrators as they see fit for their enterprise.

Fine-grained access privileges can be defined by the owners of entities or the Super Administrator.

Provisioning Elements

- Component or entity:
 - Building block of the complete software configuration
 - Self-updateable (with MOS connection)
 - Examples: OS, Oracle software, applications, and so on
- Directive:
 - An instruction set for staging, preinstallation, installation, or postinstallation of an image or a component
 - Executed during the provisioning phase
- Gold image: Compliant, tested images for consistent use
- All elements are stored in the Software Library.



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Provisioning allows automated, unattended mass deployments of software to your managed enterprise. Elements of provisioning include:

- **Components:** Are entities or primary building blocks that are combined with other components to specify the complete **software configuration or image** that is provisioned on target machines. A component can be any operating system software, Oracle software, or any third-party software or application. Many of these entities are self-updateable (if there is a connection to MyOracle Support).
- **Directives:** A directive is used as an instruction set. It is a custom script that is associated with a software component and/or image, and executed during one of the provisioning phases from either the target hardware server or the staging server. When you create a directive, specify the directive name, description, and the script type (such as Perl and BASH).
- **Gold images:** Are created by component designers based on corporate standards from reference deployments. They are compliant and tested images, stored in the Software Library, from which they can be used by all operators in a consistent manner.

The Software Library serves as the central repository for metadata and binary content of software patches, virtual appliance images, reference gold images, application software, and their associated directive scripts. The Software Library maintains versions, maturity levels, and states of its entities.

Provisioning Specific Roles and Privileges

- **Site administrator:** Super Administrator for managing all access
- **Designer:** Creates provisioning workflow and its procedures
 - Give Designers the EM_ALL_DESIGNER role.
 - Restrict access with the EM_PROVISIONING_DESIGNER role only.
- **Operator:** Views and uses published procedures
 - Give Operators the EM_ALL_OPERATOR role.
 - Restrict access with the EM_PROVISIONING_OPERATOR role only.
- May require other roles and privileges, depending on the type of target being provisioned

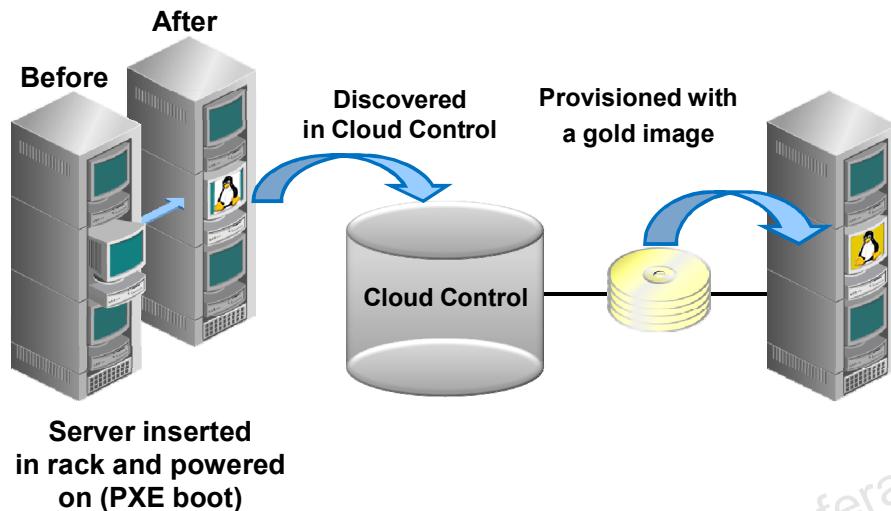
ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

To manage software provisioning, a Super Administrator may create Provisioning Designers and/or Operators. The EM_ALL_DESIGNER role includes EM_PROVISIONING_DESIGNER for provisioning tasks, or you can specifically set up an administrator with only the EM_PROVISIONING_DESIGNER role.

The EM_ALL_OPERATOR role includes EM_PROVISIONING_OPERATOR for provisioning tasks, or you can specifically set up an administrator with only the EM_PROVISIONING_OPERATOR role. Depending on the type of provisioning tasks, other roles and privileges may be required. For example, the Operator Any Target privilege is required for Designers or Operators performing database provisioning.

Bare Metal or OS Provisioning



ORACLE

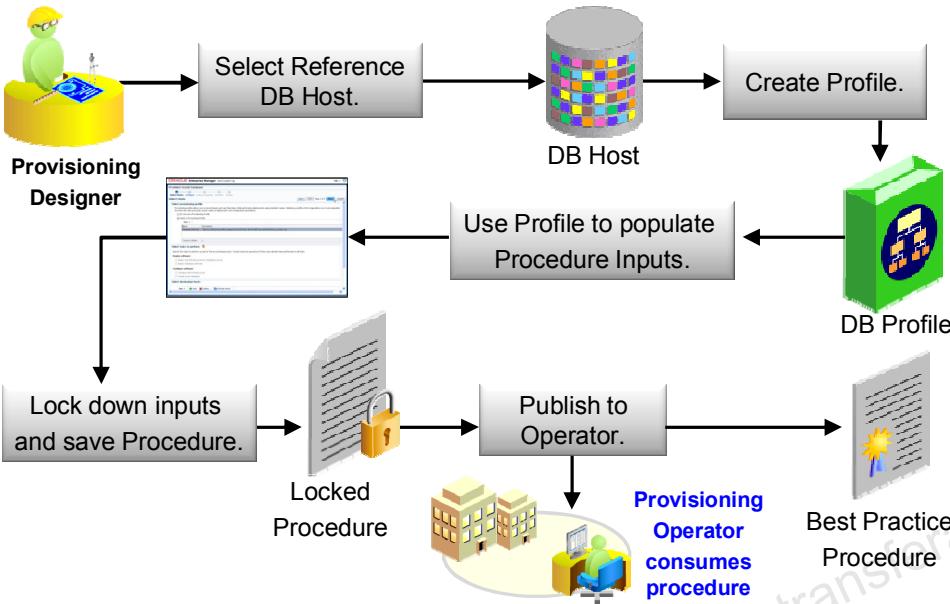
Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The **Bare Metal Provisioning** functionality provides server lifecycle management capabilities that enable you to build, manage, and optimize the server infrastructure. The application provides an automated, repeatable, and reliable solution that:

- Automates the deployment of consistent, certified Linux operating system images along with other software on a large number of servers
- Leads to faster, unattended deployment of software and operating system
- Allows provisioning of middleware, clusterware, and RAC on top of the Linux stack
- Provides a template-based approach for provisioning a variety of Linux configurations with software on servers. This also ensures compliance to standards and consistency across all deployments.
- Supports heterogeneous hardware and network configuration
- Automatically discovers bare metal and live target servers for provisioning
- Encodes Oracle-provided best practices for deployment and patching of Oracle software
- Results in reduction of manual labor that leads to substantial cost savings

The application uses the standardized Pre Boot Execution (PXE) environment booting process for provisioning both bare metal and live servers. It provides a role-based user interface for creating gold images and initiates automated, unattended installations.

Database Software Provisioning Workflow



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The slide depicts the workflow of a database provisioning operation.

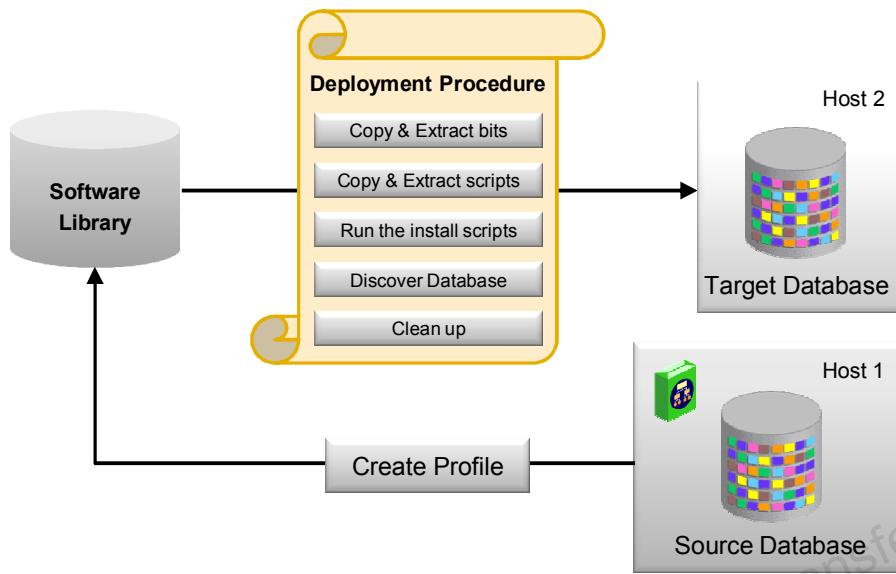
First, the provisioning designer takes a reference database host to create a software image.

So, the provisioning designer creates a profile out of this database host that will contain the software and also the configuration information of this database. The profile helps save the effort involved in repeating the configuration input for each deployment procedure when some of these inputs are identical. Then the provisioning designer uses this profile to create a procedure and populates it with new inputs like ORACLE_HOME, ORACLE_SID and other configuration parameters.

The values stored in the procedure can be locked so that the operator using the procedure for deployment is not able to modify it. The designer then saves the procedure as a locked procedure.

This locked procedure is published by the designer as a best practice procedure to operators for deployment.

Deployment Procedures for Provisioning and Patching Automation



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Deployment Procedures provide a framework to achieve synergy between Oracle's best practices and your own methods. Custom scripts and jobs can be plugged in to deployment procedures for handling special tasks.

How are Deployment Procedures Used?

First, the designer creates a profile from a source host and the software image is copied from the source to the software library.

Then the designer creates a software *deployment procedure* to use this software image from the library to deploy it to a target host, providing all the inputs stored in the procedure, such as installation of the software and also creation of a new database with specific parameters and other attributes. So not only is the software deployed on the target host, but also a new database can be created.

