ORACLE UNIVERSITY

Integrated Cloud Applications & Platform Services

Oracle Enterprise Manager Cloud Control 13*c*: Install & Upgrade

Student Guide

D92195GC20

Edition 2.0 | May 2017 | D100216

Learn more from Oracle University at **education.oracle.com**

ORACLE

Author

Lachlan Williams

Technical Contributors and Reviewers

Sumesh Balakrishnan

Angeline Dhanarani

Curtis Dinkel

Editor

Vijayalakshmi Narasimhan

Graphic Editor

Prakash Dharmalingam

Publishers

Giri Venugopal

Michael Sebastian Almeida

Raghunath M.

Contents

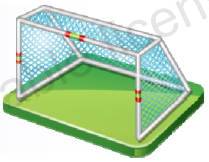
1

Introduction

Course Goals

After completing this course, you should be able to:

- Describe the architecture of Cloud Control 13*c*
- Describe various topology options for deploying Cloud Control 13*c*
- Install Cloud Control 13*c* in a single-server topology
- Map upgrade paths from Grid Control and earlier versions of Cloud Control
- Describe and perform the 1-System upgrade
- Describe Cloud Control implementation planning considerations



ORACLE

This course is designed to give you hands-on experience in installing Enterprise Manager Cloud Control 13*c* and upgrading from earlier versions. You are introduced to the general architecture of an Enterprise Manager Cloud Control 13*c* installation and the topologies within which it can be deployed, as well as the considerations to be taken into account when planning a Cloud Control implementation.

Lesson Objectives

After completing this lesson, you should be able to:

- Explain the need for Oracle Enterprise Manager Cloud Control 13*c*
- Describe the key features of Oracle Enterprise Manager Cloud Control 13*c*
- Describe the classroom environment that is used for the practice activities
- Start, log in to, and stop a virtual machine on your student desktop

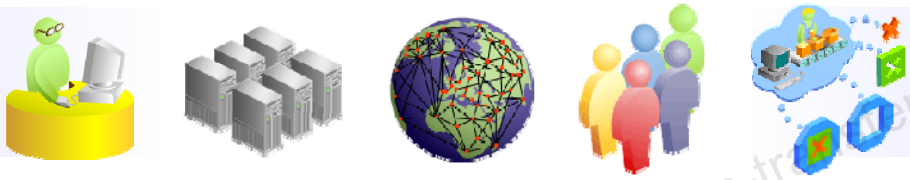
What Is Enterprise Manager Cloud Control 13*c*?

- An on-premises management platform
- 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

Oracle Enterprise Manager Cloud Control 13*c* is an application that is built on an extensible framework that uses agents deployed throughout your IT infrastructure to help you monitor and manage that infrastructure. Utilizing a core framework for authentication and authorization, job management, and metrics processing, Cloud Control 13*c*'s product management functionality is provided through a plug-in infrastructure. This allows for independent plug-in updates to keep pace with changes in the managed products, as well as the installation of new plug-ins to extend the available functionality and capability of Cloud Control 13*c*.

Why Do I Need Enterprise Manager Cloud Control 13*c*?

- Contrasting server manufacturers and 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

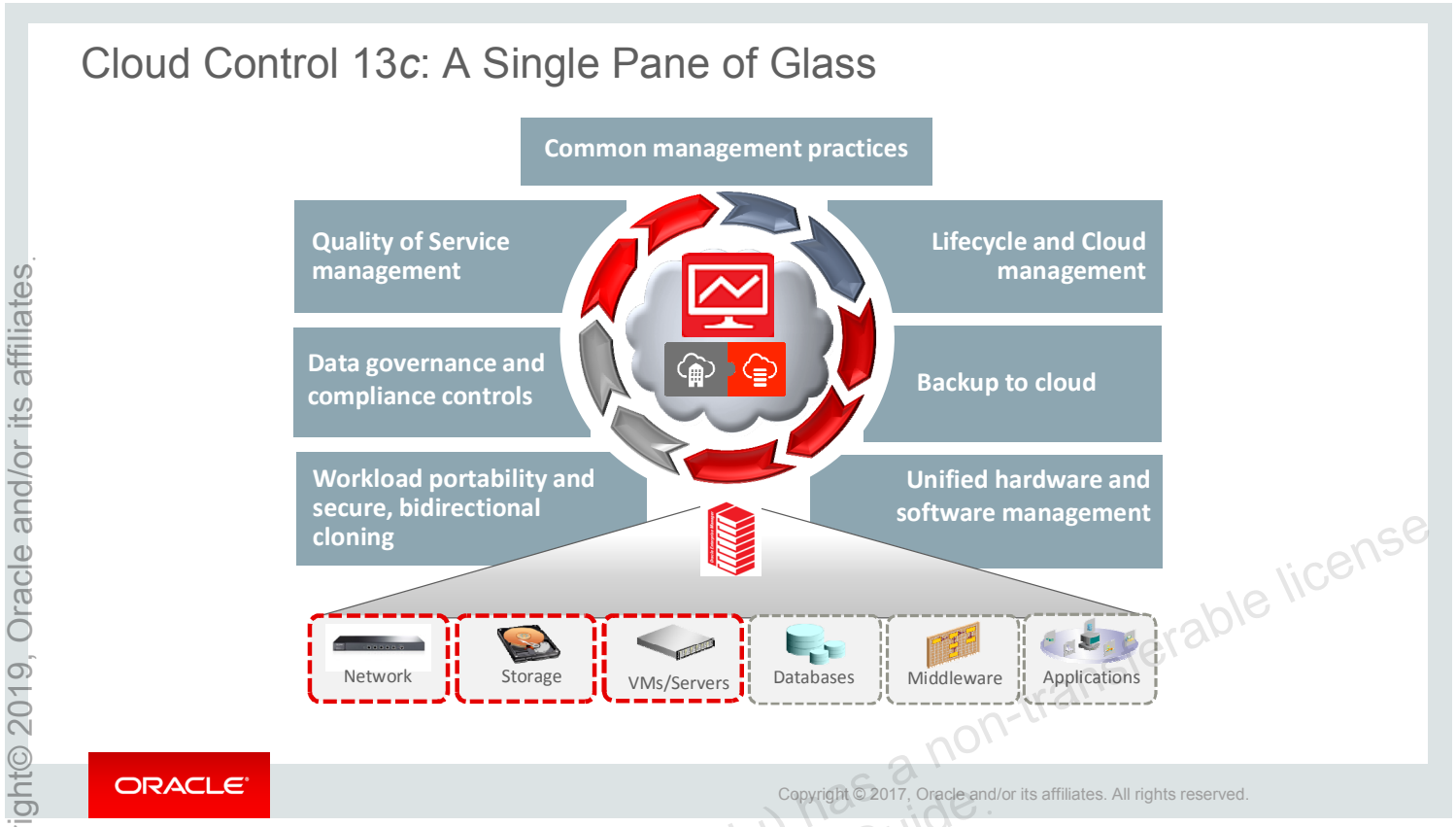


ORACLE

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 the 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 latest technologies while 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



One Management Tool to Oversee Them All

Enterprise Manager Cloud Control 13*c* has the capabilities to intelligently manage traditional and cloud-based services, thus 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-premise 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

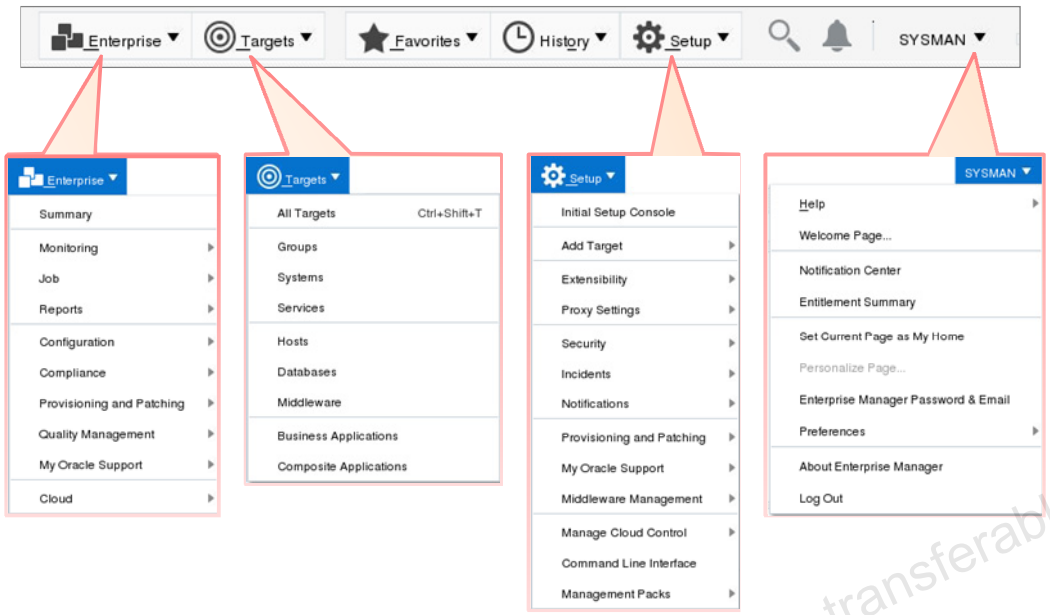
- Ability to back up to the cloud to leverage the Oracle Cloud capacity
- Hybrid cloud option to move workloads and clone targets between on-premise and Oracle Cloud

Cloud Control 13*c* Major Themes

Oracle Enterprise Manager Cloud Control 13*c* has been built around 11 major themes. Some of the key aspects of each theme are listed as follows:

- **Framework and Infrastructure:** Plug-in-based management of targets, named credentials, self-update, and jobs system
- **Enterprise Monitoring:** Status monitoring, and incident detection and notification
- **Application Management:** Built-in monitoring and management of Oracle applications
- **Database Management:** Provisioning and upgrade, data masking and subsetting
- **Middleware Management:** Discovery, monitoring, provisioning, and diagnostics
- **Hardware and Virtualization Management:** Monitoring of Oracle SUN hardware, monitoring and management of Oracle VM, Linux, UNIX, and Windows
- **Heterogeneous (Non-Oracle) Management:** Plug-ins and connectors for monitoring and managing non-Oracle applications and products
- **Cloud Management:** OVM server and server pool management, chargeback, reporting on usage and trends, and capacity planning and consolidation scenario analysis
- **Lifecycle Management:** Provisioning, configuration, patching, and compliance management
- **Application Performance Management:** User experience management, business transaction management, and Java monitoring and diagnostics
- **Application Quality Management:** Application replay and real application testing

Finding Your Way Around Cloud Control 13*c*



Four Main Menus

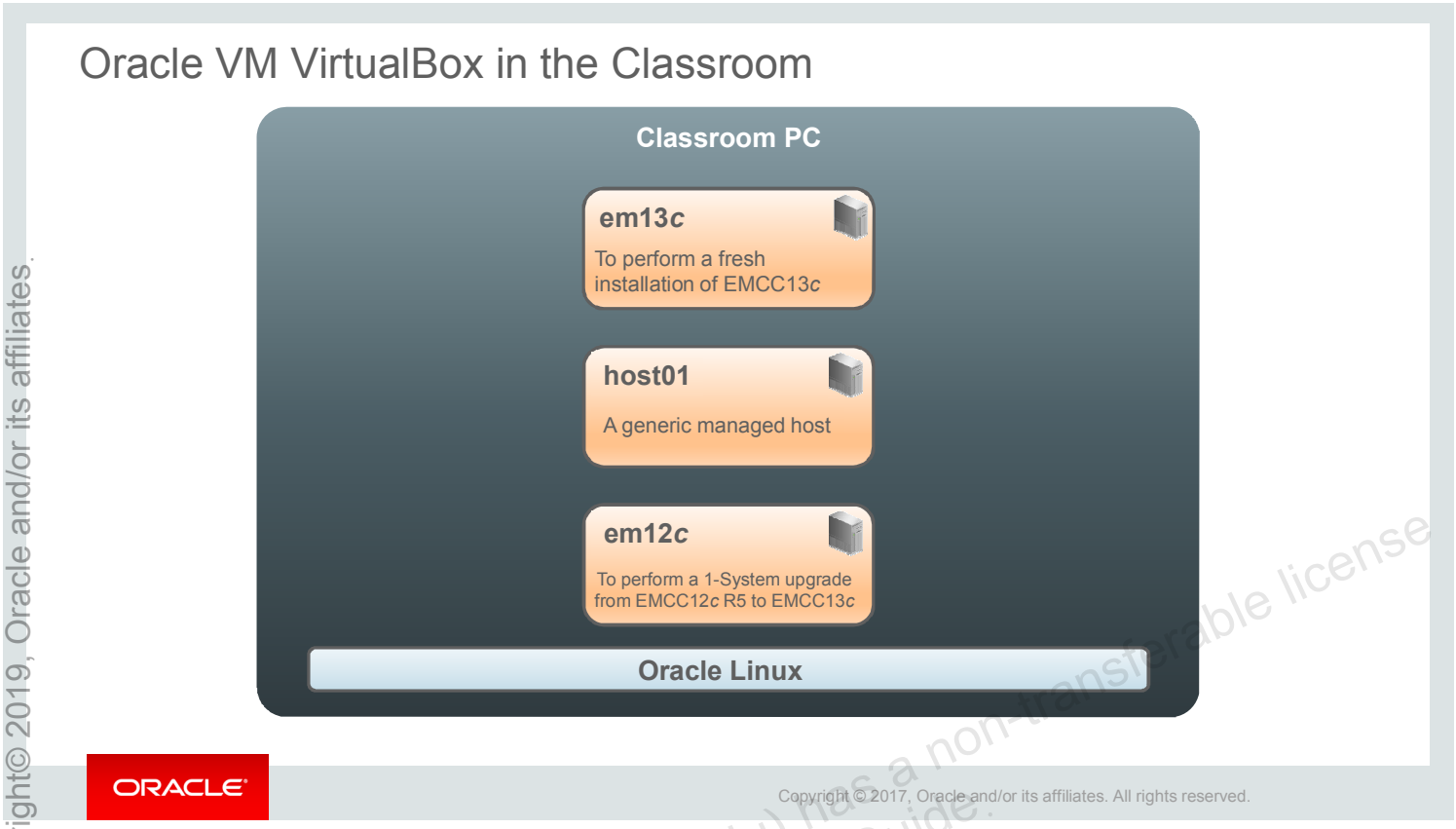
The main menu bar is displayed on every Enterprise Manager Cloud Control 13*c* page, and four of the menus within it are all you need to successfully navigate the Cloud Control 13*c* console:

- **Enterprise:** This menu allows you to navigate around the core framework of Cloud Control 13*c*, such as the summary of your managed IT infrastructure, monitoring and incident management, the job system, reporting, configuration and compliance management, provisioning, patching, and private cloud management.
- **Targets:** This menu gives you quick access to overviews of common types of managed elements such as hosts, databases, and middleware, as well as Cloud Control 13*c* artifacts such as groups, systems, and services. You can also view a filterable list of all your managed IT infrastructure.
- **Setup:** This menu is where you will spend much of your time administering Cloud Control 13*c* itself, including setting up users and privileges, connecting to My Oracle Support, using the self-update capabilities of Cloud Control 13*c*, and managing the components of Cloud Control 13*c*.
- **Logged-in User:** This menu (named for the currently logged-in user) is where users can set their preferences, such as their home page and accessibility settings, as well as view any notifications directed at them. This is also where the Log Out option is available.

This Course in Context

- **Oracle Enterprise Manager Cloud Control 13*c*: Install and Upgrade Workshop**
- Using Oracle Enterprise Manager Cloud Control 13*c*
- Oracle Enterprise Manager Cloud Control 13*c*: Advanced Configuration Workshop
- Oracle Enterprise Manager Cloud Control 12*c*: Cloud Management Workshop
- Oracle Enterprise Manager Cloud Control 12*c*: Overview Bundle: Self-Study Course
- Oracle Enterprise Manager Cloud Control 12*c*: Management Bundle: Self-Study Course

The courses listed here were available, or being developed, at the time that this course was released.



Self-Contained Multihost Environment

Your student machine is running Oracle VirtualBox on top of Oracle Linux. As illustrated, three virtual machines (VMs) have been prepared for you, and these are used as required to work through the practice activities:

- `em13c.example.com`
- `em12c.example.com`
- `host01.example.com`

The virtual machines that are running on your machine can communicate with one another, but only the base operating system can access the network outside the classroom PC.

Logging In to Your Machine

Log in to your classroom PC as the `vncuser` user. After you are logged in, the simplest way to control your guest virtual machines is by using the Oracle VM VirtualBox Manager GUI console.

Starting Your Guests

Your *Activity Guide* tells you which VMs are required to be running for each practice exercise. Use the VirtualBox Manager GUI console to start and stop the appropriate VMs.

Connecting to Guests and Running GUI Utilities

Use the GUI console presented by VirtualBox when the VM is running to interact with your VM. Take care, however, to use the VM's console and not the base operating system's console because they are all running Linux and are similar in appearance.

Viewing Webpages Served by Guests

You can use the browser in the VMs' GUI consoles to view webpages such as the Cloud Control Console. Alternatively, use the browser in the base operating system. Either way, enter a URL that refers to the VM host name, such as `https://em13c.example.com:7802/em`.

Summary

In this lesson, you should have learned how to:

- Identify the purpose of Cloud Control 13*c*
- List the major design themes of Cloud Control 13*c*
- Log in to your classroom PC
- Control the guest VMs on your classroom PC
- Log in to the guest VMs on your classroom PC
- Run GUI utilities on the guest VMs on your classroom PC

Practice 1-1 Overview: Using Oracle VM VirtualBox

This practice covers the following topics:

- Starting a VM
- Connecting to the VM's console

This practice familiarizes you with the Oracle VM VirtualBox environment that is installed on the student machine that you will use for all subsequent practices in the course.

Practice 1-2 Overview: Getting to Know the Cloud Control 13*c* Interface

This practice covers the following topics:

- Logging in to the Cloud Control 13*c* console
- Navigating around the Cloud Control 13*c* console
- Logging out of the Cloud Control 13*c* console

This practice familiarizes you with navigating around the Enterprise Manager Cloud Control 13*c* console.