Deployment Procedures: Properties

Deployment procedures:

- Can be extended
- Are reusable
- Can be duplicated
- Are hot pluggable
- Can be automated

Provisioning																																																							
Deployment Procedure Manager																																																							
Procedure Library Procedure Activity Recycle Bin																																																							
Procedures are best practices provided by Oracle for various Provisioning and Patching tasks. Procedures created by Oracle cannot be edited or extended using 'Create Like', so that you can customize the procedure to fit your environment.																																																							
Search Test Fields <input type="text"/> Go Advanced Search																																																							
<table border="1"><thead><tr><th>Launch</th><th>Go</th><th>Edit Procedure Definition</th><th>Create Like</th><th>Launch</th><th>Previous</th><th>1-2</th></tr></thead><tbody><tr><th>Select</th><th>Procedure ▲</th><th>Type</th><th>Parent</th><th>Version</th><th>Last Updated</th><th>Description</th></tr></tbody></table>							Launch	Go	Edit Procedure Definition	Create Like	Launch	Previous	1-2	Select	Procedure ▲	Type	Parent	Version	Last Updated	Description																																			
Launch	Go	Edit Procedure Definition	Create Like	Launch	Previous	1-2																																																	
Select	Procedure ▲	Type	Parent	Version	Last Updated	Description																																																	
<table border="1"><tbody><tr><td><input type="radio"/></td><td>Add Oracle Management Service</td><td>Enterprise Manager High Availability Operations</td><td>None</td><td>1.4</td><td>Jun 24, 2013 6:32:55 AM UTC</td><td>Procedure to add an additional Oracle Management Service to an existing Enterprise Manager system.</td></tr><tr><td><input type="radio"/></td><td>Application Server Deployment 10.1.3</td><td>AS Provisioning</td><td>None</td><td>7.2</td><td>Jul 18, 2013 5:43:48 AM UTC</td><td>This procedure installs or clones and configures a standard Web and Application tier for a multi-tier application server topology.</td></tr><tr><td><input type="radio"/></td><td>Application Server Deployment 10.1.3.x SOA</td><td>AS Provisioning</td><td>None</td><td>7.2</td><td>Jul 18, 2013 5:43:48 AM UTC</td><td>This procedure installs or clones and configures a standard Web and Application tier for a multi-tier application server topology.</td></tr><tr><td><input type="radio"/></td><td>BPEL Process Provisioning</td><td>BPEL Provisioning</td><td>None</td><td>1.2</td><td>Jul 18, 2013 5:43:48 AM UTC</td><td>Procedure for deploying a BPEL Process on a selected Oracle BPEL Process Manager</td></tr><tr><td><input checked="" type="radio"/></td><td>Clone and Patch Oracle Database</td><td>Patch Oracle Software</td><td>None</td><td>12.30</td><td>Jul 18, 2013 5:49:05 AM UTC</td><td>Procedure for automatically cloning a stand-alone database (single instance database) and patching it with critical patch updates, interim patches, or patches. Note: Major upgrade for example, DB 10.1 to 10.2 is not supported.</td></tr><tr><td><input type="radio"/></td><td>Coherence Node Provisioning</td><td>Coherence Node Provisioning</td><td>None</td><td>1.0</td><td>Jul 18, 2013 5:43:49 AM UTC</td><td>Procedure for adding and updating Coherence Nodes.</td></tr><tr><td><input type="radio"/></td><td>Create Oracle Database</td><td>Database Creation</td><td>None</td><td>1.2</td><td>Jul 18, 2013 5:49:05 AM UTC</td><td>Procedure to create Single Instance or RAC database.</td></tr></tbody></table>							<input type="radio"/>	Add Oracle Management Service	Enterprise Manager High Availability Operations	None	1.4	Jun 24, 2013 6:32:55 AM UTC	Procedure to add an additional Oracle Management Service to an existing Enterprise Manager system.	<input type="radio"/>	Application Server Deployment 10.1.3	AS Provisioning	None	7.2	Jul 18, 2013 5:43:48 AM UTC	This procedure installs or clones and configures a standard Web and Application tier for a multi-tier application server topology.	<input type="radio"/>	Application Server Deployment 10.1.3.x SOA	AS Provisioning	None	7.2	Jul 18, 2013 5:43:48 AM UTC	This procedure installs or clones and configures a standard Web and Application tier for a multi-tier application server topology.	<input type="radio"/>	BPEL Process Provisioning	BPEL Provisioning	None	1.2	Jul 18, 2013 5:43:48 AM UTC	Procedure for deploying a BPEL Process on a selected Oracle BPEL Process Manager	<input checked="" type="radio"/>	Clone and Patch Oracle Database	Patch Oracle Software	None	12.30	Jul 18, 2013 5:49:05 AM UTC	Procedure for automatically cloning a stand-alone database (single instance database) and patching it with critical patch updates, interim patches, or patches. Note: Major upgrade for example, DB 10.1 to 10.2 is not supported.	<input type="radio"/>	Coherence Node Provisioning	Coherence Node Provisioning	None	1.0	Jul 18, 2013 5:43:49 AM UTC	Procedure for adding and updating Coherence Nodes.	<input type="radio"/>	Create Oracle Database	Database Creation	None	1.2	Jul 18, 2013 5:49:05 AM UTC	Procedure to create Single Instance or RAC database.
<input type="radio"/>	Add Oracle Management Service	Enterprise Manager High Availability Operations	None	1.4	Jun 24, 2013 6:32:55 AM UTC	Procedure to add an additional Oracle Management Service to an existing Enterprise Manager system.																																																	
<input type="radio"/>	Application Server Deployment 10.1.3	AS Provisioning	None	7.2	Jul 18, 2013 5:43:48 AM UTC	This procedure installs or clones and configures a standard Web and Application tier for a multi-tier application server topology.																																																	
<input type="radio"/>	Application Server Deployment 10.1.3.x SOA	AS Provisioning	None	7.2	Jul 18, 2013 5:43:48 AM UTC	This procedure installs or clones and configures a standard Web and Application tier for a multi-tier application server topology.																																																	
<input type="radio"/>	BPEL Process Provisioning	BPEL Provisioning	None	1.2	Jul 18, 2013 5:43:48 AM UTC	Procedure for deploying a BPEL Process on a selected Oracle BPEL Process Manager																																																	
<input checked="" type="radio"/>	Clone and Patch Oracle Database	Patch Oracle Software	None	12.30	Jul 18, 2013 5:49:05 AM UTC	Procedure for automatically cloning a stand-alone database (single instance database) and patching it with critical patch updates, interim patches, or patches. Note: Major upgrade for example, DB 10.1 to 10.2 is not supported.																																																	
<input type="radio"/>	Coherence Node Provisioning	Coherence Node Provisioning	None	1.0	Jul 18, 2013 5:43:49 AM UTC	Procedure for adding and updating Coherence Nodes.																																																	
<input type="radio"/>	Create Oracle Database	Database Creation	None	1.2	Jul 18, 2013 5:49:05 AM UTC	Procedure to create Single Instance or RAC database.																																																	



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The following properties make deployment procedures useful:

- **Extensible:** Deployment procedures use Oracle-recommended best practices and can be used for any target. Oracle-provided deployment procedures cannot be modified. However, you can create a copy of an Oracle-provided deployment procedure and modify it to insert or delete steps and error-handling modes.
- **Reusable:** Deployment procedures are reusable. The steps of the deployment procedure can be based against directives that are stored in the Software Library. Deployment procedures can also be exported and imported across environments. This implies that the deployment procedures developed for a test environment can be reused for the production environment.
- **Duplicated:** Oracle's default procedures are locked. They cannot be modified, but they can be duplicated with the CREATE LIKE functionality.
- **Hot pluggable:** The Oracle-provided deployment procedures are metadata driven, so new sets of procedures can be added to the Cloud Control environment without any additional outage.
- **Automated:** The runtime for all the deployment procedures, such as Oracle patching, OS patching, and so forth, can be automated using the command line and associated verbs.

Deployment Procedures: Phases and Steps

- A phase contains steps or more phases and is associated with a target list. The types of phases are:
 - Rolling
 - Parallel
- A step is an abstraction of a unit of work. The types of steps are:
 - **Manual:** For example, logging in and updating kernel parameters, rebooting, or providing special privileges to users
 - **Computational:** For example, retrieving target properties from the repository and updating the runtime information
 - **Action:** For example, executing a script, patching, upgrading an Oracle home



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

There are various **phases** and **steps** in a deployment procedure. A phase defines the execution of the steps. The types of phases are:

- **Rolling:** Steps are executed serially across targets.
- **Parallel:** Steps are executed in parallel across targets.

A step is an abstraction of a unit of work (for example, starting the database). It is part of a phase or is independent. The types of steps are:

- **Manual:** A manual step is a task that requires user interaction and cannot be automated. Typically, the Deployment Procedure Manager displays the instructions that need to be performed by the user.
- **Computational:** A computational step is a task whose operations are performed within the deployment engine and does not require any user intervention. This step gathers additional information for executing a procedure. This step cannot be inserted by a user; only Oracle Corporation can insert this step.

- **Action:** An action step is a task that performs some operations that are run on a target or on multiple targets. Action steps must be enclosed within a phase. The Deployment Procedure Manager maps the action step and target pair to a job in the Cloud Control Job System. The Deployment Procedure Manager schedules, submits, and executes a job per action step per target. The types of action steps are:
 - **Job:** Job is a special type of action step that executes a predefined job type on a target. This is used if you want to execute a job type as a part of a deployment procedure. You need to pass job parameters for a step (for example, when staging a patch or starting a database).
 - **Directive:** A directive step is a special type of action step to deploy a directive alone. This is useful when users want to store their custom scripts in the Software Library and reuse them in a deployment procedure. For example, executing root scripts, applying `catpatch.sql` and restarting the database, and confirming if the prerequisites have been met.
 - **Component:** A generic component step is a special type of action step to deploy a Software Library component and the associated directive. The Deployment Procedure Manager executes the directive with respect to the component. The component used for the generic component step generally has one directive associated with it. This association is done by selecting both the component and the directive while creating the step. All directives that you associate with the component while uploading to the Software Library are ignored while executing the step. Examples of a generic component step include applying a patch, validating prerequisites before performing an installation, and installing Oracle software on target machines.
 - **Registered Component:** The registered component step is a special type of action step that consists of a job type and a Software Library component. The Deployment Procedure Manager invokes the specified job type, which handles the staging and installation of the component (for example, cloning Oracle software from the Software Library to the target machine).
 - **Host Command:** This is a special type of action step that encapsulates simple host commands. This step allows the user to enter a command line or a script (multiple commands) to be executed on the target host. For example, starting an agent (`emctl start agent`) or restarting Oracle Internet Directory (OID).

You can provide values to various properties associated with a directive or component through Map Properties. You have three execution privileges: Normal, sudo, and Pluggable Authentication Modules (PAM) for UNIX platforms. You can choose the appropriate privilege you want by selecting the privilege from the Execution privilege list in the Execution Mode section.

Examples of Customized Deployment Procedures

- Insert a custom step to back up the database before patching.
- Insert a manual step to check for key users before stopping a database.
- Shut down and start up an application server to perform operations that are outside the scope of an Oracle-provided procedure.
 - Stopping and starting an enterprise resource planning application
- Set a notification for the deployment procedure run.
 - Based on status



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

- **Shutdown and startup of an application server:** Deployment procedures can be used to perform operations that are outside the scope of the Oracle-provided procedures. Examples include stopping and starting an ERP application or registering a newly provisioned service with the load balancer. Each of these steps can run in the context of any valid operating system user and can make use of a PAM, such as “pbrun” (PowerBroker). They can also run in superuser mode by using “sudo.”
- **Set notification for the deployment procedure run:** To receive notifications from deployment procedures, perform the following steps during design time:
 1. Click **Create Like**.
 2. Select the **Enable Notification** check box, and optionally provide the Notification Tag Name.
 3. Select the statuses for which you would want the notifications to be sent from the list (for example, Success, Failure, or Action Required).
 4. Save the procedure.
 5. Select the **Send Email** option for the standard PAF Status Notification rule from the Notification Rules page under Preferences. Upon running the procedure based on the status selected for notification, the users for whom email addresses are set up would receive notifications.

Software Patching

- Is available for a subset of target types
 - Check product release information for supported patching modes.
 - Examples of products that support patching: specific versions of Oracle Database, RAC, WebLogic Server, and so on
- Must be done by privileged Administrators
- Requires configuration of Software Library
- Patch availability modes:
 - Online
 - Connected to My Oracle Support (MOS)
 - Default mode
 - Offline
 - Not connected to MOS



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Patching Workflow

1. Understand the Oracle patching concepts.
 - Patch Plans and Templates.
2. Set up the infrastructure.
 - Create patch administrators.
 - Set up MOS connection mode.
3. View patch recommendations.
 - Identify patches of interest.
4. Design a patching process for your enterprise.
 - Patch Plans.
 - Analyze Plans.
 - Patch Template.
5. Apply patches.



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Patch plans are lists of patches you want to apply as a group to one or more targets. Patch plans can include patch sets or one-off patches and they automatically map to a patching Deployment Procedure that can complete that task. A patch plan can be **analyzed** against your system or a subset of your targets. At this time, conflicts are identified. If the patch plans complete the analyze phase and are found **deployable**, you can save them as **Patch Templates** that are target independent and they can later be deployed against various other targets. **Undeployable** plans can still be used for analysis and manually downloading and applying patches.

To start using the patching functionality, you must first set up your MOS connection mode (by default, Online) and the various Administrators and their roles required for patching.

Similar to the administrators that perform provisioning tasks, patching activities can be performed by the following:

- Site administrator, a **Super Administrator** responsible for creating users, granting them appropriate roles, and maintaining the Cloud Control infrastructure
- **Patch Designer**, who takes a leading role in creating patch plans and patch templates, as they apply to your organization
- **Patch Operator**, who has a more restrictive role, typically to only view and submit patching jobs

Consider the following when creating the administrators that will be performing patching tasks:

- The EM_ALL_DESIGNER role includes the EM_PATCH_DESIGNER role needed for creating patching tasks, or you can specifically set up an administrator with only the EM_PATCH_DESIGNER role.
- The EM_ALL_OPERATOR role includes the EM_PATCH_OPERATOR role needed for viewing and submitting patching tasks, or you can specifically set up an administrator with only the EM_PATCH_OPERATOR role.

Software Patching Modes

- In-place
 1. Bring down instances in each ORACLE_HOME.
 2. Apply patches to the existing Oracle home.
 3. Restart database instances.
- Out-of-place
 1. Clone your ORACLE_HOME out of place.
 2. Apply patches to the new Oracle home.
 3. Migrate instances to the new Oracle home.
- Rolling and Parallel
 - RAC, Data Guard, and WebLogic type of targets
 - Rolling: Nodes patched one by one, sequentially
 - Parallel: All nodes patched at the same time



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Patches can be applied:

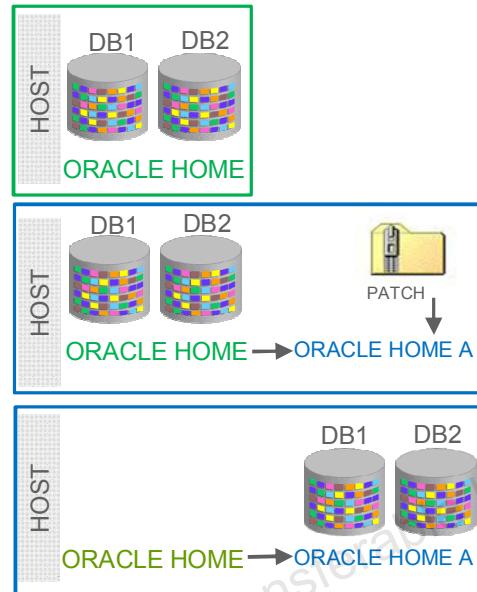
- In place, which requires down time during the patch application
- Out of place, which allows you to clone your Oracle home out of place, perform the patching, and then migrate instances to the new Oracle home. This method reduces the down time requirements for patching. This process also enhances the recoverability; because the old Oracle home has not been touched, you can revert to that in case of issues after patching. This is only available for certain targets.
- Rolling or Parallel, which are applicable to multinode targets such as RAC, WebLogic, and so on. In the rolling method application, each node is patched separately, one by one, whereas a parallel application means all nodes are patched at the same time, requiring down time for the system.

The method of choice depends on your down time requirements and what options are made available by Oracle at patch release time.

The patching process is integrated with My Oracle Support so that you can identify the recommended patches for your environment. After the patches are applied from Enterprise Manager, they do not appear in the recommended patches list for the selected target.

Out-of-Place Patching

1. Multiple databases are running from an **Oracle home**.
2. Clone **Oracle home**.
3. Patch a **cloned Oracle home (no down time)**.
4. Switch instances to the **cloned Oracle home**.
5. Apply SQL scripts (if needed).



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

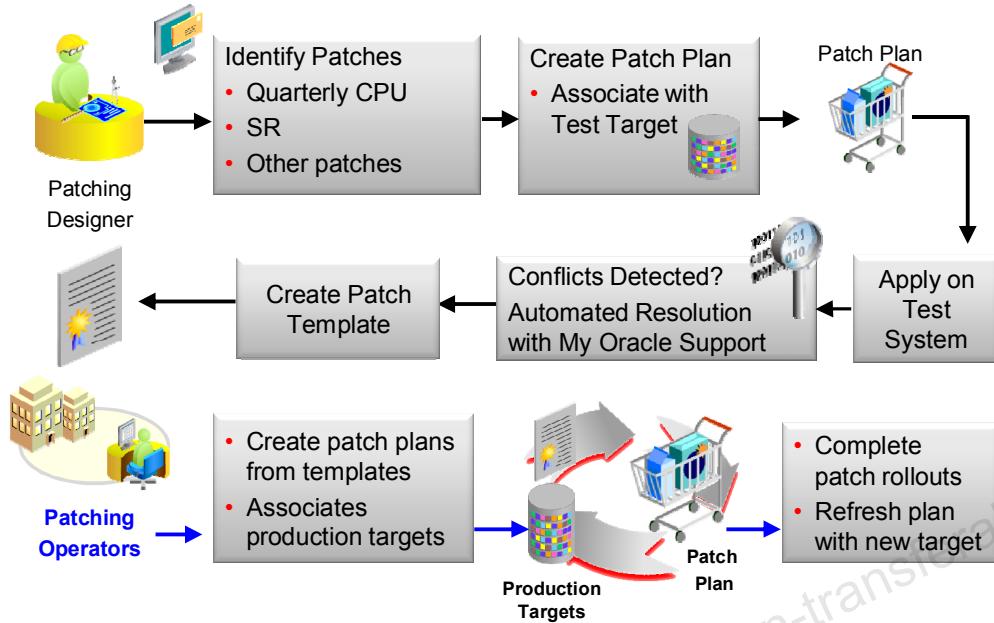
Out-of-place database patching example:

Assume that you have multiple databases in an Oracle home which you need to patch. Cloud Control does the following:

1. Clones the **ORACLE_HOME**
2. Patches the cloned home. These operations do not require down time.
3. Switches all databases to the new patched Oracle home. This requires the database to be shut down.
4. Applies SQL scripts, if required, such as CPU SQL scripts

This workflow gives you the flexibility for easy recovery because you can revert to the original **ORACLE_HOME** and the down time is reduced to the required minimum.

Patching Rollout Cycles Using Templates



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Patching Plan Example Using Templates

Patch templates can be used to define your patch rollouts.

As a patching designer, you identify the patches that need to be applied, such as the quarterly CPU patches recommended by Oracle and the patches recommended by support analysts for specific service request (SR) resolution.

Then you create a patch plan for the identified patches and associate it with a test target.

Testing detects possible conflicts. You can use the Automated Resolution with My Oracle Support to solve the issue. When the testing is complete, you create a patch template from the patch plan. This patch template is published to the patching operators.

The patching operators can create patch plans from templates, associate these patch plans to production targets, and perform regular rollouts.