2

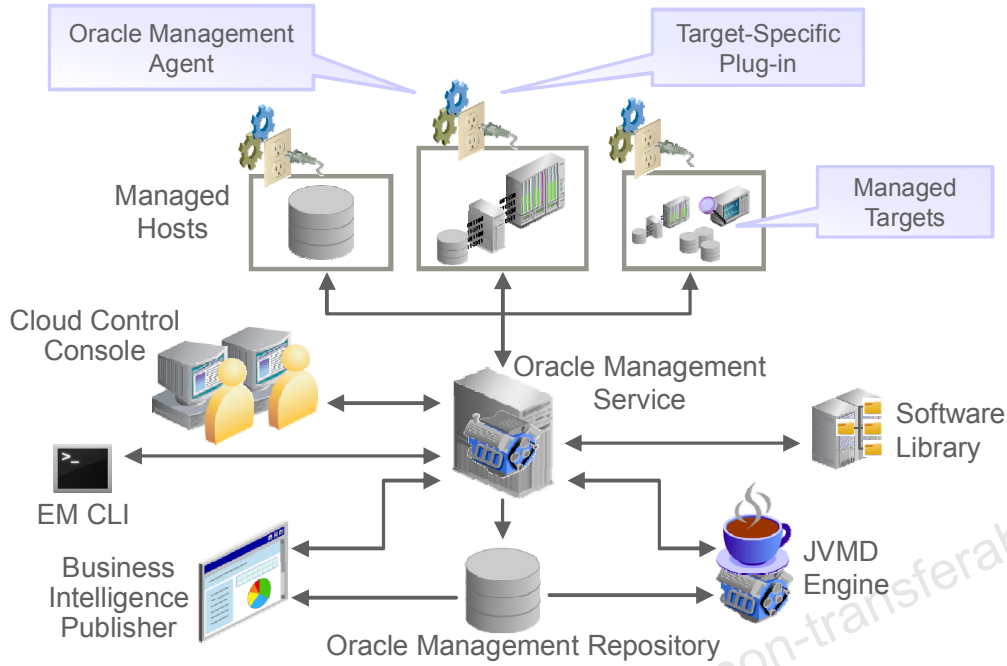
Architecture and Implementation Options

Objectives

After completing this lesson, you should be able to:

- Identify the main components of Cloud Control
- Use the Add-Host wizard to start managing hosts and their targets
- Describe implementation topologies at a high level
- Install Cloud Control in a simple single-server topology

Cloud Control Components

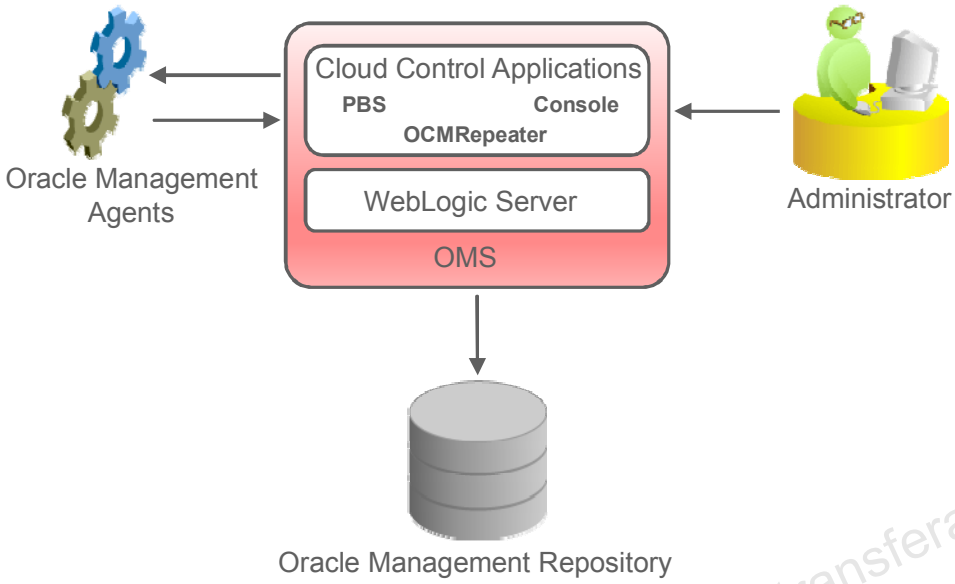


The Cloud Control ecosystem consists of the following main components as illustrated in this slide:

- Oracle Management Service (OMS)
- Oracle Management Repository (OMR)
- Managed hosts that form your IT infrastructure
- Managed targets that form your IT platforms, applications, and other non-host infrastructure
- Oracle Management Agents (simply called agents) running on managed hosts with target-specific plug-ins
- Software Library (on a shared storage location for highly available topologies) for storing patches, provisioning profiles, gold images, and so on
- Enterprise Manager Cloud Control Console, the web-based interface for Cloud Control
- Business Intelligence Publisher (BIP) for reporting
- Java Virtual Machine Diagnostics (JVMD) Engine for processing information gathered by JVM agents (not illustrated)

The Oracle Management Agent runs on hosts, gathering metric data about these hosts as well as using plug-ins to monitor availability, configuration, and performance, and to manage the targets running on the host. Agents communicate with the Oracle Management Service to upload the metric data collected by them and their plug-ins. In turn, the OMS stores the metric data in the Oracle Management Repository, where it can be accessed by the OMS for automated and manual reporting and monitoring. The OMS also communicates with the agents to orchestrate the management of their monitored targets. Along with coordinating with the agents, the OMS runs the Cloud Control Console webpages that are used by administrators and users to view reports, and monitor and manage the computing environment that is visible to Cloud Control via the agents and their plug-ins.

Oracle Management Service



As the illustration in the slide shows, the OMS is actually composed of J2EE applications deployed on Oracle WebLogic Server:

- The Console application serves up all the Cloud Control webpages.
- The Platform Background Services (PBS) application is where agents upload their metrics.
- OCMRepeater (Oracle Configuration Manager) is the link between Cloud Control and My Oracle Support for consolidating the configuration data that is collected from agents.

The OMS communicates with the agents deployed throughout the enterprise, receiving uploaded metric data from them and storing it in the Oracle Management Repository for future reference. The OMS also applies built-in and user-defined rules against received metrics to determine whether a condition exists that needs to be raised as an alert. There is also communication from the OMS to the agents, of instructions to execute against their monitored targets, as a result of either a job within the OMS or the actions of an administrator. Cloud Control administrators and users interact with the OMS via the Cloud Control Console webpages.

Oracle Management Repository

The Oracle Management Repository (OMR):

- Resides in an Enterprise Edition Oracle database
- Includes schema objects belonging to `SYSMAN`
- Is installed in a certified database instance that has been created before installation

The OMR is installed in an Enterprise Edition Oracle database as a group of approximately 4,000 schema objects belonging to the `SYSMAN` user that is stored in three tablespaces: `MGMT_ECM_DEPOT_TS`, `MGMT_TABLESPACE`, and `MGMT_AD4J_TS`. These schema objects contain information about Cloud Control users and administrators, the 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 database that you create before running the installer, and, for scalability requirements, it can be installed in a Real Application Clusters (RAC) database.

Regularly check the certification information on My Oracle Support for the most recent update about which database versions are certified for use as repositories.

Oracle Management Repository Best Practices

- Should be the only application schema present in the database
- Is recommended to be installed in a RAC database
  - For high availability
- Can be created by using predefined database templates
  - For saving time on installation

The database that is used to house the OMR should not be used for any other applications, including an RMAN catalog, for the following reasons:

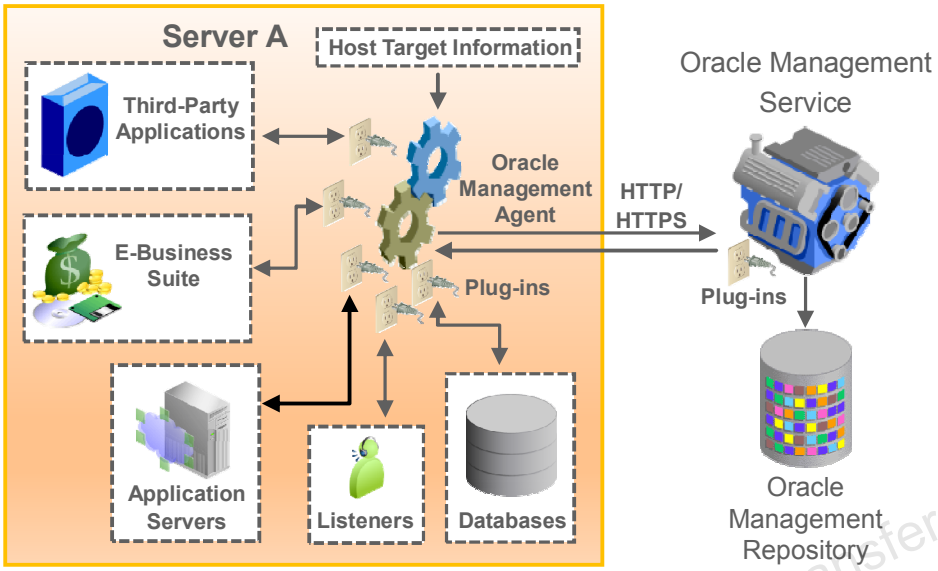
- Cloud Control's usage of the database should not have to compete with any other usage.
- Using the OMR database for other applications may restrict your ability to upgrade and patch the OMR schema and database as required.
- Cloud Control comes with a restricted-use, single-instance database license that can be used for the OMR only.

Information about the restricted-use license is detailed in the documentation set in *Oracle Enterprise Manager Licensing Information*.

RAC databases are recommended for hosting the OMR due to their high availability capabilities.

The OMR can be preconfigured in an Oracle database by using predefined database templates. In this case, a software-only installation of the database software is performed first, and then the Database Configuration Assistant (DBCA) is used to create the OMR database from one of the predefined templates.

Oracle Management Agent



The Oracle Management Agent is a Java application that runs on a host, gathering metric data about the host environment as well as using plug-ins to discover, monitor, and manage targets that are running on that host. The plug-ins gather configuration information from their targets, monitor their availability and performance, and manage those targets as directed by the OMS.

A target is any software or system for which there is a plug-in. The list of targets includes entities such as Oracle Database, Oracle Database Listener, Oracle Application Server and Oracle WebLogic Server, E-Business Suite, SOA, Exadata, and Exalogic. Using the Oracle Enterprise Manager Extensibility Framework, plug-ins can be developed by third party software vendors to monitor and manage their products, and even by individual organizations to monitor and manage in-house built applications. Only one agent is required on a host to be able to monitor and manage all the targets running on that host.

Each agent plug-in is specific to a particular target type and offers special management capabilities that are customized to suit that target type. To discover, monitor, and manage any given target, the agent must have the appropriate plug-in installed. Plug-ins only need to be installed on agents where they are required to monitor and manage their target type.

Most plug-ins have components that reside in both the agent and the OMS. The OMS plug-in determines the management options and behavior exposed through the Cloud Control Console. The Oracle Database, Oracle Fusion Middleware, and Systems Infrastructure plug-ins are installed in the OMS by default, and other plug-ins can be installed if required. Plug-ins are added to the agent as relevant targets are discovered. Plug-ins can be updated independently of the agent and other plug-ins, thus allowing for simplified maintenance to add improvements and corrections, and to align with new versions of the target.

An *agent plug-in* (also referred to as *a target plug-in*) contains two types of components:

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

The *discovery* content is deployed on a host:

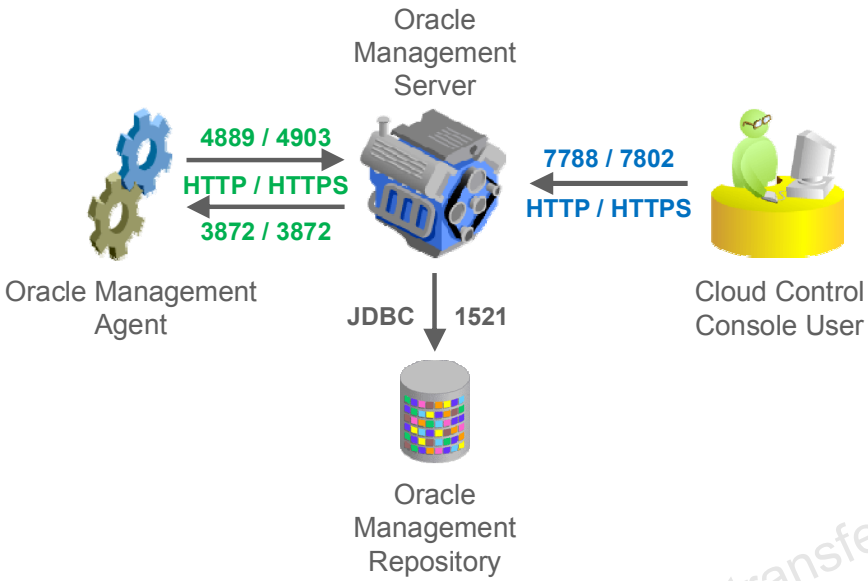
- When the agent is pushed to or installed on that host, for the default plug-ins
- When a new plug-in is deployed to the agent

The *management* content for each target type is pushed to the agent when the administrator promotes a discovered target to a managed target.

The agent communicates, via clear HTTP or secured HTTPS traffic, with the Oracle Management Service to upload metric data collected by it and its plug-ins and to receive instructions from the OMS.

Agents are installed in their own `ORACLE_HOME` as an instance of a shared binary `ORACLE_HOME`, although typically there is a one-to-one mapping of an agent instance to agent binaries (unless you are using a shared NFS-mounted agent binaries location).

Communication Flow Between Components



* Port numbers are examples only.

The communication flow between the Cloud Control components is illustrated in the slide by using directional arrows to indicate the initiator of the communication. All the ports shown are example values that can be changed during installation, either by the installer as it searches for available ports or explicitly by you. You can also change ports after installation.

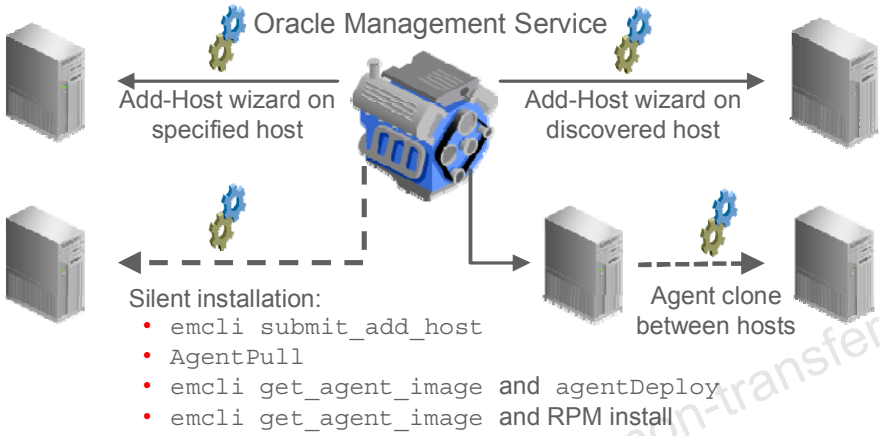
- The agent uploads data to the OMS via HTTP on a port in the range 4889–4898 or via HTTPS on port 1159 or a port in the range 4899–4908.
- The OMS communicates with the agent via HTTP or HTTPS, depending on whether the agent is unsecured or secured, respectively, on port 3872 or a port in the range 1830–1849.
- The OMS communicates with the OMR via JDBC on port 1521.
- Cloud Control Console users access the Cloud Control webpages via HTTPS on a port in the range 7799–7809 or via HTTP on a port in the range 7788–7798.

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, because communication will need to be allowed on these ports and in the directions shown.

Oracle Management Agent Deployments

Choice of agent image formats when not cloning:

- Agent software bundle from the software library
- Gold Agent Image built from an existing agent



A *managed host* is a host where an EM agent is up and running. It is recognized in the EM Console as a *host* target. When an agent exists on a host, other *targets* can be discovered on it (such as databases, listeners, and so on).

An *unmanaged host* is one that does not yet have an agent running on it.

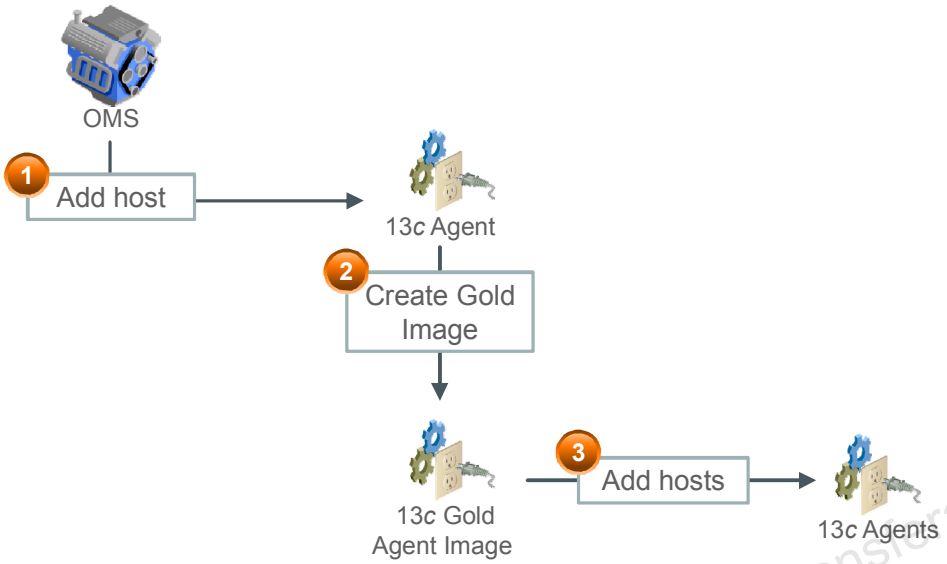
To transform an unmanaged host into a managed host, the OMS connects to the host via a secure shell (SSH) connection by using the authentication credentials supplied by you. The agent image can be sent in a compressed form that is then uncompressed and installed into directories that you nominate when initiating the Add-Host job, or it can be sent as a Gold Image built from an existing agent on the same platform as the unmanaged host. The agent can be deployed by using the console pages to hosts that are:

- Discovered automatically by Cloud Control but are still unmanaged hosts
- Known to the administrator as hosts on the network but not yet known to Cloud Control

You can also clone an agent from one host to one or more other hosts of the same operating system. Both the cloning and Gold Agent Image methods copy not just the software but the configuration of the agent, including any patches. This is typically done to define a standard agent configuration and deploy it to multiple hosts. Gold Agent Images offer the advantage of managing the life cycle of the subscribed agents beyond the initial installation. They allow you to focus on ensuring that the original agent's configuration, patches, and plug-ins are up-to-date, leaving you comfortable in the knowledge that you can easily reflect those changes in other agents.