Oracle Database Software Upgrades

- Upgrade multiple single instance databases in parallel:
 - Check versions supported.
 - Check and implement all prerequisites.
- Extensive pre-upgrade and post-upgrade validation
- Upgrade software and instances combined or separate
- Ability to pause and resume upgrade by setting breakpoints



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Cloud Control supports mass database upgrades via a Deployment Procedure called Upgrade Oracle Database. You can upgrade multiple single instance databases in parallel. There are limited combinations of “Target” and “Release to Upgrade to” versions. Upgrading databases also requires specific privileges and meeting certain prerequisites. Always check the Oracle documentation for the current supported versions and all prerequisites.

This upgrade method is designed to minimize down time by:

- Doing extensive pre-upgrade analysis using MyOracle Support for pre-upgrade patch requirements such as CPUs and PSUs to apply
- Using out-of-place copies and in-context backup before an upgrade
- Including support for pause and resume upgrade execution by setting breakpoints in the process step by step

Using this Deployment Procedure allows you to pre-create a gold image of the version on a test system with all patches applied, which is usable for upgrading your databases.

For more information, view the product documentation and the OLL “Mass Database Upgrade” demonstration.

Oracle Database Software Upgrades: Using Breakpoints

- Set breakpoints to minimize down time.
- Option to set breakpoint at:
 - Initialize Deployment Procedure
 - Execute System Checks
 - Deploy Oracle Database Software
 - Database Upgrade Checks
 - Upgrade Database Instance

ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Quiz



Deployment procedures provide a workflow of all the tasks that need to be performed for a particular lifecycle management activity.

- a. True
- b. False



Answer: a

Quiz



Out-of-place patching:

- a. Involves patching software outside of your data center
- b. Keeps your original Oracle home available for recovery operations
- c. Installs patches directly into your Oracle home



Answer: b

Summary

In this lesson, you should have learned how to:

- Define software lifecycle management
- Describe the different roles and responsibilities
- Define provisioning, patching, and the Software Library
- Configure the Software Library
- Use deployment procedures for provisioning and patching automation
- Patch software
- Define bare metal provisioning



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Practice 11-1 Overview: Preparing for Offline Patching

This practice covers the following topics:

- Verifying a configured Software Library
- Verifying that offline patching is enabled
- Uploading patches to the Software Library
- Creating a patch plan
- Patching software



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Recommended Cloud Control 12c OLL demonstrations that are still applicable:

“Perform Out-of-Place Database Patching” for the Oracle-recommended patching approach, as well as “Mass Database Upgrade”

Practice 11-2 Overview: Patching Offline

This practice covers the following topics:

- Verifying saved patches
- Creating a patch plan
- Patching your targets



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Unauthorized reproduction or distribution prohibited. Copyright© 2019, Oracle and/or its affiliates.

GANG LIU (gangl@baylorhealth.edu) has a non-transferable license
to use this Student Guide.

Managing Configurations

ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Objectives

After completing this lesson, you should be able to:

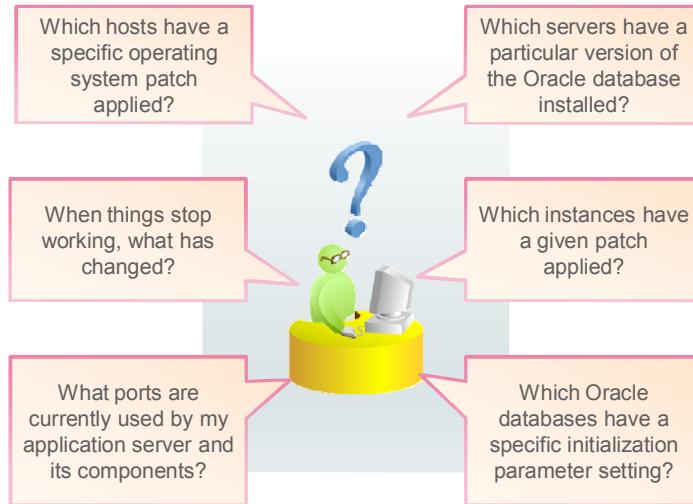
- Explain the need for configuration management
- Describe configuration management
- View configurations of managed targets
- Compare configurations of managed targets
- View the configuration summary for managed targets
- Enable drift and consistency tracking
- Use change activity planning



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

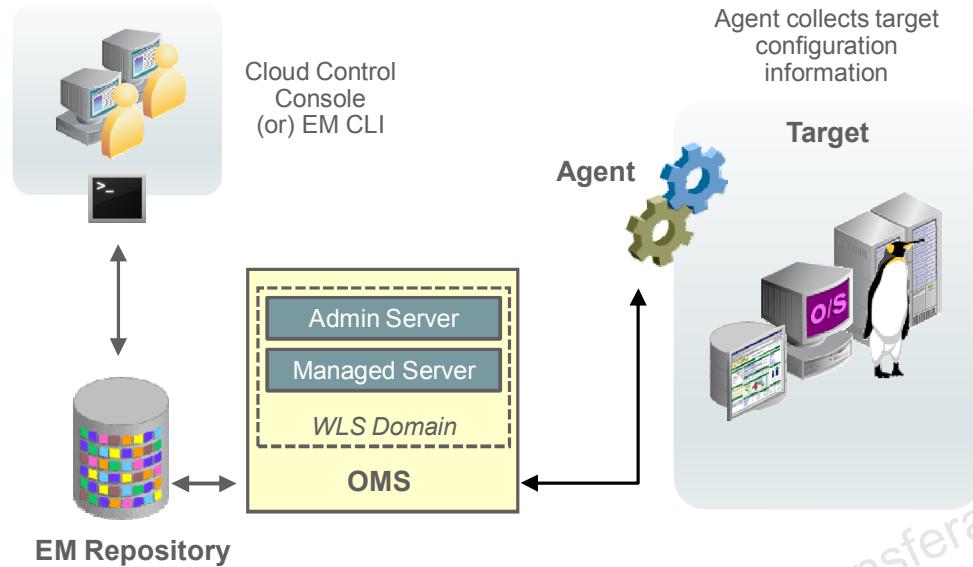
What Is Configuration Management?



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Configuration Management



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Examples of Configuration Information

Target Type	Configuration Information
Host	Hardware, operating system, installed Oracle software (product, patch sets, and interim patches), and operating system-registered software
Database	SGA, PGA, undo tablespace, initialization parameters, and database features
Application Server	Installation type, version, components, and Oracle Process Manager and Notification Server (OPMN) details



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Comparing Configurations

- The Compare Configuration feature finds the similarities and differences between configurations.
- Use it to compare:
 - The current configuration of a selected target type with one or more current configurations of other targets of the same type
 - Saved configurations with one or more saved configurations of the same or other targets
 - Saved configurations with one or more current configurations of the same or other targets
 - A specific configuration with another configuration, and then list the differences immediately
 - A specific configuration with another configuration, and then schedule the comparison as a job
- It is best used for troubleshooting a small number of targets.

ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

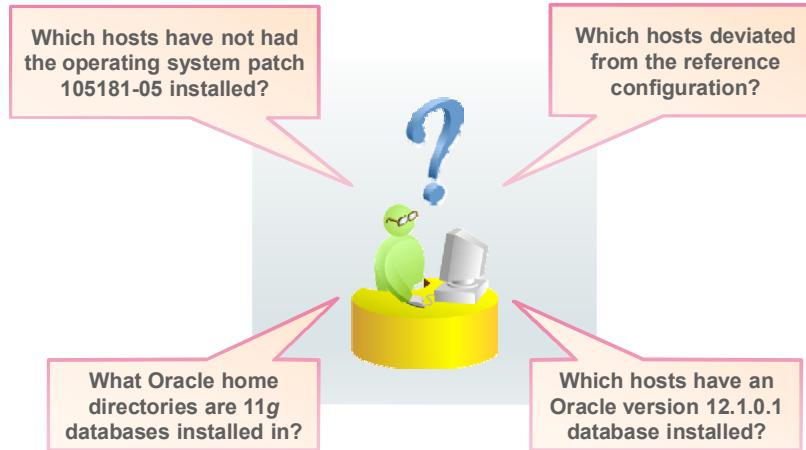
The Compare Configuration feature enables you to compare the configurations of two targets or compare the configuration of one target with a saved configuration stored in a file or in the repository. Using this generic Compare wizard, you can do the following:

- Compare the current configuration of a selected target type with one or more current configurations of other targets of the same type.
- Compare saved configurations with one or more saved configurations of the same or other targets.
- Compare saved configurations with one or more current configurations of the same or other targets.
- Compare a specific configuration with another configuration and list the differences immediately.
- Compare a specific configuration with another configuration and schedule the comparison as a job.

The **Comparison Results Summary** page summarizes the configuration comparison results. You can view the summary of the comparison on this page, and you can navigate to more detailed information about differences in the comparison items.

The comparison feature is best used for a small number of target comparisons, typically for troubleshooting purposes.

Searching the Enterprise Configuration



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

In some cases, you may want to search your enterprise configuration to get answers to specific questions about your enterprise. Enterprise configuration searches query enterprise configuration views in the management repository to find configuration information that satisfies the specified search criteria.

Types of Enterprise Configuration Searches

- **Examples of predefined searches:**
 - Oracle products, patch sets, and interim patches
 - Software registered with the host operating system
 - Initialization parameter settings
 - Tablespaces, data files, and database settings
 - Database feature usage
 - Host operating system components, patches, property settings, and property changes
 - Host operating system and hardware summaries
 - Host file systems and network interface card configurations
 - Various WebLogic searches such as ports and deployed applications
- **User-defined searches**

ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Drift and Consistency Management

- Drift Management
 - Ability to compare configuration against a golden standard
 - Drifted targets tracking
 - Notifications upon deviations
 - Used for a large set of targets
- Consistency Management
 - Ensures targets of similar types remain identically configured
 - Defined consistency is associated with targets
 - Used for a large set of targets
 - Inconsistent targets tracking

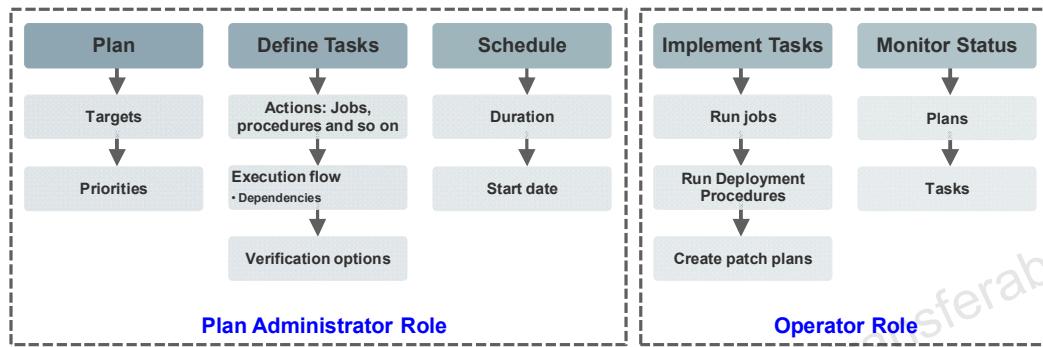


ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Change Activity Planner

- Interface that allows planning, implementing, and tracking of change activities
 - Examples: patching (PSUs), upgrading databases, building and commissioning new databases
- Based on collected configuration data



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The **Change Activity Planner** is a Cloud Control interface tightly integrated with the configuration framework that allows planning, implementing, and tracking of change activities such as scheduling and deploying patches across your enterprise (Patch Set Updates), upgrading databases, building and commissioning new databases, and so on.

Managers, typically with a Plan Administrator type of role, can create change activity plans for complex, long-running projects. They plan resources, designate targets, set priorities, define tasks and their flow, and then schedule tasks. Upon activation of a plan, tasks are automatically assigned to individual owners (typically Operator type of role) based on target ownership. These operators can run and monitor their tasks to completion. Tasks use the Enterprise Manager Cloud Control automation features such as patch plans, jobs, or deployment procedures, or they can be defined as custom tasks.

For more details on this functionality, watch the OLL video still applicable:

Enterprise Manager 12c R3: Change Activity Planner Manages Long-Running Change Process

Quiz



You can use the **Compare Configuration** feature to compare:

- a. Two configurations in the management repository
- b. One configuration with multiple configurations
- c. A configuration in the management repository with a saved configuration file
- d. All of the above



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Quiz



By using configuration management in Cloud Control, you can:

- a. View running jobs
- b. Evaluate down targets
- c. View the hardware configuration of your host
- d. Automatically apply patches



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Summary

In this lesson, you should have learned how to:

- Explain the need for configuration management
- Describe configuration management
- View configurations of managed targets
- Compare configurations of managed targets
- View the configuration summary for managed targets
- Enable drift and consistency tracking
- Use change activity plans



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Practice 12-1 Overview: Viewing Configuration Details

This practice covers the following topics:

- Viewing configuration details:
 - Installed OS packages and their version numbers
 - Other inventory and usage details



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Practice 12-2 Overview: Viewing Configuration History and Topology

This practice covers the following topics:

- Performing a one-time comparison of target configuration
- Creating a drift management definition
- Reviewing drift results



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Practice 12-3 Overview: Comparing Configurations and Managing Drift

This practice covers the following topics:

- Viewing configuration history
 - History records
- Viewing topology
 - Graphical format
 - Table format



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Practice 12-4 Overview: Searching Configurations

This practice covers the following topics:

- Searching configurations
- Saving configurations



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Unauthorized reproduction or distribution prohibited. Copyright© 2019, Oracle and/or its affiliates.

GANG LIU (gangl@baylorhealth.edu) has a non-transferable license
to use this Student Guide.

Managing Compliance

ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Objectives

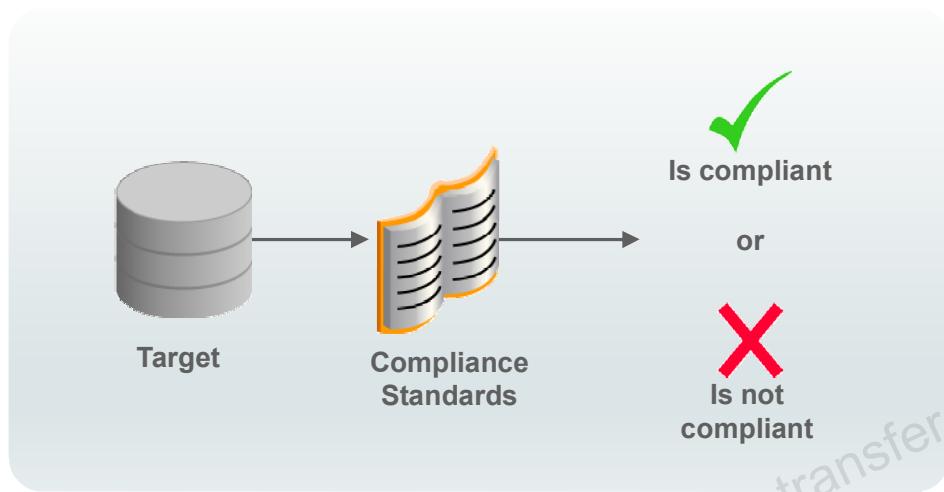
After completing this lesson, you should be able to:

- Define compliance management: framework, standards, rules, and facets
- Describe the predefined compliance standards
- Assign compliance standards to targets
- Explain the compliance evaluation method
- Analyze compliance results



Compliance: Overview

Compliance is conformance to standards or requirements.

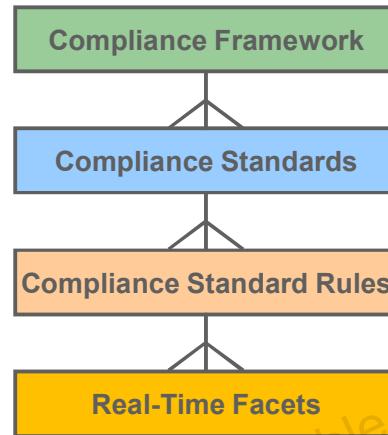


ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Understanding Compliance Management

- **Compliance Standard Rule**
 - Discrete check or test
 - Specific to a target type
 - May result in multiple violations
- **Real-Time Facet**
 - Group of related files, processes, and so on
 - Used by a real-time rule
- **Compliance Standard**
 - Collection of compliance rules
 - Specific to a target type
- **Compliance Framework**
 - Collection of compliance standards
 - Compliance standards can be of different target types



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The compliance management framework of EM Cloud Control provides ways to evaluate targets or systems for compliance with business best practices in terms of configuration, security, storage, and other factors. To use them, you define **compliance frameworks**, **compliance standards**, **compliance standard rules**, and **real-time facets**.

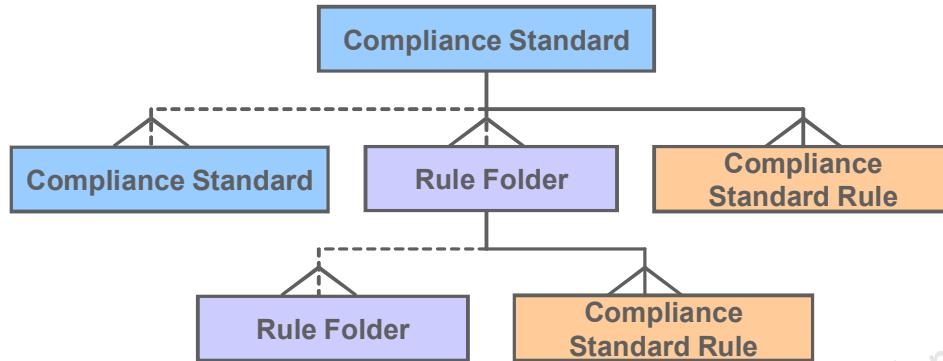
To effectively use a compliance framework, organize the framework to mimic the compliance framework you use in your organization. The compliance framework helps administrators create rules and standards. Compliance security officers and auditors can take advantage of comprehensive compliance reports that are generated based on the structure.

There are two types of compliance frameworks:

- Out-of-the-box predefined compliance frameworks, such as the Security Technical Implementation Guide (STIG), Certification, Payment Card Industry Data Security Standard (PCI DSS), or Oracle Generic Compliance Framework
- User-defined compliance frameworks, which can be based on a predefined compliance framework

Understanding Compliance Standards

Compliance standards comprise compliance standard rules, rule folders, and include compliance standards in a hierarchical structure.



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

A compliance standard defines what to monitor and the conditions for evaluation, and is used to define a compliance framework.

Compliance standards have a hierarchical structure composed of the following entities:

- **Compliance standard rules:** Checks in the form of SQL or other OS scripts. Rules can be part of multiple compliance standards.
- **Rule folders:** Include individual compliance standard rules and nested rule folders. Rule folders are a mechanism to organize rules in a compliance standard. A rule folder can only be used within the compliance standard in which it is created.
- **Other compliance standards:** Various compliance standards of the same target type can be included.

Compliance standards are the entities that must be *associated* to targets in order for evaluations to take place. All rules within a standard are then evaluated.

Hundreds of predefined compliance standards, with thousands of rules, are provided with Enterprise Manager Cloud Control, for various target types such as database instance, listener, and host. You may use these compliance standards when defining your own compliance frameworks or define new compliance standards. You can use the “Create Like” feature to create a new compliance standard with the same definition as a predefined compliance standard. Only user-defined compliance standards can be edited and tailored for your environments.

Understanding Compliance Standard Rules

- **Repository rule:**
 - Used to validate metric collection data in the Enterprise Manager repository
 - Repository browser can be used to aid in rule creation
- **Real-time monitoring rule:**
 - Used to monitor actions against files, processes, and other structures
 - Also can be used to capture login/logout information
- **WebLogic Server signature rule:**
 - Used to check a WebLogic target for best practice configuration
- **Agent-side rule:** Checks for violations on agent side, metrics automatically collected



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Compliance standard rules specify the “check” that is to take place against the target to help determine its compliance.