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

Agent Installation Best Practice: Gold Agent Images



A Golden Best Practice

Although you could use the Add-Host wizard to manually deploy all of your 13*c* agents, taking advantage of Cloud Control 13*c*'s Gold Agent Image functionality provides benefits beyond the point of installation itself. By subscribing your agents to a Gold Agent Image, keeping your agents updated is vastly simplified, thereby helping to ensure currency and compliance across your Enterprise Manager site.

Using a Gold Agent Image to install your agents to 13*c* is a multistep process:

- Install at least one 13*c* agent by using the manual Add-Host wizard.
- Create a Gold Agent Image by using the newly installed agent as the source.
- Mark the Gold Agent Image as the current version.
- Add hosts by using the current version of the Gold Agent Image.

Every host you add by using the Gold Agent Image becomes a subscriber to that image, and from that point onwards you can create new versions of the Gold Agent Image and use them to update subscribers.

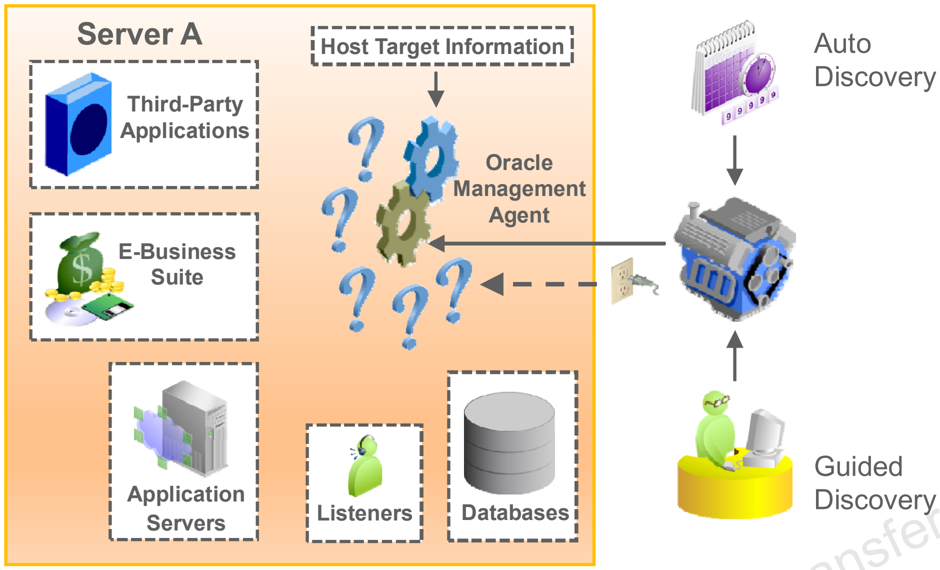
Host and Target Discovery Mechanism

- Host discovery
  - Automatic
    - IP Scan
  - Manual
    - Installing an agent to convert to a managed host
- Target discovery
  - After an agent is installed
  - Automatic
    - Discovered automatically
    - Promoted manually to a managed target
  - On-demand
    - Added manually

Hosts in your system can be discovered by a special agent (usually the Central Agent, which is installed with the primary OMS) that is tasked with scanning the entire network based on the IP address ranges that you specify. The result of this IP scan is a list of unmanaged hosts, services running on them, and the ports in use. To convert any of these hosts to managed hosts, you must deploy agents to them. After an agent is deployed to the host, the components that are running on the host can be discovered and reported as potential targets. These components can then be promoted to managed target status, thus enabling them to be managed and monitored by Cloud Control.

Hosts can also be manually discovered by simply specifying a host name/IP address and installing agents on them.

Target Discovery



ORACLE

After an agent has been installed on a host, it needs to look for targets that it can manage. As a Cloud Control administrator, you can guide this process by using the Cloud Control Console Add Non-Host Target wizard. Guided discovery allows you to nominate a family of target types to search for, such as databases and listeners, and the agents where you want the search to be executed. When any new targets are discovered, the appropriate plug-in is pushed from the OMS. If required, the target is recorded in the OMR, and monitoring commences.

You can also configure auto discovery to run at regular intervals and get agents to search for known target types unattended, allowing you to review the results at a later stage and promote the discovered targets to become managed targets.

Key Differences Between 13*c* and Earlier Versions

- Next generation installer
- Redesigned user interface that is cleaner and mobile friendly
- Shared Oracle Home for middleware and OMS
- BI Publisher
  - Automatically configured in 13*c* for every installation, upgrade, and HA expansion. 12*c* required separate configuration.
  - In HA topologies, the OMS, BI Publisher, or both can be running on each node.
- Java Virtual Machine Diagnostics (JVMD) Engine automatically deployed on every OMS
- Larger installation footprint

Rather than distribute the installation media in the traditional directory structure, Enterprise Manager Cloud Control 13*c* employs the next generation installer delivery method of a self extractor, meaning that you need to download only a handful of files before commencing installation.

The user interface of Enterprise Manager Cloud Control 13*c* has been redesigned to have a cleaner visual appearance that is friendlier to mobile and tablet devices.

Previously, the OMS home directory was a child directory of the middleware home, but in 13*c,* the two Oracle Homes have been merged into one.

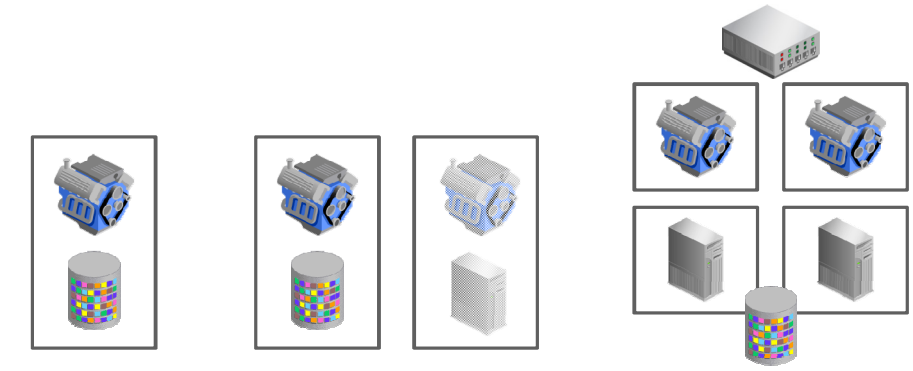
BI Publisher is now configured as well as installed alongside the OMS whenever you install, upgrade, or HA expand your OMS nodes. This means that you need to only set up BIP security to enable end users to use BIP reports. Furthermore, in HA topologies, you have the option of running the OMS, BIP, or both on each HA node.

In Enterprise Manager Cloud Control 12*c,* the Java Virtual Machine Diagnostics (JVMD) Engine had to be manually deployed to the OMS nodes. In Cloud Control 13*c*, the JVMD Engine is deployed to every OMS alongside the default Fusion Middleware Plug-in. However, JVMD agents still need to be manually deployed to the targets.

The OMS now requires at least 10 GB RAM and 24 GB storage to accommodate BIP and the JVMD engine.

Implementation Options

Cloud Control can be implemented in a variety of topologies to suit all enterprise sizes and availability requirements, as shown in the following examples:



One Size Does Not Fit All

Consideration should be given to several criteria when deciding how and where to deploy Enterprise Manager Cloud Control 12*c*.

Single-Server Deployment

This is the simplest topology in which all components are installed on the same server.

Advantages:

- Simple installation
- Ease of maintenance

Disadvantages:

- It can scale only within the limitations of the server resources.
- The server becomes a single point of failure.

Multi-Server Deployment

The OMS and the OMR can be separated onto their own servers, and in turn, can both be installed in multi-server topologies. Such topologies would be fronted by load balancers in active-passive or active-active modes, and physically co-located or geographically distributed. The OMR can use the Data Guard technology to replicate data between sites.

Examples of such topologies include:

- Multiple OMS servers fronted by a load balancer for scalability and availability of the Cloud Control application
- Multiple OMS servers fronted by a load balancer with a RAC OMR for scalability and availability end to end
- Multiple OMS servers that are geographically distributed and fronted by multiple load balancers with a Data Guard–enabled OMR for maximum availability

Advantages:

- High to maximum availability
- No single point of failure
- Possibility of Cloud Control maintenance without an outage
- Easy relocation of both tiers because virtual host names are used to front the OMS and the OMR

Disadvantages:

- Cost and maintenance of extra hardware
- Complex topology that may impede troubleshooting
- Complex topology that would require careful planning and phased rollout

Deployment planning is covered in greater detail in the lesson titled “Implementation Planning.”

Single-Server Installation Process

1. Read the documentation and release notes.
2. Check hardware and software compliance with prerequisites.
3. Prepare the database for the OMR.
4. Run the installer and select Simple or Advanced installation.
5. Execute any post-installation steps.

Prevention Is Better Than a Cure

Before installing any software, it is important to read the release notes and installation guide to become familiar with the full process, taking care to note and check compliance with prerequisites, as well as performing any post-installation steps that may be required. Anecdotal evidence from Oracle Support suggests that many Oracle Enterprise Manager Cloud Control installation attempts ended unhappily because one or more prerequisites were not met.

Prerequisite Checks

The documentation lists comprehensive requirements for the system on which Cloud Control is to be installed, including:

- Hardware and operating system requirements
- Operating system groups and users, and their setup
- Networking requirements
- Certified Oracle Database versions for the Management Repository

Preparing Your Oracle Database for the OMR

If you have not used an Oracle-provided DBCA template for your repository, the Cloud Control distribution includes a command-line utility, EM Prerequisite Kit (emprereqkit), which you can run against the database that you intend to use as a repository.

emprereqkit makes recommendations, if necessary, and can also make some configuration changes to the database for you. It can also be used to reverse some of the changes after installation if they were only temporary installation requirements.

Running the Installer in GUI Mode

Start the installer process, select Simple or Advanced installation, and enter information as required. Keeping a record of the values entered on each screen for future reference is easier than examining logs after installation. Some administrators go one step further by taking screenshots of each installer screen before moving to the next step. You will need to make some decisions during the installation process:

- **Host Name**

  To ensure that the OMS installation is best prepared to support active/passive disaster recovery, provide an alias host name. The OMS and central agent installations will be configured with this alias host name, thus enabling the OMS software to run on a configured host at the primary or standby site. This input parameter should not be the application virtual host name that is used with a load balancer—that configuration is achieved with a post-installation configuration operation.

- **Deployment Size**

  In an Advanced installation, you nominate a deployment size to use for building the repository. This indicates the number of targets, Management Agents, and concurrent user sessions that you plan to have. When using a repository that is built with an Enterprise Manager Cloud Control DBCA template, your selection should match the template size. The installer provides three choices:
  - **Small:** To monitor up to 999 targets, with up to 99 Management Agents and up to 10 concurrent user sessions
  - **Medium:** To monitor about 1,000 to 9,999 targets, with about 100 to 999 Management Agents and about 10 to 24 concurrent user sessions
  - **Large:** To monitor 10,000 or more targets, with 1,000 or more Management Agents and about 25 to 50 concurrent user sessions

- **Central Agent Base Directory**

  Nominate a directory for the central agent that is outside the middleware home. This allows the central agent to be patched and upgraded independently like any other management agent.

- **Software Library**

  Ideally, you designate the Software Library location to be a shared file system that can be mounted on other hosts that will run additional OMSes. If a local file system is chosen, it is recommended that it be outside of the middleware home. The installer provides a default location during the installation process.

- **BI Publisher**

  Choose whether BI Publisher will be enabled alongside this OMS, and a shared location for HA topologies.

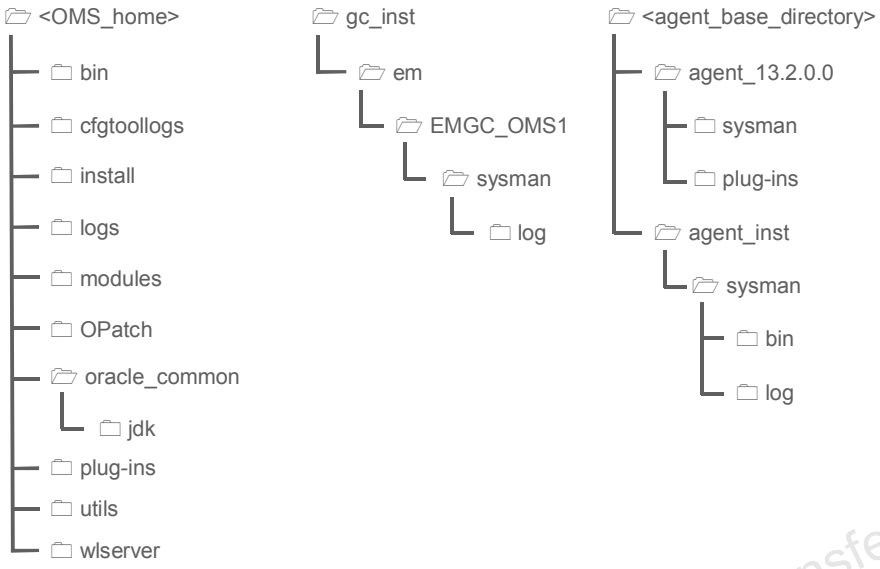
Running the Installer in Silent Mode

You can run the installer without the GUI by providing all the requisite information in a response file. Extract the response file template, `new_install.rsp`, by executing the installer with the `getResponseFileTemplates` and `outputLoc` switches, for example, on Linux x86-64: `em_linux64.bin -getResponseFileTemplates -outputLoc /tmp`.

Executing Post-Installation Steps

Be sure to execute any post-installation steps, either as directed by the installer or as described in the documentation and release notes. If not specified, you should always back up the initial configuration of the OMS by using the `emctl exportconfig oms` command as well as back up `$ORACLE_HOME/sysman/config/emkey.ora` that is the key used to encrypt all sensitive information in the repository.

Installation Directories



* Only a selection of directories are shown here.

Some of the installation directories are illustrated in the slide. The OMS Instance Base location (`gc_inst`) is at the same level as the OMS middleware home and it contains all OMS configuration details. In Advanced Installation mode, this location can be customized.

The installation log files are located in:

`<oraInstLoc>/oraInventory/logs` and `<middleware_home>/cfgtoollogs/oui`

The configuration log files are in various locations:

`<OMS_home>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log`

`<OMS_home>/cfgtoollogs/cfgfw/*`

`<agent_base_directory>/agent_13.2.0.0.0/cfgtoollogs/cfgfw/*`

The component-specific logs are in the following locations:

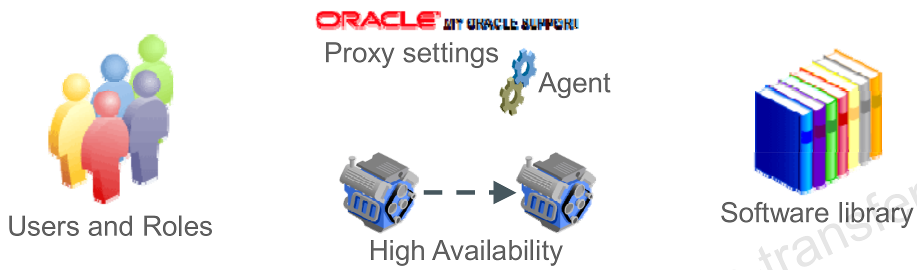
`<OMS_home>/cfgtoollogs/omsca/*` for the OMS Configuration Assistant

`<OMS_home>/cfgtoollogs/pluginca/*` for the Plug-in Configuration Assistant

`<OMS_home>/sysman/log/schemamanger/latest/*` for the Repository Configuration Assistant

Initial Setup Console

- All essential setup tasks are gathered in one place.
- It is accessible only by super administrators.
- The setup tasks are presented on a dashboard interface.
- Each task is marked as pending, completed, or ignored.
- Some tasks can be completed directly on the console.



Every Journey Starts with the First Step

The Initial Setup Console is a convenient agglomeration of basic setup tasks that would otherwise need to be accessed via their individual menu navigation paths. Some of the tasks can be completed directly in the Initial Setup Console, whereas the others have links to the appropriate pages in Enterprise Manager Cloud Control 13*c*. Tasks are flagged with one of three states–Pending if they are yet to be completed, Completed after you have undertaken the task, and Ignored if you choose to flag the task as unnecessary for your site.

The tasks that are gathered in the Initial Setup Console are considered to be the fundamental steps in setting up your Enterprise Manager Cloud Control site. They include the following:

- Software library: Add upload file locations (usually at least one is added during installation).
- OMS Agent proxy setting: Define a proxy to sit between the OMS and the agents.
- My Oracle Support proxy setting
- OMS addition for high availability topologies
- Mail server configuration for outgoing email notifications
- My Oracle Support credentials setup
- Roles and users creation

Starting and Stopping Cloud Control 13*c*

- Start, stop, and check the status of the OMS with `emctl`.

```
$OMS_HOME/bin/emctl start oms
$OMS_HOME/bin/emctl stop oms [-all][-force]
$OMS_HOME/bin/emctl status oms [-details]
```

- Start, stop, and check the status of an agent with `emctl`.

```
$AGENT_INST_HOME/bin/emctl start|stop|status agent
```

- Start and stop BIP only.

```
$OMS_HOME/bin/emctl start oms -bip_only
$OMS_HOME/bin/emctl stop oms -bip_only
```


Enterprise Manager Control

Enterprise Manager Control (`emctl`) is used to control the OMS and all the agents, although it must be invoked from the appropriate directory to be able to control the desired component.