You can define the following types of compliance standard rules:

- **Repository rule:** A repository rule is evaluated against the repository data only when the data changes underneath and uses the current data that exists in the repository. A repository browser is provided to aid in rule creation to build the query.
- **Real-time monitoring rule:** A real-time monitoring rule activates the agent to perform real-time change detection for file actions, schema actions, and process actions, to detect when and where a particular action took place and who performed the action. You can apply the rule to a particular target type. A real-time monitoring rule can also be used to detect unauthorized changes and correlate them to the Change Management System.
- **WebLogic Server Signature rule:** A WebLogic Server Signature rule performs BEA Guardian health checks using the Cloud Control agent and is used to check a WebLogic target against Oracle Support best practices.
- **Agent-side rule:** An agent side rule checks for violations on the agent side.

Agent-side rules are implemented using **configuration extensions**, which provide a way to extend the compliance framework. These extensions must first be defined to collect data that Cloud Control does not already collect, and then associated with an agent side rule. The association automatically deploys to the agent all needed logic to perform the checks.

In addition, you can define a **manual** rule for tasks that cannot be automated.

Implementing Compliance Management

1. A **Super Administrator** defines the Compliance users.
 - A. Creates or assigns Enterprise Manager users: Compliance Author, IT Administrator, and Compliance Auditor
 - B. Assigns the appropriate roles and privileges to the Compliance Author and the IT Administrator
 - C. Assigns the same target privileges to the IT Administrator and the Compliance Auditor
2. The **Compliance Author/Designer** defines company compliance rules and standards.
 - A. Reviews out-of-the-box compliance standards and rules
 - B. Creates new compliance standard rules as needed



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The steps in this slide and the next slide describe how a typical Cloud Control structure can be defined so that auditors can verify that targets are in compliance with the organization's compliance framework.

1. First, a Super Administrator creates or assigns existing EM administrators the following three distinct job roles:
 - A **Compliance Author or Designer** is the designer of the compliance standards, rules, and facets. This user is given the predefined role `EM_COMPLIANCE_DESIGNER`, which includes some target management privileges.
 - A **Compliance Auditor or Officer** is the consumer of the compliance entities defined by the author/designer. The Auditor creates the Compliance Frameworks. This user is given the `EM_COMPLIANCE_OFFICER` role with visibility across a data center and no specific target privileges.
 - An **IT/DBA Administrator** associates targets with standards, and reviews and resolves compliance violations. This administrator typically is the owner of the targets.
2. The Compliance Author/Designer reviews Oracle pre-created standards and rules and creates new ones based on the company policies.

Implementing Compliance Management

3. The **IT Administrator** works on targets.
 - A. Sets up monitoring configuration parameters as needed by compliance standards and rules, for a particular test target
 - B. Creates monitoring templates from the test target and applies them to the other targets that require compliance standards
 - Use of Administration Groups and Template Collections recommended
 - C. Associates the targets with the appropriate compliance standards
4. The **Compliance Auditor/Officer** oversees compliance.
 - A. Creates Compliance Frameworks
 - B. Views violations and errors at the enterprise level



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

3. IT Administrators or DBAs prepare the targets to be monitored for compliance, starting with a test target and then all targets in that category. Compliance checks use data collected on targets. It is recommended that you group targets into Administration Groups, for easy management of targets, including auto-deployment of monitoring settings to targets when a new target joins the group. Management and monitoring settings can be defined via monitoring templates, or sets of templates (Template Collections), and associated with targets.
4. Compliance Officers evaluate compliance at the enterprise level based on frameworks created and their compliance rolled-up information.

Understanding Compliance Measurement

- Compliance is measured through the evaluation of compliance standards.
 - Scores are calculated.
- Compliance evaluation process:
 - Evaluate standard rules that are part of a compliance standard by performing single health or real-time monitor checks:
 - Can result in one or more violations
 - Summarize the evaluation scores for a compliance standard as a whole.
 - Roll up the results to the framework level.
 - Violations against a target are reported to the OMS and presented on the Compliance Results page and target home pages.



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Score and Its Factors

- Score:
 - Percentage that reflects the degree of conformance with a given standard
 - By rule, target, or framework
- Dependent on:
 - Severity: Critical, Warning, or Minor Warning
 - Set at standard or rule creation time
 - Importance: Low, Normal, or High
 - Set when standard or rule is added to a framework



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The compliance **score**, measured as a percentage, is the degree of conformance with a particular standard. The score is a combination of *severity*, *importance*, and the percentage of *objects* found to be noncompliant.

The *severity* level is defined at rule creation time and can typically be specified as Critical (serious if this rule is violated), Warning, or Minor Warning (a minor impact if violated). Each level translates to a number during the internal calculations.

You can also set the *importance* of compliance standards when you define a compliance framework. The importance setting of a compliance standard within the compliance framework impacts the overall framework compliance score. Importance can be set to Low, Normal, or High, and these translate internally to a number.

The score for each standard *rule* is calculated as a function of the high and low range severity values and the number of violations per rows evaluated. For example, this is the formula used here:

High Range - (High Range - Low Range) * (number of violations / number of rows evaluated), where High Range and Low Range are predefined values depending on the importance.

In turn, the compliance score of a particular *target* against a set of rules is calculated as an average of the individual rule scores and their importance.

Finally, a compliance *framework* score is a rolled-up weighted average of all target scores across all compliance standards within that compliance framework.

Refer to the *Enterprise Manager Cloud Control Oracle Database Compliance Standards* for detailed information about database compliance score calculation formulas.

Accessing the Compliance Library

Use each tab to view and define the Compliance Library entities.

Compliance Framework	Description	Compliance Framework State	Author	Keywords	Last Updated Date
Certification	A set of standards for tracking certifications of Oracle products across your IT infrastructure	Production	ORACLE	Configuration	Aug 24, 2015 1:30:33 PM GMT+00:00
Oracle 11.2g Database Security Technical Implementation Guide (STIG)	A set of standards to ensure Oracle 11.2g Database Security Technical Implementation Guide (STIG) compliance.	Production	ORACLE	Security	Aug 24, 2015 1:43:00 PM GMT+00:00

ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Access the Compliance Library page to manage your compliance infrastructure by selecting **Enterprise > Compliance > Library**. Use the tabs to access each of the compliance entities. You can view the predefined out-of-the-box compliance frameworks, compliance standards, and compliance standard rules on the corresponding tabs. You also use each tab to access the feature to create a new compliance entity or to use the “create like” functionality to define a new entity based on an existing entity.

Associating Targets to Compliance Standards

The screenshot shows the 'Compliance Library' page. At the top, there are tabs for 'Targets', 'Compliance Standards' (which is selected), and 'Compliance Standard'. Below the tabs is a toolbar with buttons for 'View', 'Create...', 'Create Like...', 'Show Details', 'Edit...', 'Delete', 'Associate Targets...', and 'Associate Groups...'. A red box highlights the 'Associate Targets...' button with the instruction: '1. Select the compliance standard you want to associate a target to.' Another red box highlights the 'Associate Targets...' button with the instruction: '2. Click "Associate Targets" to access the Target Association page.' The main area displays a table with two rows of compliance standards. The columns are 'Compliance Standard', 'Description', 'Compliance Standard State', 'Applicable To', and 'Keywords'. The first row contains 'Security Recommendations For Oracle Products' with a description about patch recommendations, 'Production' as the state, 'Host' as the applicable target, and 'Security, Configuration' in the keywords. The second row contains 'Storage Best Practices for ASM' with a description about ASM settings, 'Production' as the state, 'Automatic Storage Management...' as the applicable target, and 'Storage' in the keywords.

Compliance Standard	Description	Compliance Standard State	Applicable To	Keywords
Security Recommendations For Oracle Products	Ensures adherence with best-practice security patch recommendations settings that help protect against Oracle products, providing a more secure operating environment for Oracle products.	Production	Host	Security, Configuration
Storage Best Practices for ASM	Checks the Automatic Storage Management (ASM) settings to ensure that customers are correctly setting up the disk groups and therefore avoiding potential space and performance problems.	Production	Automatic Storage Management...	Storage

ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Investigating Compliance Violations

- Compliance is integrated with Incident Manager.
 - Events can be set and generated for:
 - Each compliance rule violation
 - Compliance score below a threshold
- First resolve the most critical compliance violations.
 - View Compliance Dashboard for a summary of all systems.
- You can then investigate:
 - Compliance violations with critical severity
 - Security-related violations
 - Targets with the lowest compliance scores
 - Compliance violations of a database or host target by using the compliance summary and trend information



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Viewing Compliance Evaluation Results

The screenshot shows the 'Compliance Results' page. At the top, there are three tabs: 'Compliance Frameworks', 'Compliance Standards' (which is selected), and 'Target Compliance'. Below the tabs, there are sections for 'Evaluation Results' and 'Errors', with buttons for 'Search', 'View', 'Show Details', and 'Manage Violations'. A 'Compliance Standards' section displays 'Security Recommendations For Oracle Products' and metrics for 'Production' and 'Host' environments. An 'Average Score (%)' bar chart shows a score of 100. A callout box points to the 'Compliance Standards' tab with the text: 'Use the Compliance Frameworks and Compliance Standards tabs to view summary information.' Another callout box points to the 'Target Compliance' tab with the text: 'Use the Target Compliance tab to view target compliance evaluation results.' A third callout box points to the 'Compliance Summary' section with the text: 'The Compliance Summary region of the target home page displays compliance evaluation results.'