OMS Log Files

Log files for the OMS are primarily in the following locations:

- `gc_inst/em/EMGC_OMS1/sysman/log`
- `gc_inst/user_projects/domains/GCDomain/servers/EMGC_OMS1/sysman/log`
- `gc_inst/user_projects/domains/GCDomain/servers/EMGC_OMS1/logs`

Agent Log Files

Log files for the central agent (the agent installed on the OMS server) are in the following location:

- `<agent_base_directory>/agent_inst/sysman/log`

Quiz

How will you prepare for installing Enterprise Manager Cloud Control 13*c*? (Select all that apply.)

a. Getting comfortable at your desk
b. Reading the installation documentation and release notes
c. Making a cup of tea
d. Ensuring that your environment meets all prerequisites
e. Doing nothing. You don't need to prepare. What could possibly go wrong?

Answer: b, d

Although it is important to be relaxed and well hydrated, it is vital that you are familiar with the installation process before embarking on the installation of Enterprise Manager Cloud Control 13*c*. This includes checking the environment where you propose to install Enterprise Manager Cloud Control 13*c* against all documented prerequisites and addressing any deficiencies that are found before starting the installation.

Practice 2-1 Overview: Installing Cloud Control in a Single-Server Topology

This practice covers the following topics:

- Checking system prerequisites
- Creating a database instance for the OMR
- Installing Oracle Enterprise Manager Cloud Control 13*c*
- Cloud Control Console first-time login
- Applying Daylight Saving Time (DST) patches

In this practice, you install a database instance to be used for the OMR. You then install Oracle Enterprise Manager Cloud Control 13*c* onto the same server as the OMR instance. You log in to the Cloud Control Console before applying Daylight Saving Time (DST) patches to the OMR and OMS.

Practice 2-2 Overview: Using the Initial Setup Console

This practice covers creating a user through the Initial Setup Console.

In this practice, you create a user by using the Initial Setup Console.

Practice 2-3 Overview: Adding Managed Hosts

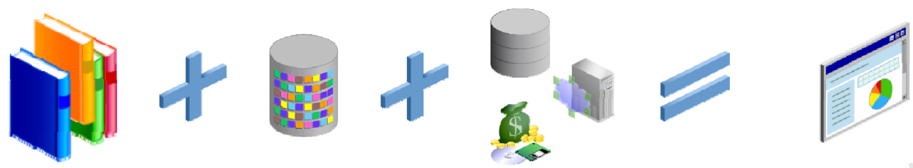
This practice covers the following topics:

- Using the Add-Host wizard
- Discovering targets on a host
- Creating a Gold Agent Image
- Adding a host with a Gold Agent Image

In this practice, you add a managed host to your Cloud Control 13*c* site by using the Add-Host wizard, and then discover targets to be managed on that host. Next you create a Gold Agent Image from the host that you just added, and use that image to add another host to your Cloud Control 13*c* site.

BI Publisher

- Always installed with the OMS
- Enterprise quality reporting solution
- Out-of-the-box catalog of reports
- Report builder that allows for full customization
- Honoring of Cloud Control users' target privileges
- Security model for full separation of duties

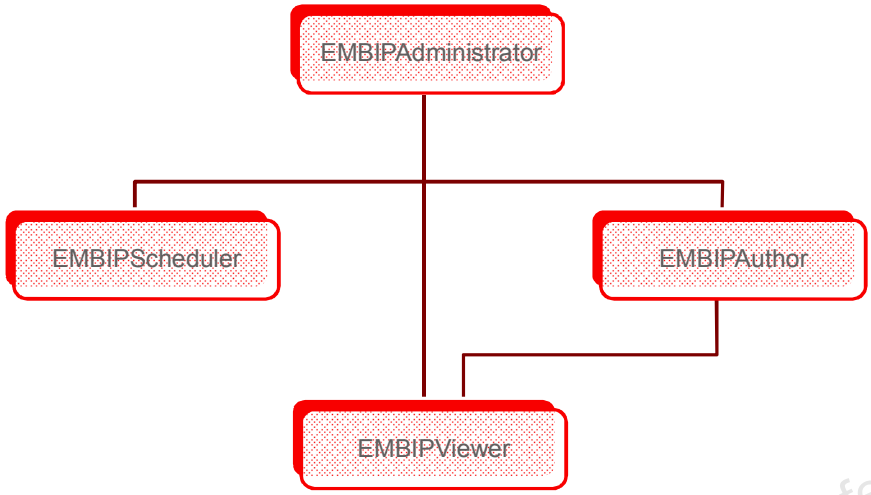


Built-In Enterprise Reporting

Every installation of Enterprise Manager Cloud Control 13*c* includes BI Publisher as the preferred reporting tool. Configured and ready to use out of the box with a built-in catalog of reports, BI Publisher is a product that provides a mature and flexible reporting environment. Using BI Publisher's report wizard and the preconfigured OMR data source, you can create a multitude of reports to satisfy your end-users' needs, who can in turn be safe in the knowledge that they can report only on targets on which they have view privileges.

In high availability topologies, BI Publisher can be configured to run on every node or only on some nodes, alongside or separated from the OMS.

The BI Publisher Security Model



The BI Publisher security model for Enterprise Manager Cloud Control consists of four roles that are arranged in a hierarchy that can be assigned to Cloud Control administrators through the Enterprise Manager Command Line Interface (EM CLI):

- **EMBIPViewer:** Granting this role to Cloud Control users will allow them to log in to BI Publisher and run reports.
- **EMBIPAuthor:** Granting this role to Cloud Control users will allow them to log in to BI Publisher and create reports. This role also includes the EMBIPViewer role.
- **EMBIPScheduler:** Granting this role to Cloud Control users will allow them to schedule reports. However, they will also need the EMBIPViewer role to view the reports that are to be scheduled.
- **EMBIPAdministrator:** Granting this role to Cloud Control users will allow them to log in to BI Publisher and administer folder and report privileges, create new folders for shared reports, and perform other BI Publisher administrative tasks. This role also includes the EMBIPAuthor, EMBIPViewer, and EMBIPScheduler roles.

Practice 2-4 Overview: Setting Up BI Publisher Security

This practice covers granting BI Publisher privileges to Cloud Control users.

In this practice, you grant BI Publisher privileges to a Cloud Control user by using the Enterprise Manager Command Line Interface (EMCLI).

Summary

In this lesson, you should have learned how to:

- Describe the main components of Cloud Control and their relationship with one another
- Install an agent on a host and discover targets on that host
- Differentiate between the available topologies
- Install Cloud Control in a simple single-server topology

3

Oracle Cloud in Your IT Ecosystem

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 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 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 13*c* 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.

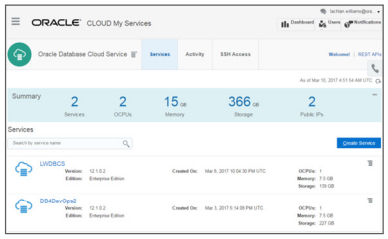
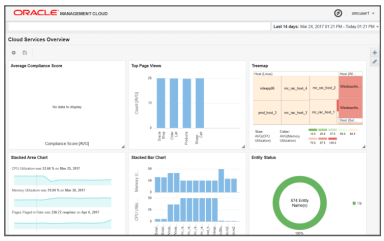
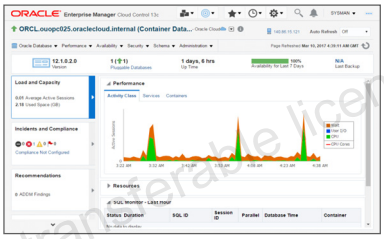
At the time of writing, the following services were supported by Hybrid Cloud:

- 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 web pages
  - 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

Tools for Every Need

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

- **Oracle Cloud service web pages:** 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

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 13*c*: 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

ORACLE

Apply What You Already Know

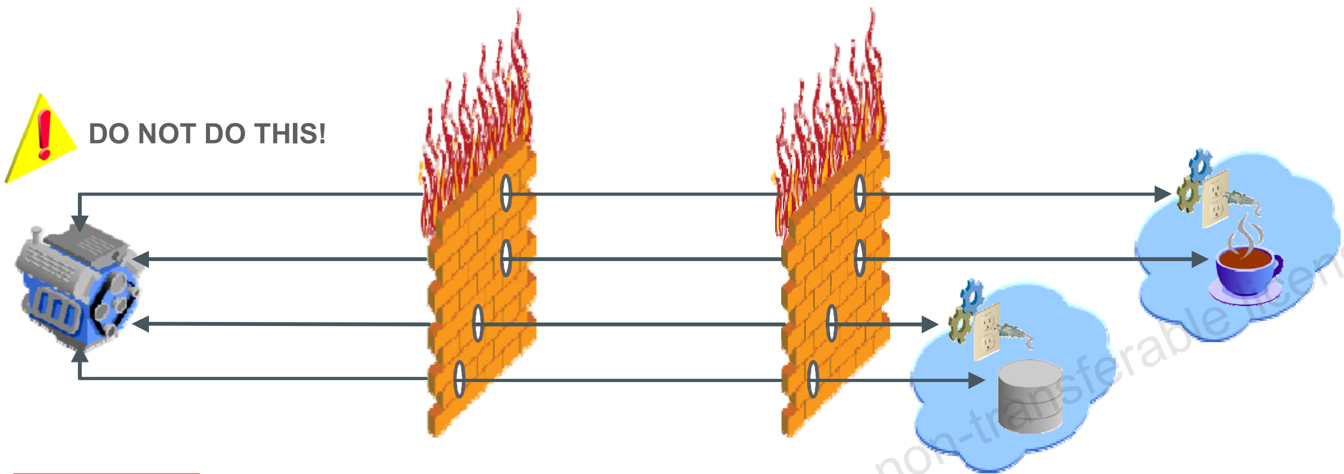
The Enterprise Manager Cloud Control infrastructure that you use to monitor and manage your on-premises targets is used to monitor and manage your Oracle Cloud targets, so you already know how to turn your Oracle Cloud service virtual machines (VMs) into managed hosts, and then discover your service instances. It is simply a matter of installing the Cloud Control agent on your Compute, Database, or Java Cloud Service virtual machine, and then discovering the manageable targets that are running on those VMs.

After they are discovered, you can monitor and manage your Oracle Cloud targets in the same way as the on-premises targets. The only caveat to this is when it comes to patching—when you are given the responsibility to patch your Oracle Cloud VMs, database and Java service instances should be patched only through the relevant Oracle Cloud Service Console.

Additionally, if you have installed Enterprise Manager Cloud Control 13.2 Plug-ins Update 1 (released in March 2017), you also have the option to discover your Oracle Cloud services directly by using the Oracle Cloud REST APIs. The same APIs are then used to expose the Oracle Cloud console functions within Enterprise Manager Cloud Control.

How to Get Past the Firewalls That Protect You?

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

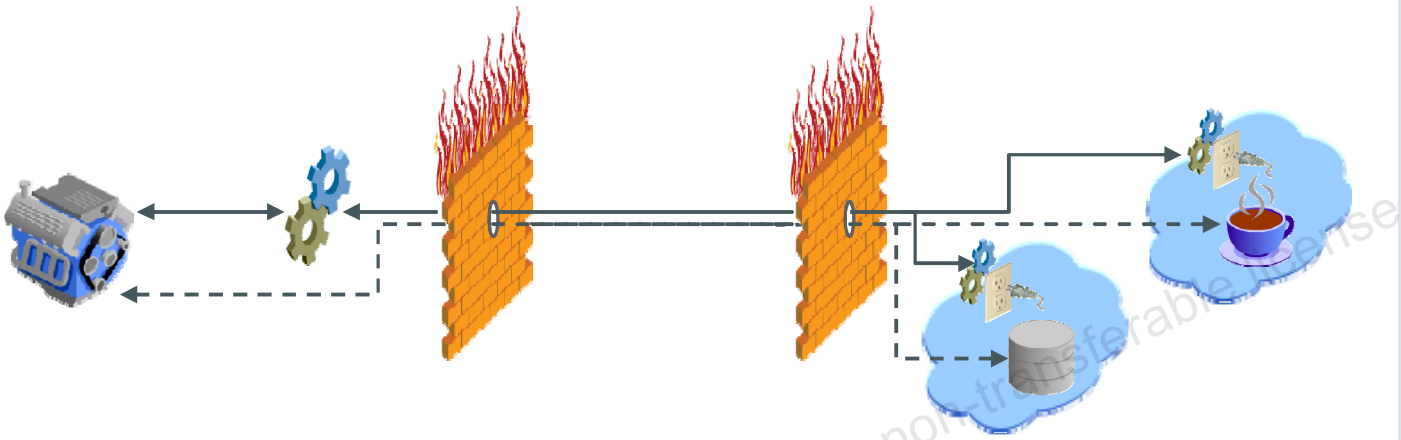


It's a Firewall, Not Swiss Cheese

Firewalls are prohibitive by design, so they block traffic coming in or going out unless configured otherwise. This poses a problem for a monitoring and management tool such as Enterprise Manager Cloud Control that needs access between the OMS and agents and between the OMS and targets. Although you could configure your firewalls to allow all traffic in and out between your on-premises OMS and Oracle Cloud host agents and targets, this may leave your firewalls full of holes that defeat their primary purpose of preventing unwanted and unnecessary traffic.

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



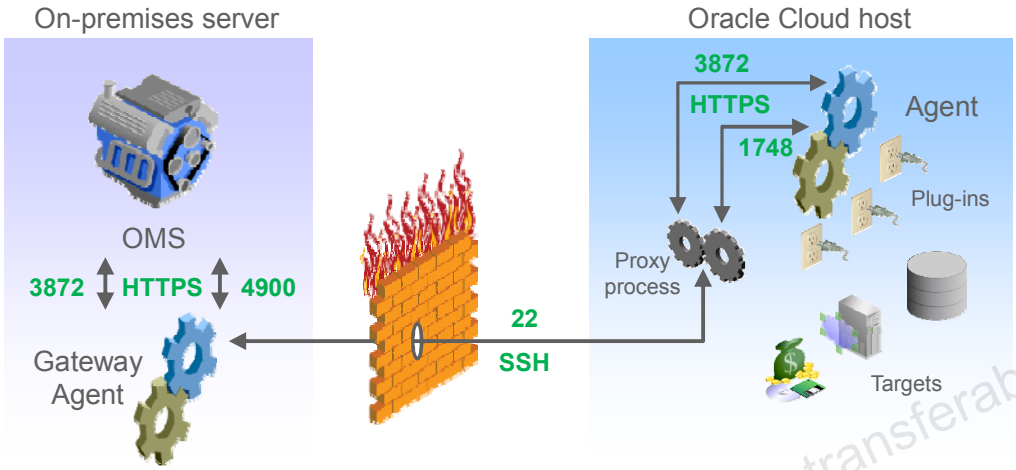
One Tunnel for All Traffic

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

- The OMS and cloud agents are protected from direct communication.



ORACLE

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 the OMS, it does so via a local proxy process which, in turn, communicates via the SSH tunnel with an on-premise 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.

Doing More with the Same

Having deployed a hybrid cloud agent to your Oracle Cloud VM, you can start taking advantage of the benefits that come from managing your on-premises and Oracle Cloud environments with the same tool.

The primary benefit of using Enterprise Manager Cloud Control to manage your combined on-premises and Oracle Cloud ecosystem is the ability to easily transfer database and middleware instances between your on-premises hosts and your Oracle Cloud services. Commonly referred to as “lift and shift,” this allows you to easily move database or middleware load from your on-premises environments to Oracle Cloud services. Lift and shift can be used for other purposes too, such as developing locally and deploying to the cloud, or setting up a test-master database in your on-premises environment and using it to refresh test instances in the cloud.

Summary

In this lesson, you should have learned how to:

- Describe the benefits of using Enterprise Manager Cloud Control to manage Oracle Cloud service instances
- Explain how Enterprise Manager Cloud Control manages Oracle Cloud service instances

4

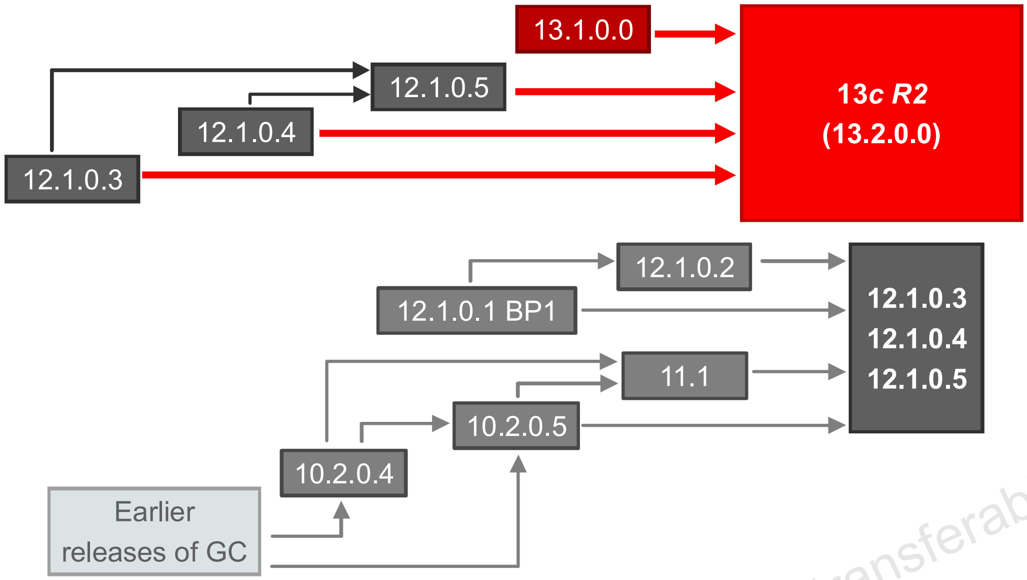
Upgrade Paths

Objectives

After completing this lesson, you should be able to:

- Describe the upgrade paths that can be used when upgrading from earlier releases
- Describe the 1-System upgrade process

Upgrade Paths



Good Planning Results in Successful Upgrades

Before starting an upgrade to Enterprise Manager Cloud Control 13*c* R2 from an earlier version of Grid Control or Cloud Control, consider your starting point, because this will determine the upgrade path that you will select.

As illustrated in the slide, you can upgrade directly from Enterprise Manager Cloud Control 13*c* R1 or the 12*c* versions 12.1.0.3, 12.1.0.4, or 12.1.0.5. If you are currently running an earlier version of Cloud Control 12*c*, you first need to upgrade to one of the three upgradeable versions.

It is possible to upgrade from Enterprise Manager 11*g* Grid Control version 11.1 or from Enterprise Manager 10*g* Grid Control version 10.2.0.5 by first upgrading to an upgradeable version of Cloud Control 12*c*. If you are currently running an earlier version of Grid Control, you first need to upgrade to 10.2.0.5 or 11.1. All these upgrade paths involve one or more updates through the intervening versions between your starting point and an upgradeable version of Cloud Control 12*c*, including upgrading your OMR repository to a version of the database that is supported with 12*c*.

12*c* to 13*c* Upgrade Utilities

- Oracle Universal Installer (OUI)
  - Upgrade the OMS and OMR to 13*c*.
  - Run in graphical or silent mode.
- Cloud Control 13*c* built-in Agent Upgrade Console (AUC)
  - Upgrade the agents.
  - Delete the old agents.
  - Perform other agent post-upgrade tasks.
- Gold Agent Images
  - Use AUC for initial agent upgrades.
  - Create Gold Agent Images from upgraded agents.
  - Add 12*c* agents as subscribers to Gold Agent Images.
  - Use Gold Agent Images to upgrade the remaining agents.

ORACLE

When upgrading from an upgradeable version of Cloud Control 12*c* to 13*c*, most of the upgrade steps are handled by the Oracle Universal Installer (OUI) in graphical or silent mode. The agents are upgraded later by using the Agent Upgrade Console (AUC), which is an interface that is integrated with the Cloud Control Console. The AUC also handles agent post-upgrade tasks.

In line with the best practice for Cloud Control 13*c*, use the AUC for your initial agent upgrades, and then create Gold Agent Images from those upgraded agents. You can then add your remaining 12*c* agents as subscribers to the Gold Agent Images and use the Gold Agent Image upgrade process to upgrade the 12*c* subscribers.

The 1-System Upgrade Process

- Upgrade of Cloud Control 12*c* OMS, OMR, and agents to 13*c*
- Choice of procedures:
  - All-at-once upgrade of OMS and OMR
    - OMS is shut down for the entire upgrade.
  - Software-only installation of 13*c* software followed by configuration of OMS and OMR
    - OMS is shut down only for the configuration phase.
    - You choose when the configuration phase occurs.
    - This is the Oracle-recommended procedure.
- Agent/OMS compatibility across versions:
  - 12*c* agents can communicate with the 13*c* OMS.
  - 12*c* agents cannot support 13*c* plug-ins.
- OMR is upgraded to the 13*c* schema.
  - Rolling back the 13*c* upgrade requires the 12*c* OMR to be restored from backup.

Choose Your Own Down Time

Upgrading the 12*c* OMS requires shutting it down but you can determine when that happens by choosing between the all-at-once procedure or the software-only install, and then configure procedure. You can also elect to install new plug-ins, and if you are using the software-only procedure, you can opt to install them with the software or during the configuration phase. Finally, you have the choice of running the installer in graphical or silent mode, although silent mode precludes the ability to install plug-ins during the software installation phase of the software-only procedure.

Oracle-Recommended Procedure

The recommended procedure is to use the software-only method along with additional plug-ins in graphical mode. This procedure is made up of three phases:

- Installing the 13*c* software
- Configuring the 13*c* OMS and upgrading OMR to the 13*c* schema
- Upgrading the agents in a rolling fashion

The detailed steps for this procedure are outlined in the following slides.

Agent/OMS Incompatibility Across Versions

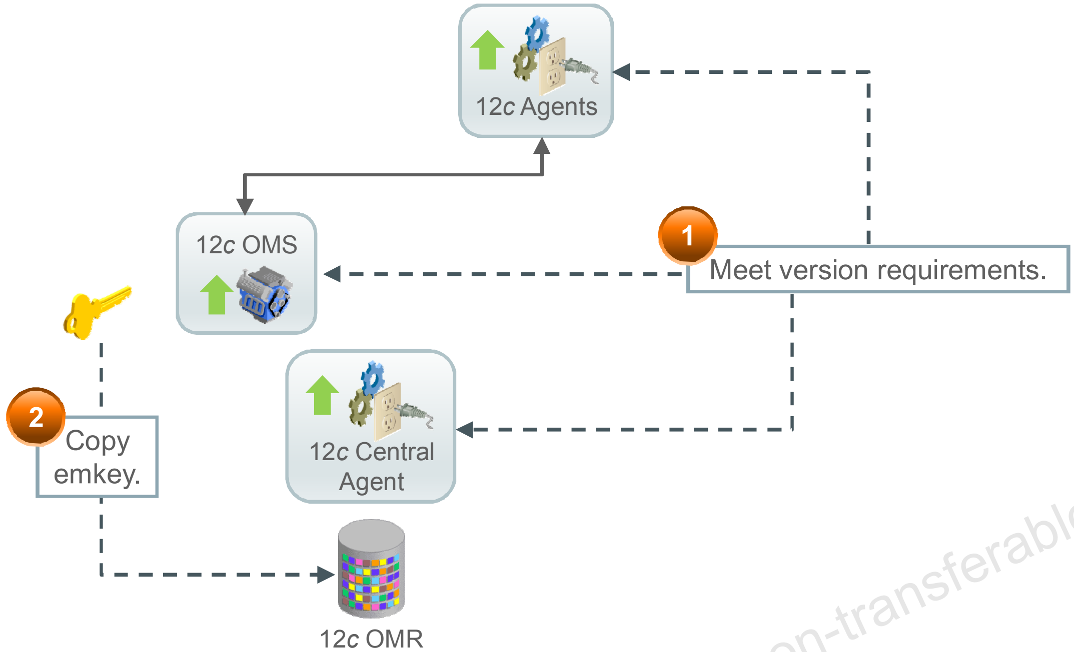
Cloud Control 12*c* agents version 12.1.0.3 and later are compatible with Cloud Control 13*c* OMS. Therefore, there would appear to be no imperative to upgrading agents after upgrading the OMS. However, when you consider that the 12*c* agent does not support 13*c* agent plug-ins, it is clear that you should ensure that all 12*c* agents are upgraded to 13*c* to take full advantage of current and future 13*c* functionality.

Cloud Control 12*c* Software-Only with Plug-ins Upgrade Procedure

1. Ensure that the existing 12*c* system is up-to-date and upgradeable (12.1.0.3 or later).
2. Copy the `emkey` to the OMR.
3. Run the 13*c* OUI with `INSTALL_SWONLY_WITH_PLUGINS=true` and `PLUGINS_LOCATION=<location>` in the 1-System upgrade mode.
4. Shut down the 12*c* OMS and central agent.
5. Back up the OMR and apply the required database patches.
6. Run the `ConfigureGC.sh` script.
7. Upgrade the agents.
   - First the central agent by using the Agent Upgrade Console (AUC)
   - Other agents by using the AUC or the best practice by using Gold Agent Images
8. Clean up the old agents.

The steps of the software-only with plug-ins procedure to upgrade from Cloud Control 12*c* to 13*c* are described in detail on the following pages.

Cloud Control 12*c* 1-System Upgrade Procedure: Steps 1 and 2



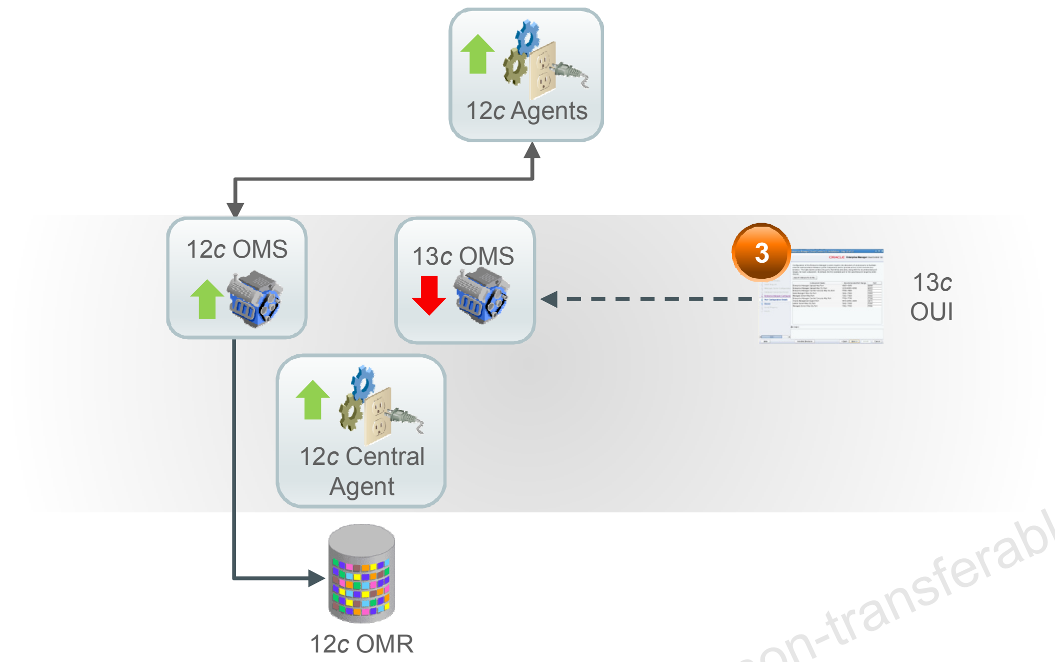
Preparing for a Cloud Control 12*c* 1-System Upgrade

The first two steps in the Cloud Control 12*c* 1-System Upgrade procedure are preliminary to the actual upgrade itself.

Step 1: The first step in the 1-System upgrade of a 12*c* system to 13*c* is to ensure that you are at least on version 12.1.0.3. You must also apply all the latest recommended patches for agents. These patches are available from My Oracle Support and will indicate the versions they are intended for, along with detailed steps to apply them. Note that 12*c* agents earlier than 12.1.0.3 must be brought up to at least version 12.1.0.3. Follow the support instructions to perform this step if your agents belong to earlier versions.

Step 2: Copy your `emkey` into the repository. The `emkey` is the encryption key that is used to encrypt and decrypt all sensitive data in the repository, and is stored in the file system to protect the integrity of the OMR and its backups. In an upgrade, you must preserve the same key, saving it temporarily in the repository, and then moving it back to the OMS after the system is upgraded. The upgrade process will automatically copy the `emkey` from the OMR to the upgraded OMS.

Cloud Control 12*c* 1-System Upgrade Procedure: Step 3

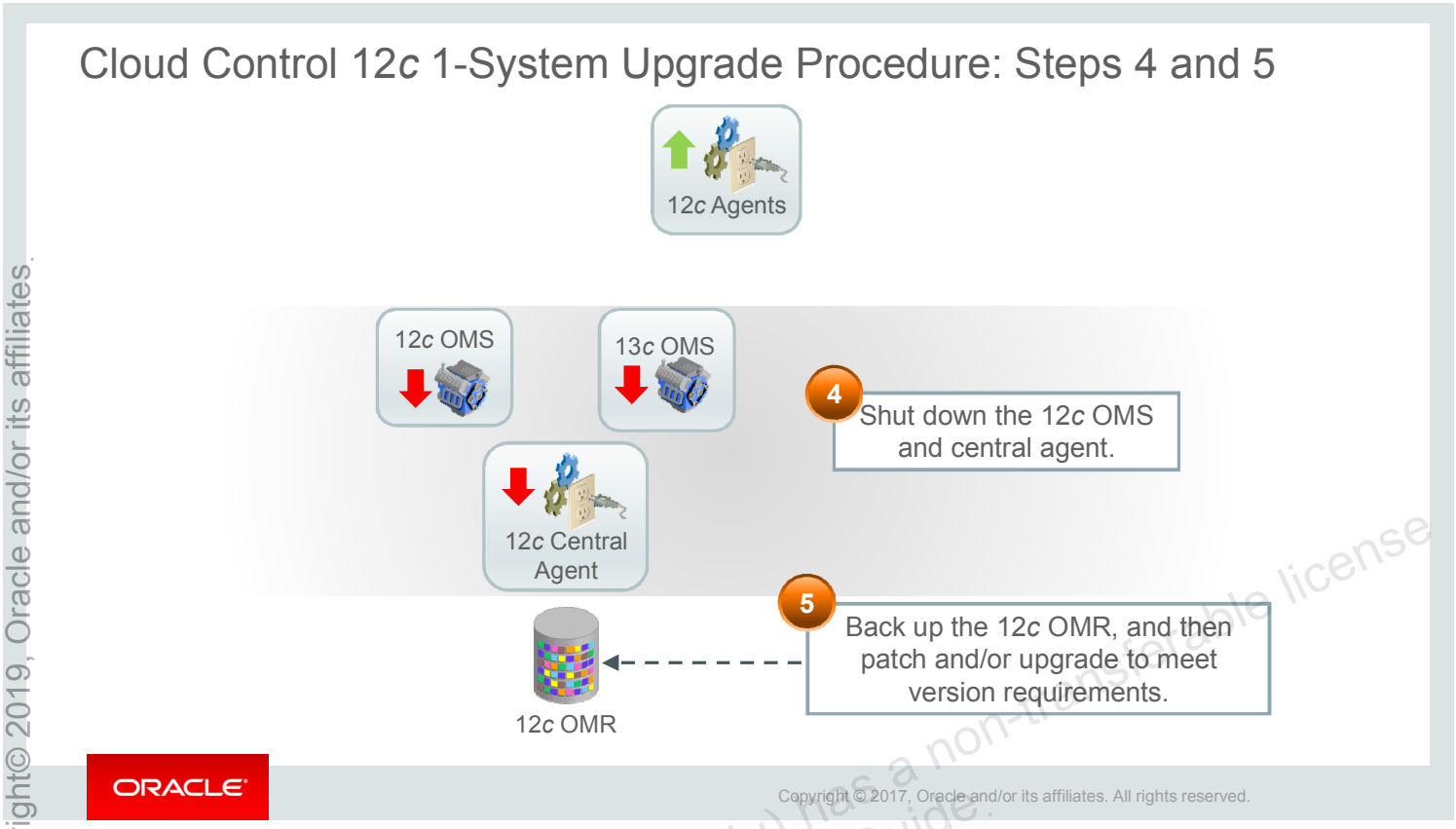


Installing the 13*c* Software and Extra Plug-Ins

The next step involves installing the 13*c* software along with any extra plug-ins by using the Oracle Universal Installer (OUI).

Step 3: Run the 13*c* OUI in software-only with plug-ins upgrade mode and install the Cloud Control 13*c* software as well as any new plug-ins. This mode of the installer can be triggered only by passing two parameters to the installer on the command line when invoking the installer: `INSTALL_SWONLY_WITH_PLUGINS=true` and `PLUGINS_LOCATION=<location>`.

Note that the OMS upgrade is an out-of-place upgrade; therefore, it will create a new middleware home. You must ensure that the OMS server meets all the requirements of the new Enterprise Manager Cloud Control 13*c* version.

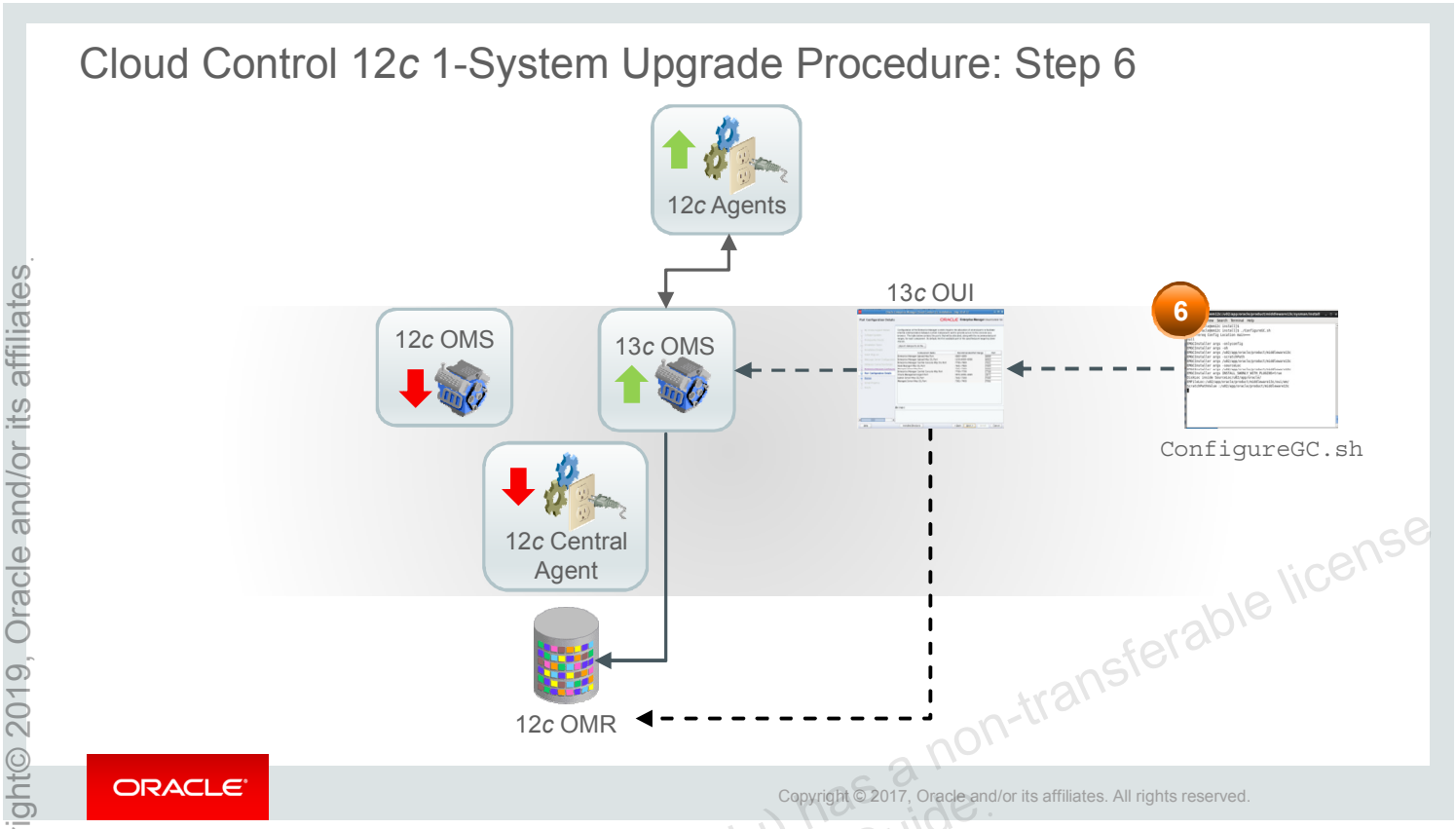


Down Time While Preparing the OMR

The next steps involve shutting down the current OMS and central agent, and then ensuring that your OMR database is certified against the 13*c* requirements. At this point, your Cloud Control 12*c* console will be unavailable.