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

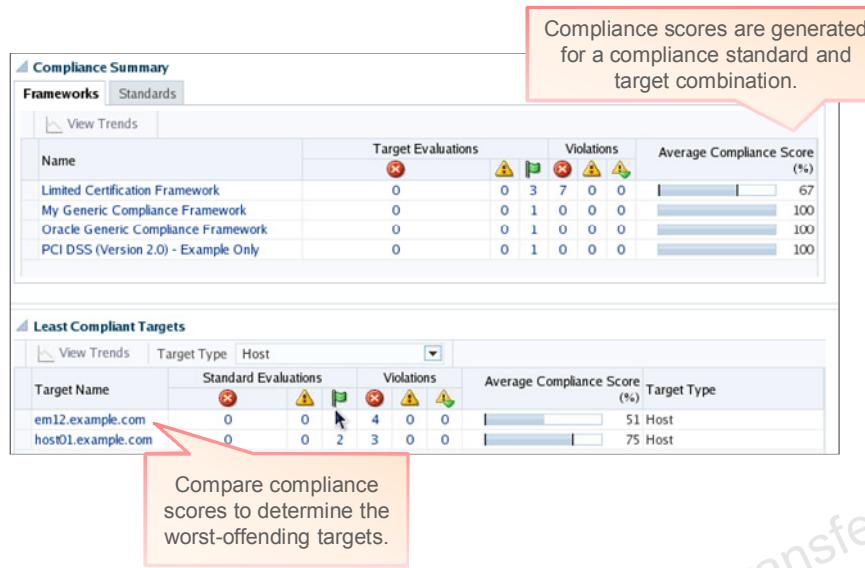
ORACLE

You can view compliance summary information on the Enterprise Manager Cloud Control Summary page and on the individual target home pages.

In the Compliance Standard Summary region of a target's home, you can obtain a comprehensive view of a target's compliance over a period of time. Use the tables and graphs to watch for trends and changes.

You can drill down into each compliance standard listed to get more information about trends, the rules that are violated, what targets violated them, and how many times they were violated, as well as specific events that were triggered due to these violations and their recommended resolution.

Viewing Compliance Scores



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

The screenshot in the slide shows the Compliance Summary section and the Least Compliant Targets section of the Enterprise Manager Cloud Control Summary page.

Compliance scores provide an overall evaluation of a target's compliance to defined standards.

Compliance scores are generated for a compliance standard and target combination, which represents a target's compliance with a certain standard. The score indicates the degree to which the target is compliant with the standard. A 100% Compliance Score indicates that the target follows all requirements/regulations imposed by the compliance standard.

By comparing compliance scores, you can determine the worst-offending targets, which enables you to give those targets particular attention. In other words, as the score becomes lower, the compliance status becomes worse. A compliance score of 100% indicates a fully compliant target with respect to that policy.

Compliance scores are also shown on the Compliance Results pages (**Enterprise > Compliance > Results**).

Viewing Out-of-the-Box Compliance Reports: Dashboard

You can view descriptive reports showing the compliance entities in the Compliance Library.

ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

You can access compliance reports by selecting Information Publisher Reports in the Enterprise menu. Scroll to the Compliance section to view the following types of compliance reports:

- **Descriptions:** Reports that list all the compliance frameworks, compliance standards, and compliance standard rules available in the Compliance Library. You can use these reports to help you determine whether you need to create additional compliance entities to correspond to your organization's compliance standards.
- **Results:** These reports provide detailed information about the evaluation against the defined compliance frameworks and compliance standards. The "Target with Lowest AVG COMPLIANCE SCORE" report helps you determine any targets that need immediate attention.

Quiz



Oracle Enterprise Manager Cloud Control provides predefined compliance rules, standards, and frameworks.

- a. True
- b. False



Quiz



A compliance framework:

- a. Is unique for a target type
- b. Can span several target types
- c. Does not take target types into account



Answer: b

Summary

In this lesson, you should have learned how to:

- Define compliance management: framework, standards, rules, and facets
- Describe the predefined compliance standards
- Assign compliance standards to targets
- Explain the compliance evaluation method
- Analyze compliance results



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Practice 13-1 Overview: Reviewing Predefined Compliance Objects

This practice covers the following topics:

- Reviewing predefined (out-of-the-box) compliance objects
- Searching for a specific compliance standard rule



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Recommended demonstrations on OLL that still apply:

“Oracle Enterprise Manager 12c: Use and Report on Out-of-Box Compliance Standards” (some newer functionality may not be part of this demo)

“Oracle Enterprise Manager 12c: Using STG Compliance Std”

“Oracle Enterprise Manager 12c: Using Agent-Side Compliance Rules”

Practice 13-2 Overview: Using Compliance Standards

This practice covers the following topics:

- Using compliance standards:
 - Creating a new compliance standard
 - Associating targets to the new compliance standard



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Recommended demonstrations on OLL that still apply:

“Oracle Enterprise Manager 12c: Use and Report on Out-of-Box Compliance Standards” (some newer functionality may not be part of this demo)

“Oracle Enterprise Manager 12c: Using STG Compliance Std”

“Oracle Enterprise Manager 12c: Using Agent-Side Compliance Rules”

Unauthorized reproduction or distribution prohibited. Copyright© 2019, Oracle and/or its affiliates.

GANG LIU (gangl@baylorhealth.edu) has a non-transferable license
to use this Student Guide.

Using the Cloud Control Reporting Framework

The Oracle logo, consisting of the word "ORACLE" in white capital letters on a red rectangular background.

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Objectives

After completing this lesson, you should be able to:

- Explain the basics of BI Publisher reporting
- View and customize out-of-the-box reports
- Create custom reports
- Schedule reports



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Oracle recommends the use of BI Publisher (BIP) for reporting. BIP offers many advantages such as flexible formatting, various access and scheduling capabilities, and so on. Information Publisher reports are deprecated from release 12c 12.1.0.2 on; older versions remain supported.

This lesson is intended only as an **introduction** to BI Publisher.

Introduction to BI Publisher

- Framework for creating custom reports based on management repository data:
 - Custom data, charts, and layouts
 - High-quality formatting
 - Security integrated with Cloud Control
 - Java application deployed in a J2EE container
- Oracle predefined reports:
 - Various formats
- Has the ability to:
 - Schedule report generation.
 - Deliver produced reports via email and FTP.
 - Store scheduled copies for future reference.



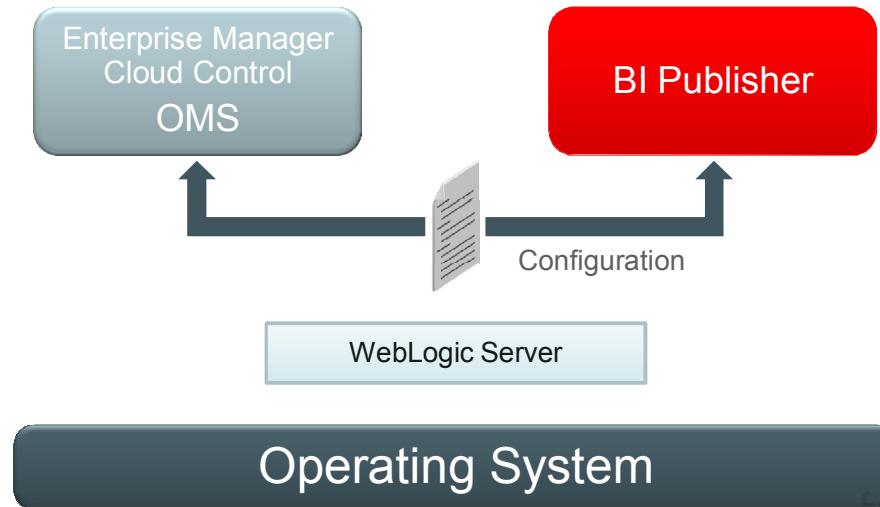
Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

BI Publisher, Cloud Control's integrated reporting framework, makes information about your managed environment available to users across your enterprise. Reports are used to present a view of enterprise-monitoring information for business intelligence purposes, but can also serve an administrative role by showing activity, resource utilization, and configuration of managed targets. IT managers can use reports to show availability of sets of managed systems. Executives can view reports on the availability of applications (such as corporate email) over a period of time.

The reporting framework allows you to create and publish high-quality customized reports. Reports can be stored and shared with selected recipients. BI Publisher comes with a comprehensive library of predefined reports that allow you to generate reports out-of-the-box without additional setup and configuration.

Starting with Enterprise Manager Cloud Control 12.1.0.4, Oracle BIP is installed and configured by default.

BI Publisher Configuration with Enterprise Manager



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

BI Publisher Access

- Cloud Control administrators must explicitly be granted access to the reporting framework.
- EM CLI interface for granting BIP Roles:
 - **EMBIPViewer:** Log in and run the out-of-the-box reports or reports to which you have access.
 - **EMBIAuthor:** Create reports.
 - **EMBIPScheduler:** Schedule execution of reports of which you have view access.
 - **EMBIPAdministrator:** Provides full access to all BI Publisher functionality and is automatically granted to Super Administrators to allow initial setup



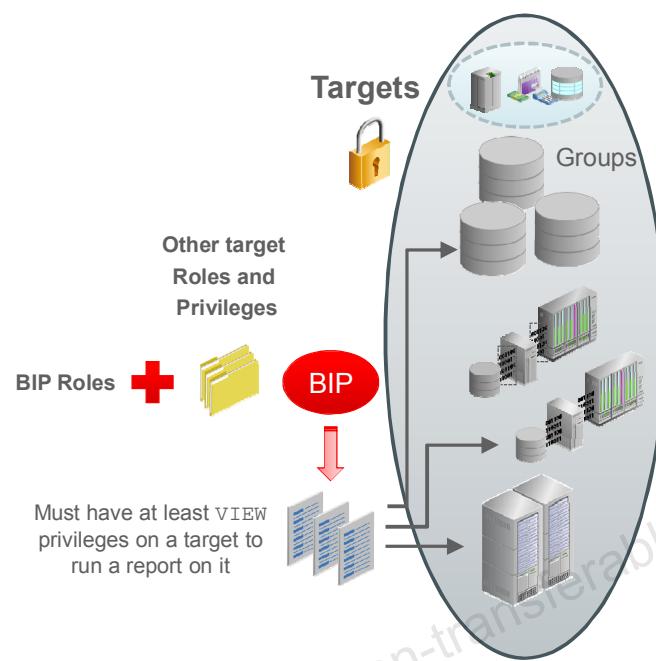
Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Reporting on Targets

Cloud Control
Administrators with
BIP Roles



- EMBIPViewer**
- EMBIPAuthor**
 - Includes EMBIPViewer
- EMBIPScheduler**
 - Includes EMBIPViewer
- EMBIPAdministrator**
 - Includes all BIP roles



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

ORACLE

BIP roles control the reporting functionality available to a user, while Cloud Control as well as target roles and privileges control the data that can be displayed on the reports.