Step 4: Shut down the 12*c* OMS and the central agent that monitors the repository, but leave all your other 12*c* agents running. The 12*c* agents will continue to gather metrics on your managed hosts and targets, but will not be able to upload or report any problems.

Step 5: Back up your OMR, and then apply any patches that may be required for 13*c*. You may also need to upgrade the OMR database to a version that is certified as a 13*c* repository. Backing up before patching the database means that your backup can still be used to revert to Cloud Control 12*c* if required. Deferring the database patching and upgrade to this step has the advantage that you can use the downtime window of the upgrade. Alternatively, you may decide to perform the OMR database upgrade as a completely separate exercise on your Cloud Control 12*c* environment before embarking on the 13*c* upgrade.

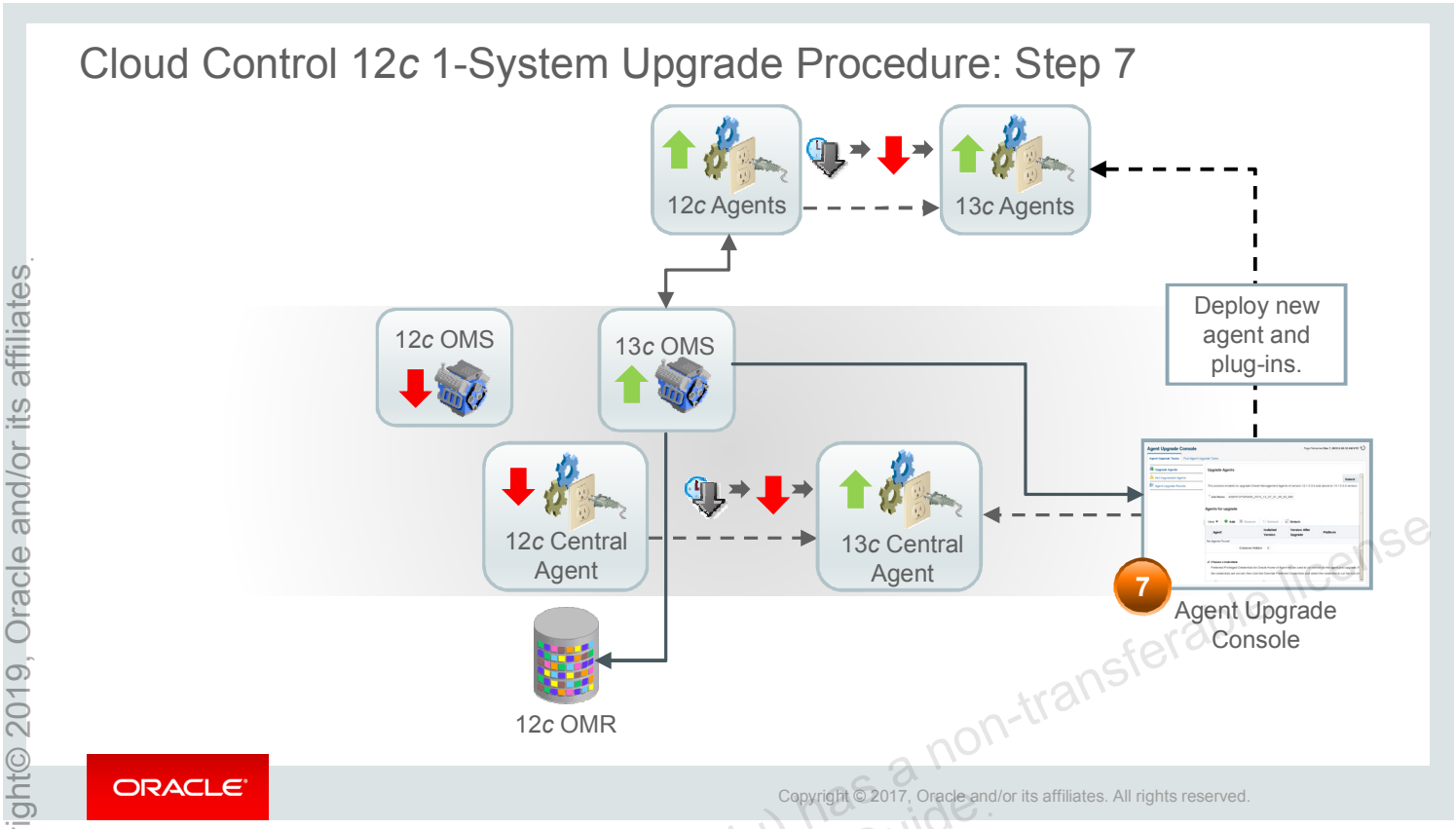


Upgrading the OMS and the OMR

The next step involves upgrading Cloud Control 12*c* to 13*c* by using the Oracle Universal Installer (OUI).

Step 6: Run the 13*c* OUI in 1-System upgrade mode again to configure your 13*c* OMS and upgrade your OMR to the 13*c* schema. You initiate the OUI by executing the `ConfigureGC.sh` script from your Cloud Control 13*c* installation. The OUI will automatically start your upgraded OMS, at which point your 12*c* agents will be able to upload metrics and monitoring information again.

At this point, only the data in your OMR that is required to ensure ongoing monitoring and management of current targets will have been migrated to the new 13*c* schema unless you opt otherwise. Deferred Data Migration (DDM) is the collective term for jobs that are used to migrate noncritical data from the 12*c* OMR schema to the 13*c* OMR schema. After the upgrade, the Deferred Data Migration jobs can be seen on the Post-Upgrade Tasks page where they are listed by data type. You can drill down to see information about the job and retry, if necessary. Deferred Data Migration jobs are executed as Enterprise Manager Cloud Control 13*c* jobs.

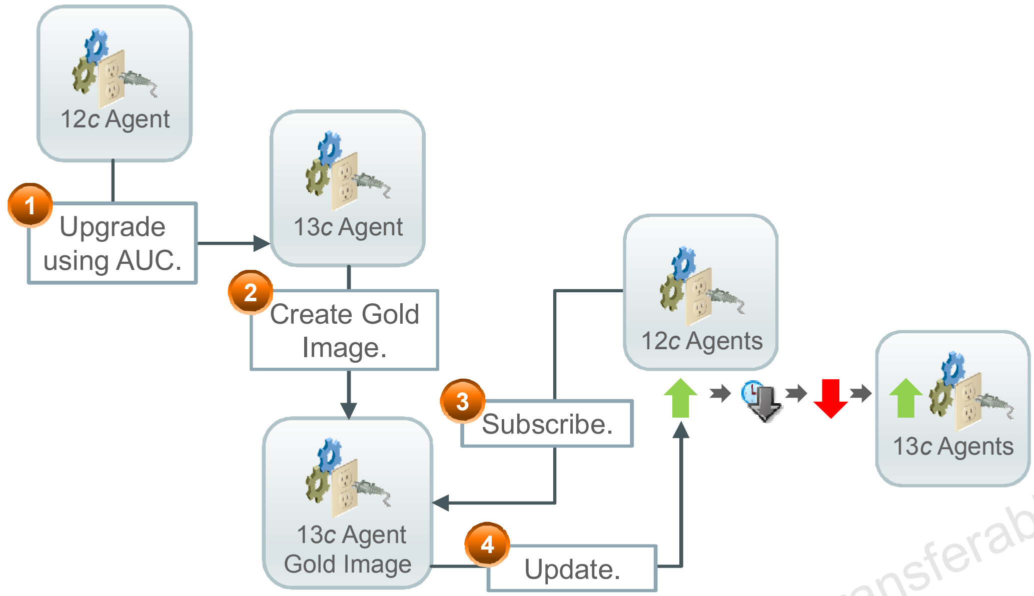


Upgrading all Agents and Their Plug-Ins

The final step in the Cloud Control 12*c* 1-System upgrade involves the management agents.

Step 7: Use the Agent Upgrade Console (AUC) to upgrade your management agents, starting with the central agent. In the background, the AUC will place the 12*c* agent under a blackout while deploying the 13*c* agent, before finally switching over to the 13*c* agent.

Agent Upgrade Best Practice: Gold Agent Images



ORACLE

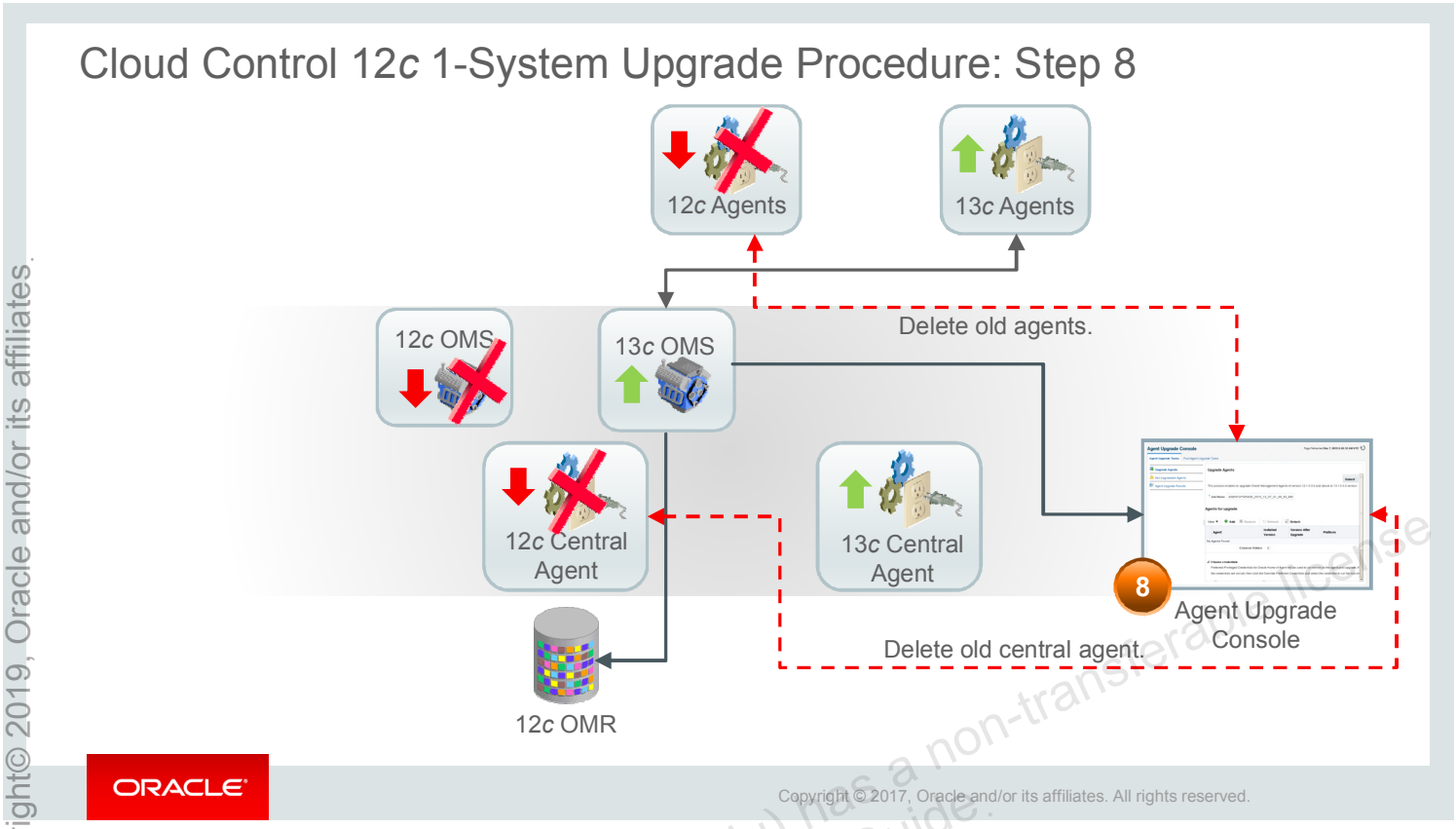
A Best Practice Worth its Weight in Gold

Although you could use the Agent Upgrade Console (AUC) to upgrade all of your 12*c* agents, taking advantage of Cloud Control 13*c*'s Gold Agent Image functionality provides benefits beyond the point of the upgrade itself. By subscribing your agents to a Gold Agent Image, the process of keeping your agents updated is vastly simplified, thus helping to ensure currency and compliance across your Enterprise Manager site.

Using a Gold Agent Image to upgrade your agents to 13*c* is a multistep process:

- Upgrade at least one agent (that is not the central agent) by using the AUC.
- Create a Gold Agent Image by using the newly upgraded agent as the source.
- Mark the Gold Agent Image as the current version.
- Subscribe other 12*c* agents to the Gold Agent Image.
- Update the subscribed agents to the current version of the Gold Agent Image.

You can also get the update process to remove the old 12*c* agent when the upgrade succeeds.



Post-Upgrade Tasks

Step 8: If you have not used the Gold Agent Image upgrades to delete the old 12*c* agents, use the Post Agent Upgrade Tasks tab in the AUC to delete the old 12*c* agents. When you are satisfied that your Cloud Control 13*c* system is operational, you can also delete the 12*c* OMS directories by using the OUI that will ensure that the Oracle Inventory is also updated.

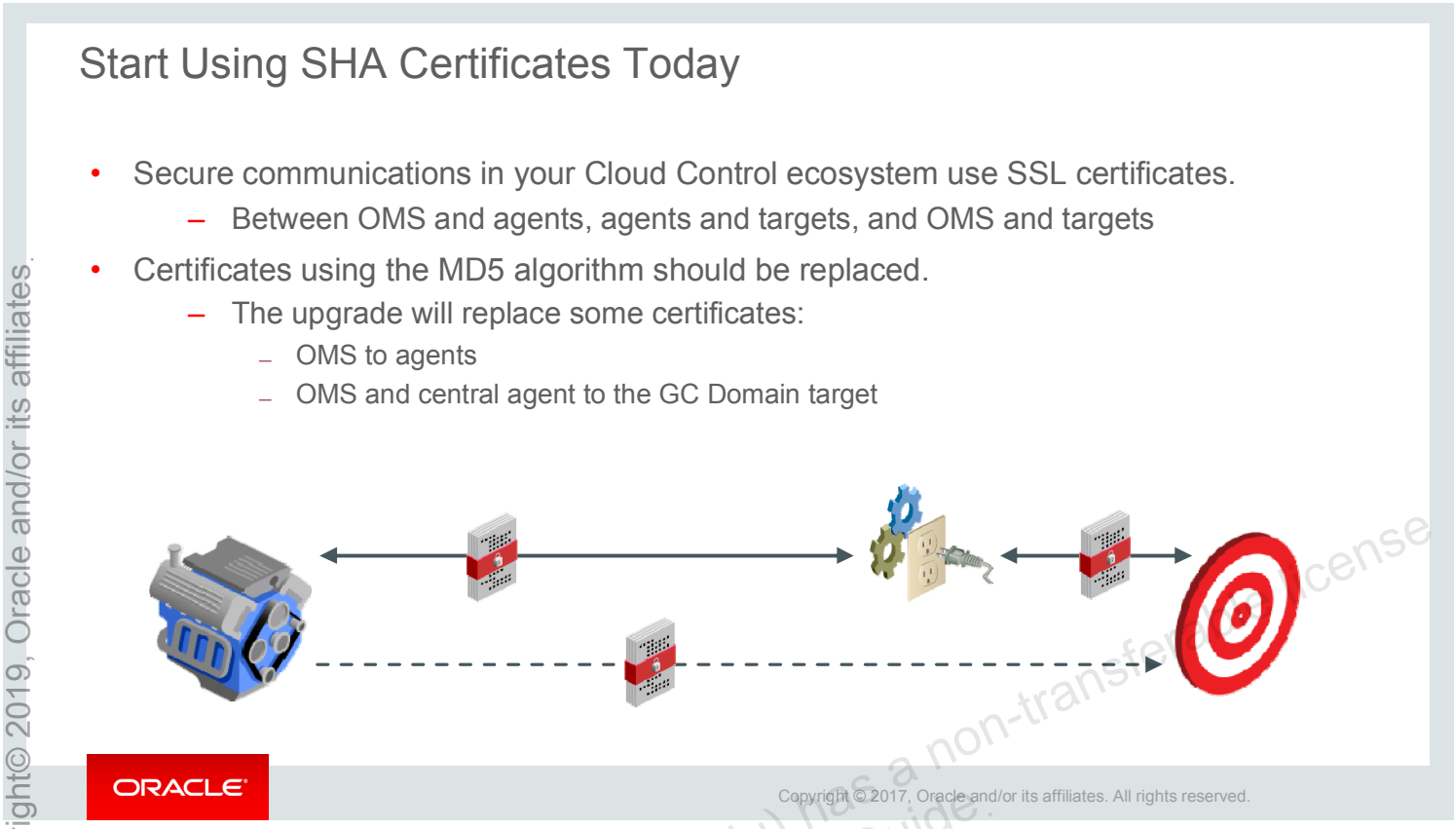
12*c* Upgrade Requirements and Best Practices

- You must have a minimum starting point of 12.1.0.3 for a 12*c* to 13*c* upgrade.
- Best practices:
  - The upgrade requires planned down time.
  - A software-only installation before upgrade reduces down time.
  - Agent upgrades:
    - Use Gold Agent Images.
    - Patch agents while upgrading.
    - Perform a phased upgrade in batches.
    - Use EM CLI.
  - OMS, agent, and target communications:
    - Replace any MD5 certificates with SHA certificates.