For example, a Cloud Control administrator with the EMBIPViewer role and with at least VIEW privileges on a target can view a BIP report on that target.

BI Publisher Elements

- Reports
 - Formatted set of data for a given set of managed targets
 - Attributes: Parameters, Layout, Output type
- Catalog
 - Collection of reports
 - Predefined and custom
- Data Models
 - Queries against the Cloud Control repository
- Templates
 - Layout and formatting
- Report Jobs
 - Scheduled reports
 - Various delivery methods



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

BI Publisher reports are based on sets of data that have been collected for your managed targets and presented as professionally formatted documents.

Reports have various attributes such as:

- **Parameters:** Targets you want to include in the report, date ranges, and so on
- **Layout:** The desired way of sorting and displaying the report data
- **Output type:** Various types of documents, such as HTML, PDF, RTF, and so on

BI Publisher stores all reports and other objects in a **Catalog**. Cloud Control includes predefined reports out-of-the-box and custom reports can be created using the BIP framework.

A **data model** is an object that contains a set of instructions for BIP to retrieve and structure data for a report. Data models reside as separate objects in the catalog.

A **style template** contains style information that can be applied to RTF layouts to provide a consistent look and feel across your enterprise reports.

Reports can be scheduled, one-time or on a recurring basis, to run via **Report Jobs** and be delivered to email addresses, printers, and so on.

Report Definitions

- Define and save a report:
 - Data Model
 - Data source
 - Data set and its structure
 - Layout
 - User access
 - Location for storing reports
- Generate a report:
 - Output format: PDF, HTML, Excel
 - Destination: Email, printer, fax
 - Scheduling information
 - Notification options



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

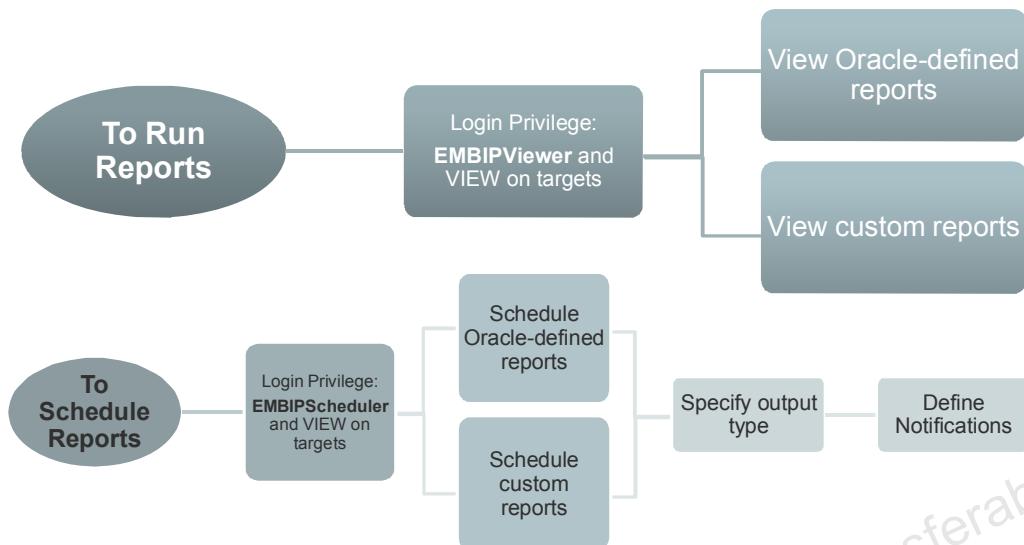
A report definition indicates how to create a report. It provides information such as the following:

- **Data source:** Where the data comes from, how it is structured, and what should be displayed in the report. The data source for these reports is the Cloud Control repository.
- **Layout:** How the information should be displayed
- **User access:** Who should have access to view, edit, or run the report
- **Save location:** The folder the report should be saved in

When running a saved report, you describe the following:

- **Output type:** What format the output will be in
- **Destination:** Email, printers, fax, and so on
- **Scheduling information:** When the report should run (immediately, later, or on a periodic basis)
- **Notification options:** Where and how to be notified when the report is available

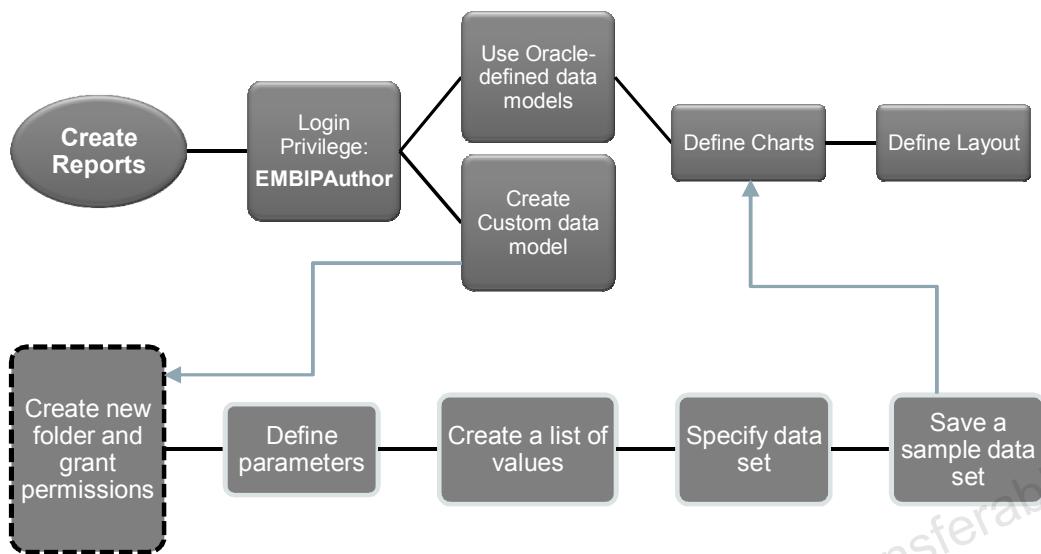
Running and Scheduling Reports: Workflows



A Cloud Control administrator with EMBIPViewer privileges can run Oracle predefined or custom reports on targets that it has at least VIEW privileges on.

A Cloud Control administrator with EMBIPScheduler privileges can schedule Oracle predefined or custom reports on targets that it has at least VIEW privileges on. This administrator can also define the types of outputs and notifications for these reports.

Creating Custom Reports: Workflow



Custom reports can only be created by Cloud Control administrators with EMBIPAuthor privileges. These administrators have full privileges to define new data models or use predefined data models, and they can define custom layouts by using the Layout Editor.

Full report definitions and details on creating custom data models and layouts are beyond the scope of this course. Be sure to watch the Oracle Enterprise Manager Cloud Control 13c BI Publisher video series published on OLL.

Scheduling Reports

- Frequency of the run
 - Once (immediately)
 - One time (later)
 - Start date
 - Start time
 - On a repeating schedule
 - Frequency
 - Start date and time
 - End date and time (can be indefinite)
- Condition of the run
 - No trigger
 - Use trigger
 - Trigger checked at the scheduled time
 - Trigger defined in the data model



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

By default, a report runs one time (immediately). If you want, you can schedule a report to run once at a later time or repeatedly over a period of time. Choices for type of schedule are as follows:

- **One Time (immediately):** This is the default behavior.
- **One Time Later:** You specify time zone, start date, and start time information.
- **Repeating:** You choose a frequency type and then enter how often to repeat based on the frequency type. Also, specify the time zone, start date, start time, and repeat until (indefinite or specified date/time) information.

Scheduled reports must always be run by using the target privileges of the report owner.

Reports Output Options

- Multiple outputs can be defined for one report.
- Saved for future reference:
 - Republishing
 - Can be made public
 - Viewed from Report Job History
- Various formats:
 - HTML, PDF, RTF, Excel, and PowerPoint
- Sent to multiple destinations:
 - Email, Printer, Fax, FTP, and Web folder
 - Destinations must be preconfigured



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Oracle-Provided Reports

- A catalog of predefined reports and data models comes with BI Publisher out-of-the-box.
- They are available to all Cloud Control administrators who were given access.
- They can be used to create customized reports to suit specific operational needs.
 - Must make a copy and then customize
- They are grouped by functional categories.



Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Quiz



In order to **run** a report on a target, you must:

- a. Log in to BI Publisher
- b. Connect to the target as a privileged user
- c. Have at least **VIEW** privileges on that target within Cloud Control
- d. Do nothing. Cloud Control can run reports automatically.



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Quiz



Valid BI Publisher report formats include:

- a. .BAT and .SH
- b. .HTML, .PDF, .RTF, .XLS, and .PPT
- c. .UPS and .DHL



Answer: b

Summary

In this lesson, you should have learned how to:

- Explain the basics of BI Publisher reporting
- View and customize out-of-the-box reports
- Create custom reports
- Schedule reports



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Practice 14-1 Overview: Reviewing and Running Oracle-Provided Reports

This practice covers the following topics:

- Accessing BI Publisher
- Exploring the out-of-the-box sets of reports and data models
- Running and viewing a predefined report
- Granting various privileges to users



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Practice 14-2 Overview: Editing a Report with BI Publisher

This practice covers the following topics:

- Accessing BI Publisher with authoring privileges
- Editing a report



ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Practice 14-3 Overview: Scheduling a Report with BI Publisher

This practice covers the following topics:

- Accessing BI Publisher with scheduling privileges
- Scheduling a report



ORACLE

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Unauthorized reproduction or distribution prohibited. Copyright© 2019, Oracle and/or its affiliates.

GANG LIU (gangl@baylorhealth.edu) has a non-transferable license
to use this Student Guide.