Be Prepared

Like all major patching and upgrade operations, you should carefully plan your Cloud Control 12*c* upgrade to 13*c*. This includes:

- Ensuring that you meet the minimum start point requirements for the upgrade, in this case, version 12.1.0.3
- Notifying your stakeholders that the upgrade involves down time of the OMS, although the agents will still be running
- Considering performing a software-only installation of the new Cloud Control 13*c* binaries and upgrading only during your change window with the `ConfigureGC` script
- Using Gold Agent Images to upgrade your 12*c* agents to 13*c*
- Knowing that you can apply patches to your agents at the same time as upgrading them. Gold Agent Images are an ideal way to achieve this. Refer to the documentation for more information.
- Thinking about using EM CLI to script the mass upgrading of your agents
- Proactively replacing any MD5 certificates used to communicate with your targets with SHA certificates



Java Has Already Disabled MD5 Certificates

You should follow the lead of Java and stop using any MD5 certificates in your Cloud Control ecosystem, replacing them instead with Secure Hash Algorithm (SHA) certificates. By default, usage of MD5 certificates is disabled in Java 7 Update 95 and later, but in order to allow you enough time to make any necessary changes, Cloud Control 13cR2 (built with Java 7 Update 111) has re-enabled them. This will be reversed in a future Cloud Control update and when that happens, any communication that is secured with an MD5 certificate between your OMS and agents, OMS and targets, or agents and targets will be broken.

Using an SHA certificate between the OMS and agents

When you upgrade to Cloud Control 13cR2, the OUI will automatically create an SHA certificate for use between the OMS and agents, which will be deployed to your agents as you upgrade them.

Using an SHA certificate between the OMS or agents and targets

The Fusion Middleware targets in the GC Domain (that are part of the OMS) will be configured by the OUI to use an SHA certificate. You will need to intervene for all other targets that use secure communications, and are currently using an MD5 certificate. Details on how this can be done can be found in each target type's documentation.

How do I know where MD5 certificates are used?

The OUI will test to see where MD5 certificates might be used, and present you with a warning if it finds any signs of possible usage. At that point, you can simply dismiss the warning and choose to deal with the issue later, or you can cancel the upgrade and proactively deal with the issue. Of course, you can also address the issue of MD5 certificate usage before commencing your Cloud Control 13cR2 upgrade.

My Oracle Support note *EM 13.2 SHA2 Certificate Pre-upgrade verification for OMS & Agent* (Doc ID 2179909.1) includes a utility called CheckForMD5Usage that can be registered with Cloud Control 12*c* or 13c and executed to determine where, if at all, MD5 certificates are being used in your Cloud Control ecosystem.

Quiz

In the 1-System upgrade from 12*c* to 13*c*, when do you upgrade to the new 13*c* agents? (Select all that apply.)

a. Before shutting down the 12*c* agent
b. After shutting down the 12*c* agent
c. Whenever you feel like it
d. Before installing the 13*c* OMS
e. After installing the 13*c* OMS

Answer: a, e

Deploying the 13*c* agent before shutting down the 12*c* agent is an easily understood concept, because it makes sense to keep the 12*c* agent up and running for as long as possible while we prepare the 13*c* agent. The current agent continues to collect data while the new agent software is being installed, and then the switch is performed.

Because the 13*c* agent can communicate only with a 13*c* OMS, the 12*c* to 13*c* upgrade requires that the OMR and OMS be upgraded before the agents are upgraded.

Quiz

When undertaking the 1-System upgrade, which of the following should you tell your end users and administrators?

a. There will be no disruption in service.
b. Cloud Control will be unavailable for the entire process.
c. It is anybody's guess as to what their targets are doing during the upgrade.
d. Nothing. They don't need to know about the upgrade.
e. Anything. They will believe any explanation.

Answer: b

Strictly speaking, you should consider the current Cloud Control unavailable for the entire 1-System upgrade process because this sets a firm expectation in the minds of all those who use and rely on Cloud Control. Contingency plans for monitoring and management must be put in place because the managed hosts and targets continue to operate and be used even though the current system will be temporarily unavailable.

Communication with your "customer base" is an important aspect of any operation of this type and should be given serious consideration, along with the technical aspects, from the start of the upgrade planning process.

Quiz

In the 1-System upgrade, why don't you really need to back up the current OMR?

a. Nothing ever goes wrong, and all your practice upgrades on your test system go without a hitch.
b. The daily backup is good enough.
c. You do not have the disk space.
d. Your CV is up-to-date.
e. Of course you will take a backup.

Answer: e

You will not use the backup of the OMR as part of the upgrade, so why do it? Because it mitigates against the unforeseeable, taking a backup at a specific point in time will give you the confidence to proceed safe in the knowledge that you can revert if you have to. Including a possible reinstatement of the current OMS in your upgrade plan is vital. Even if your site does not impose change control processes that strictly require and enforce a change window that includes a point in time at which the call must be made to roll back, planning for failure is one of the keys to avoiding it.

Furthermore, be sure to use the same backup process in your upgrade tests that will be used in the production upgrade, and also include a rollback as part of your upgrade tests to ensure that the backup is usable.

Practice 3-1 Overview: 1-System Upgrade (12.1.0.5 to 13.2.0.0)

This practice covers the following topics:

- Bringing the current 12*c* system up to date
- Copying `emkey` to the OMR
- Backing up the OMR
- Shutting down the current OMS
- Running an OUI 1-System upgrade to 13*c*
- Upgrading agents
- Post-upgrade tasks

Summary

In this lesson, you should have learned how to:

- Identify the starting point for an upgrade to Enterprise Manager Cloud Control 13*c*
- Identify applicable upgrade paths
- Describe the 1-System upgrade process

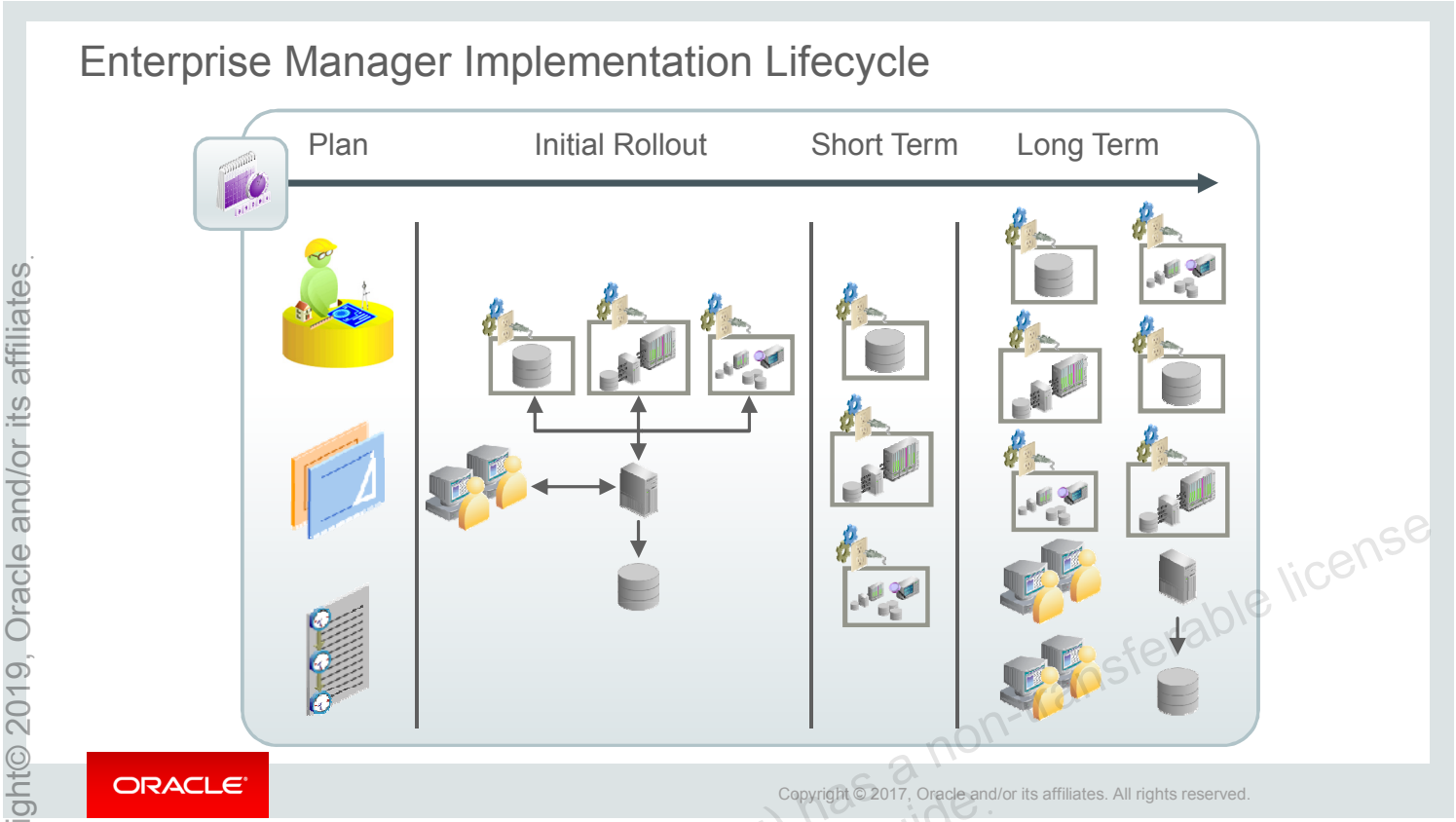
5

Implementation Planning

Objectives

After completing this lesson, you should be able to describe the following:

- Enterprise Manager implementation life cycle
- Implementation planning considerations
- Post-implementation activities
- Enterprise Manager high availability topologies



A Life Cycle of Continuous Growth

The life cycle of an Enterprise Manager implementation ideally starts with the following:

- The appointment of an Enterprise Manager administrator/owner
- Design of the installation topology
- Plan of the implementation, starting with the initial rollout and looking toward future expansion

Initial Rollout

Your initial rollout will, of course, include the Enterprise Manager Cloud Control installation itself, but will also include the initial set of managed hosts and targets, how they will be monitored, and who will administer them. Consideration should be given to how many hosts and targets you want to initially manage, especially if this is your first exposure to Enterprise Manager. For example, you may simply want to start by managing a handful of databases.

Short-Term Growth

After the initial rollout, you can expect to add more managed hosts and targets in the short term.

Long-Term Growth

After Enterprise Manager has been in use for some time, you will see an increase in the number of managed hosts and types of targets, and also a probable increase in your user base as you expand beyond the initial scope. You may also consider adding more infrastructures to your implementation for scalability and/or high availability.

The Implementation Plan

- Appoint an Enterprise Manager owner.
- Think long term and ensure that the foundation is solid.
- Take other business units' requirements into consideration.
- Have a test site.

The Implementation Plan Is Crucial to Success

The implementation plan is probably the most important element of an Enterprise Manager Cloud Control rollout because it maps what you are going to do and when, what resources you have available, what you are monitoring, and how you will monitor it. Controlling the expansion of Cloud Control through your environment is vital to ensure that the implementation is successful.

Role of the Enterprise Manager Owner

The Enterprise Manager owner is given (and takes) the responsibility for the Enterprise Manager implementation meeting its success criteria and serving the needs of its user base. Oracle Enterprise Manager, by its very nature, can touch all parts of a business, so the incumbent in this role must be someone who has a vision of the entire IT enterprise. The owner should know all the key technical people and business stakeholders for every system that is being monitored and managed.

Think Long Term and Ensure That the Foundation Is Solid

- Plan what is going to be monitored, how it will be administered, and by whom.
- Determine the initial size, scope, and growth plan of everything: administrators, targets, management servers, and so on.

- Phase the rollout and use logical milestones to track progress. Rome wasn't built in a day!
- Consider site availability and disaster recovery.

Take Other Business Units into Consideration

- Understand what your business users want so that you can deliver what they need, because they are the owners of the systems that you are monitoring and managing.
- Consider:
  - **Security and access:** Administrators, groups, and privileges
  - **Business requirements:** Availability, monitoring, administration, and reports

Have a Test Site

- It is very important to have a non-production site where you can experiment with metrics extensions, patch updates, and so on.
- You want to test changes and discover possible performance hits before rolling them out to production.
- A test site provides an internal proof-point to showcase additional features.
- Consider using a virtualized environment. Oracle provides VM templates for OVM and VirtualBox through the Oracle Software Delivery Cloud.

Cloud Control Infrastructure Growth

- Initial rollout size (*Now*)
  - Your reason for getting started
- Projected growth (*Next Quarter*)
  - What is projected to be added in the near future
- Long-term growth (*Next Year*)
  - Opportunities and potential additional usage

Growth Is Inevitable

An enterprise-wide management system such as Cloud Control is considered because the enterprise is large enough to dictate it. Therefore, growth is inevitable in the managed hosts and targets that fall under the scope of Cloud Control. As such, your Cloud Control infrastructure may need to grow too.

Initial Rollout Size

There is no hard and fast rule for determining the size of the infrastructure that should be placed under Cloud Control, although you can estimate the volume of metric data that will be gathered by the agents and, therefore, the potential growth of your OMR. As long as you plan carefully, you can always grow the infrastructure as your Cloud Control enterprise expands. In particular, you can provide for future growth by:

- Using RAC for your OMR, even if it is only a single-node cluster, to give it the potential to scale
- Avoiding communicating directly from the agents to an OMS. Instead, use the abstracted management server or load balancer host name.
- Using nonlocal (shared) storage for your software library to ease the transition to multiple OMSes in the future

Projected Growth

Think in terms of the next quarter after rollout or the very short-term future. After Enterprise Manager Cloud Control is in place, you will want to add more targets and people will also start wanting you to add their systems as targets. What, if any, down time of Cloud Control will the owners of your targets tolerate? Will you need to start allowing business groups to administer and monitor their own targets?

Long-Term Growth

Long-term growth is something that the Enterprise Manager administrator needs to map and see coming in the future. There might be other groups or geographically distant sites in the organization that can be brought into the Enterprise Manager fold. There may be internally developed systems that could be monitored through custom plug-ins. It may be appropriate to duplicate the Enterprise Manager hardware at this point to scale up the infrastructure.

An Enterprise Manager Site

A site is a distinct set of Enterprise Manager components and supporting infrastructure that comprises the following:

- Oracle Management Repository
  - Instance, storage, RAC, Data Guard
- Oracle Management Servers
  - Firewalls, load balancers, shared storage
  - On replicated storage for disaster recovery solutions
- Oracle Management Agents
  - Communications to/from OMS
  - Proxy monitoring (off-host targets)
- Software Library
  - Shared storage
  - Synchronized file systems, replicated technology

Considerations for an Enterprise Manager Site

In planning your implementation, consider the performance, configuration, and accessibility of each component to optimize your end users' experience of Enterprise Manager Cloud Control.

Oracle Management Repository

Your Oracle Management Servers must be able to insert data into and retrieve data from the OMR as efficiently and quickly as possible. The performance of your OMR will be sensitive to the underlying CPU, memory, and storage capability and capacity of the OMR server.

Oracle Management Servers

As Cloud Control's view of your IT enterprise grows, so too will the amount of data being uploaded by agents which, in turn, needs to be stored in the OMR. Therefore, the OMS is sensitive to network latency between it and the OMR. You must also take into account any firewalls between the OMS and its agents, and any load balancers fronting your OMSes. For disaster recovery implementations, the OMSes must be on replicated storage (such as Oracle's Sun ZFS Storage Appliance Remote Replication or NetApp Filer).

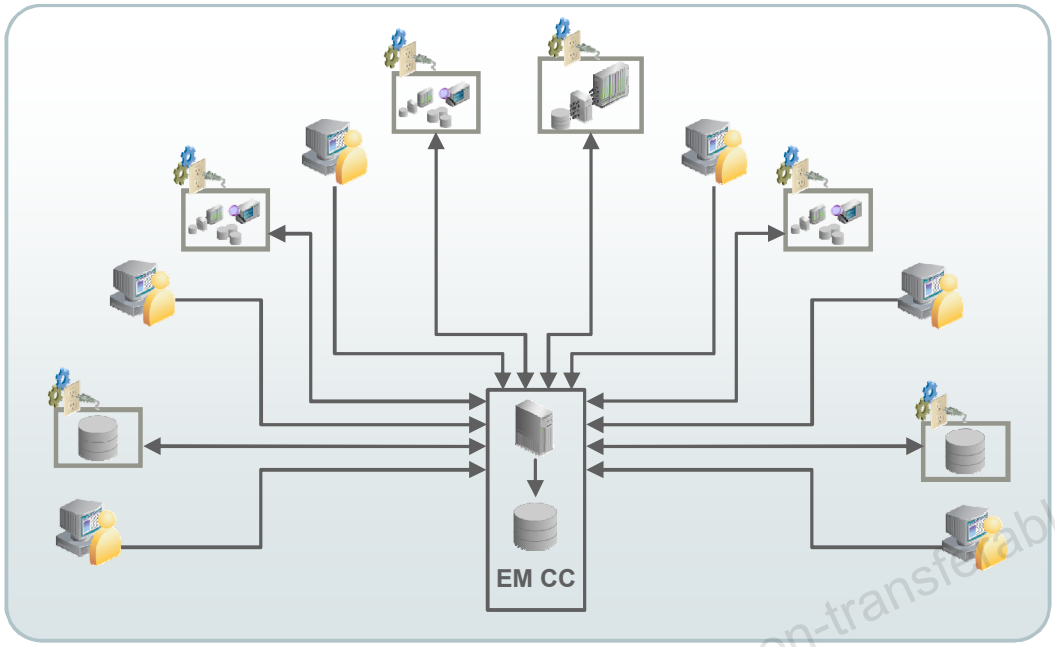
Oracle Management Agents

Agents can reside anywhere on your network. The only requirement is that the agent should be able to access the OMS upload port and, conversely, that the OMS should be able to access the agent URL.

Software Library

The Software Library storage must be shared among all OMSes in a system. In addition, for disaster recovery solutions, the software library files should be duplicated and periodically synchronized.

One Site Managing the Entire IT Enterprise



Having one Enterprise Manager site to monitor and manage your entire enterprise implies:

- One set of hardware
- A centralized infrastructure
- Global network access to all machines
- Global security requirements

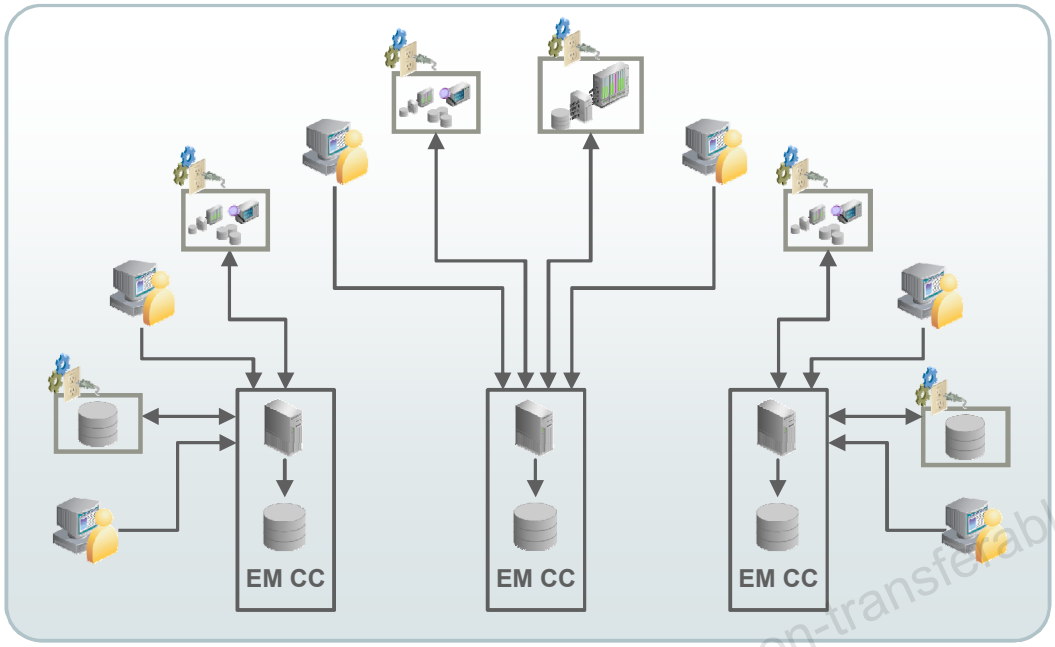
Advantages:

- A centralized global view of the entire IT enterprise
- Security controlled at one point
- One monitoring standard enforceable at a single point

Disadvantages:

- Increased requirement for high availability because your site may be utilized across multiple time zones and the International Dateline
- Latency or network disruptions between your management agents and the OMS

Multiple Sites Managing the IT Enterprise



Using multiple Enterprise Manager sites to monitor and manage your enterprise implies:

- Each site has its own Cloud Control hardware.
- Each site has its own localized infrastructure.
- Localized network access to the managed hosts is all that is required.
- Local security requirements can be enforced and are all that need to be adhered to.

Advantages:

- Restricted access to only local targets for local administrators
- Specialized management setup per site (SLA, notifications, monitoring)

Disadvantages:

- There is no centralized overview of the entire enterprise.

Because of the complexities involved, you should consider using multiple sites only if business requirements demand it. Regardless of your implementation plan, it is recommended that your initial rollout consists of only a single site to remove a layer of complexity and potential problems in the short term.

Sizing the Repository

- Repository size is based on:
  - The number of discovered targets
  - The amount of retained historical data
  - The number of administration tasks defined and used
- Start with the documented recommendations.
- Use advanced installation and select from preconfigured small, medium, and large sizes.
- Don't forget JVMD metrics collection if you intend to use Java Virtual Machine Diagnostics.

Repository Size Can Be Estimated

Although the size of your repository cannot be accurately calculated in advance, the size can be estimated based on the initial rollout and projected growth predicted for your installation. The documentation contains recommendations for small, medium, and large deployments, and these are ideal starting points.

Discovered Targets

The agent will upload a certain amount of metric data in each 24-hour period for each discovered target. The quantity of data depends on the target type. The OMS also stores configuration data for each target, which we can estimate to be 10% to 30% of the size of that target's metric data.

Retained Historical Data

Historical data contributes to the size of the repository. By default, the OMS applies the following retention periods:

- Weekly, monthly, and yearly metric data rollups
- Retention of state information for six months
- Retention of configuration data for one year

Administration Tasks

Each administration task involves some overhead in terms of configuration and state information, which you can estimate at around 1 KB per task. These tasks include:

- Cloud Control jobs
- Patching and Provisioning jobs (and patches in the patch cache)
- Templates

JVMD Metrics

Collection of Java Virtual Machine (JVM) diagnostic metrics from JVMs across the enterprise is often overlooked in the planning phase because the JVM instances are seen as a subtarget of middleware. However, JVMD diagnostics will cause your OMR to grow rapidly, and it is easier to cater to such growth in the planning phase rather than during post-implementation. For example, collecting diagnostic metrics for 1,000 JVMs each with 8 GB heap size over a two-second sample interval and raw data retention of 10 days with 30 days of aggregated data is estimated to require almost 1.6 TB of storage.

OMR Life Cycle and Security

- Maintain the OMR database.
  - Patch as you would any other production database.
  - Apply patches to your test environment first.
- Apply security measures.
  - Secure communications between OMS and OMR.
  - Restrict SQL access to only OMS servers and Enterprise Manager administrators.
- Back up the OMR.
  - Use your site's standard backup regime.

Maintain and Secure the OMR Database

The OMR database should be treated like any other database in your enterprise and kept current by applying Enterprise Manager patches and database patches as they become available. For this reason, the Enterprise Manager test environment takes on renewed importance as the site where you can test patches before applying them to your production environment. If you are using a multinode RAC cluster, rolling patches can be applied without any outage to your OMR.

Use the network security feature of the database Oracle Advanced Security Option (AOS) to secure communication between the OMR and OMS. AOS combines network encryption, database encryption, and strong authentication.

You can further restrict access to the OMR so that the database accepts connections only from those servers that are hosting the OMS.

The OMR is a production database and should be protected with your standard production database backup regime. Make sure that the backups are valid and can be used to perform a restore operation.

OMS Life Cycle and Security

- Maintain the middle tier.
  - Apply WLS and OMS PSUs as per Oracle Support recommendations.
  - Apply patches to your test environment first.
- Apply security measures.
  - Lock OMS in secure mode to disable unsecure access.
  - Secure the Console with an SSL certificate from a trusted authority.
  - Do not allow the installation owner to log in directly to the operating system.
- Back up the OMS configuration.
  - Back up after installation and after every infrastructure change.

Maintain and Secure the OMS

The OMS and its underlying WLS installation should be treated like any other middle-tier application in your enterprise, and kept current by applying Enterprise Manager and WLS patches as they become available. As with OMR maintenance, the Enterprise Manager test environment takes on renewed importance as the site where you can test patches before applying them to your production environment.

Assuming that you use the default secure communication between the agents and the OMS, disable unsecure communications with the `emctl` command: `emctl secure lock`.

Enterprise Manager Cloud Control, out of the box, uses an SSL certificate that is a self-signed "demonstration" certificate and is not issued by a valid certificate authority. Replacing this with a certificate issued by a trusted authority increases the security of the Cloud Control Console.

The user who owns the middleware home should not be able to log in directly to the operating system; instead, access should be only through impersonation utilities such as `sudo` and `pbrun`.

Back up the OMS configuration after installation and again after every change in infrastructure with the `emctl` command: `emctl exportconfig oms`.

Elements of High Availability

- High availability (HA)
  - Eliminating single points of failure
- Disaster recovery (DR)
  - Recovering from failure
- Maximum availability architecture
  - Combining the HA and DR elements
- Down time
  - How long can you tolerate your system being unavailable
  - Maintenance window unavailability included

Pieces of the Same Puzzle

Designing a highly available system involves taking various elements and combining them to suit your needs and requirements.

High Availability

Strictly speaking, high availability gives consideration to the single points of failure in your system and eliminates them through redundancy. Examples are RAC databases, ASM storage, and multiple OMSes fronted by a load balancer.

Disaster Recovery

Disaster recovery extends the concept of high availability beyond single points of failure by providing secondary elements that can be brought into play when the primary elements fail. Examples are active/passive middleware clusters and standby databases.

Maximum Availability Architecture

Implementing high availability to address single points of failure and disaster recovery to address system failure leads you down the path of maximum availability architecture (MAA).

Down Time

The key to determining which elements of high availability are appropriate for your site is how much down time you can tolerate; this includes unexpected as well as planned down time. Availability is commonly expressed as a percentage, but it is often more meaningful when expressed as hours. For example, 99.9% availability is roughly equivalent to 8 hours and 45 minutes of down time per year.

Four Levels of High Availability

- Level 1: Best practice installation
- Level 2: Local active/passive HA
- Level 3: Local HA
- Level 4: Local HA and Remote Active/Passive DR

Building Levels of Availability

The levels of availability build on each other, expanding the redundancy and recovery options of the previous level. Observing these recommended topologies will open pathways for transition from a lower to a higher level.

Level 1: Best practice installation

Level 1 availability involves implementing a best practice, out-of-the-box configuration of Enterprise Manager Cloud Control, which is ready for future transition to higher levels of availability, but with no specific high availability elements. Even with no action taken other than installing the product, availability is considered to be around 95%. Consider using a database instance for the OMR with protected storage (ASM) that will provide an element of protection against a storage-level failure, but there is no redundancy for any of the Enterprise Manager components.

Level 2: Local active/passive HA

Level 2 availability consists of an active and passive OMS with shared storage at the same physical location, which employs Data Guard to replicate the OMR to the failover hardware. Some down time is incurred during the failover to the redundant system.

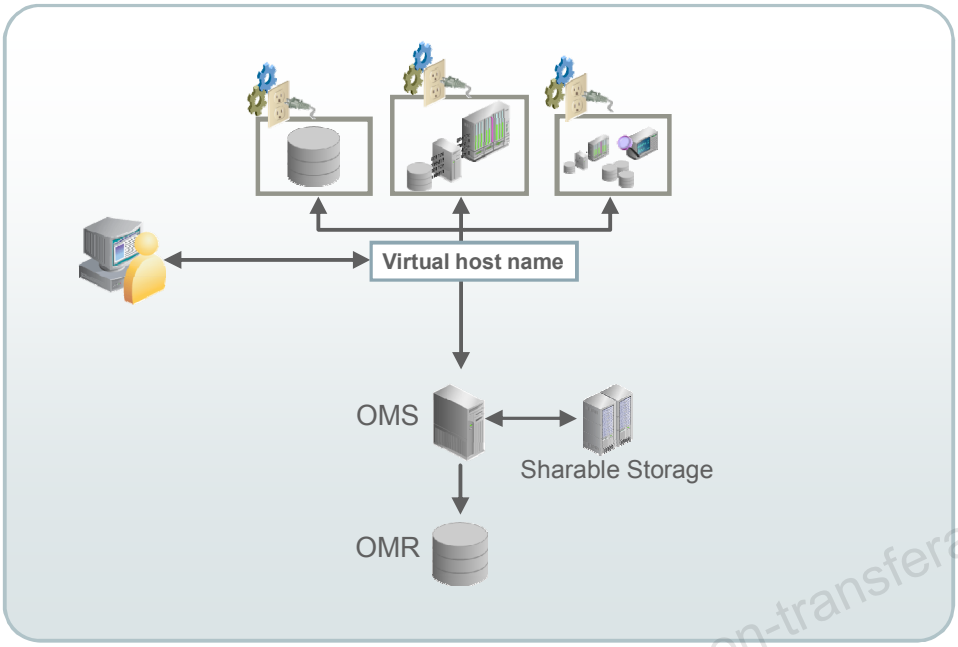
Level 3: Local HA

Level 3 availability adds active/active local HA for the OMS and OMR through the addition of multiple active OMSes that are fronted by a load balancer and a multinode RAC, all hosted at the same physical location.

Level 4: Local HA and Remote Active/Passive DR

Level 4 availability adds Disaster Recovery (DR) protection with the addition of a remote site in accordance with Maximum Availability Architecture (MAA) principles. A best practice for implementing dual-site Active/Passive DR in this solution is to place the Oracle Inventory, Oracle Homes, Software Library, and BI Publisher storage for the OMSes on replicated storage (such as Oracle's Sun ZFS Storage Appliance Remote Replication or NetApp Filer) and replicate the OMR by using Data Guard.

High Availability Level 1 Best Practice Installation

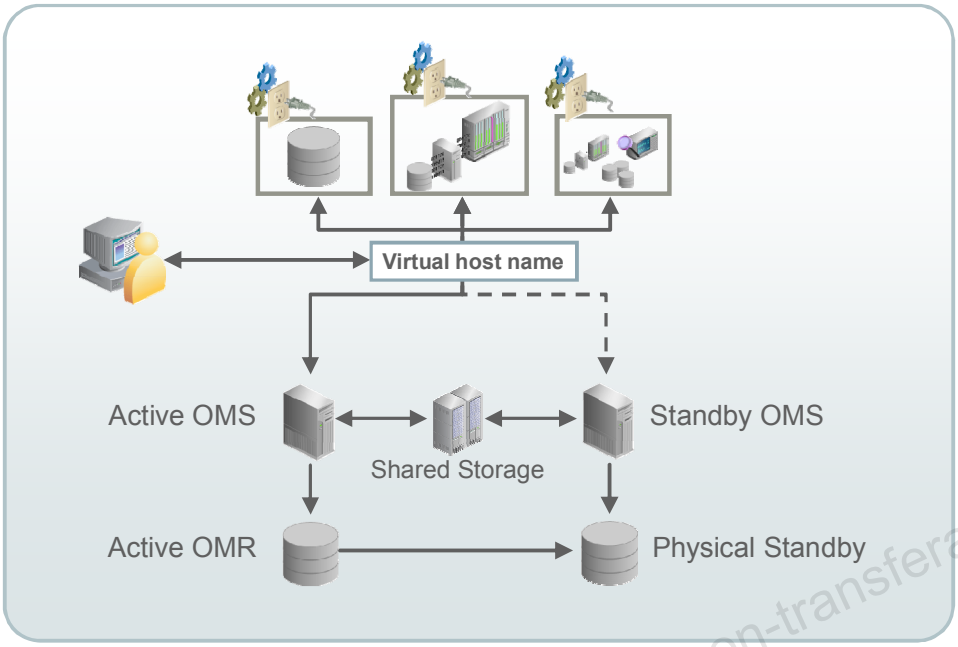


Level 1: Preparing for the Future

Even though the Level 1 architecture is effectively nothing more than an out-of-the-box installation, you can incorporate features of the other high availability architectures that will smooth any future transition to a higher HA level:

- Install the OMS under a subdirectory of `ORACLE_BASE` on media that can be shared, for example, `/u01/app/oracle/product/oms`.
- Use sharable storage for the Oracle Inventory, Software Library, and BI Publisher.
- Install against an alias host name that your agents and web console connections will use instead of the actual OMS server's host name.

High Availability Level 2 Sample Design



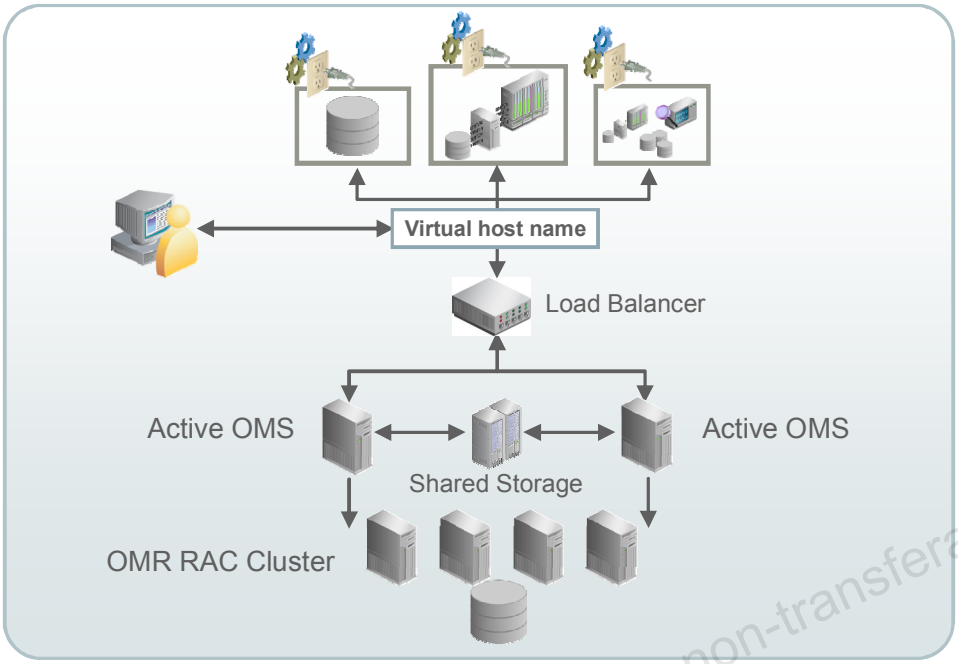
Level 2: Local Active/Passive HA

An Enterprise Manager High Availability Level 2 topology is characterized by being confined to a single physical location with high availability achieved by failing over from an active OMS and OMR to a passive standby OMS and OMR.

This Level 2 design consists of the following:

- An active OMS
- An active OMR
- A standby OMS
- A physical standby OMR
- Shared storage for the Oracle Inventory, Oracle Homes, Software Library, and BI Publisher
- Software installed against alias host names
- Agent and Cloud Control Console connections made to the application virtual host name
- Failover performed at the network level

High Availability Level 3 Sample Design

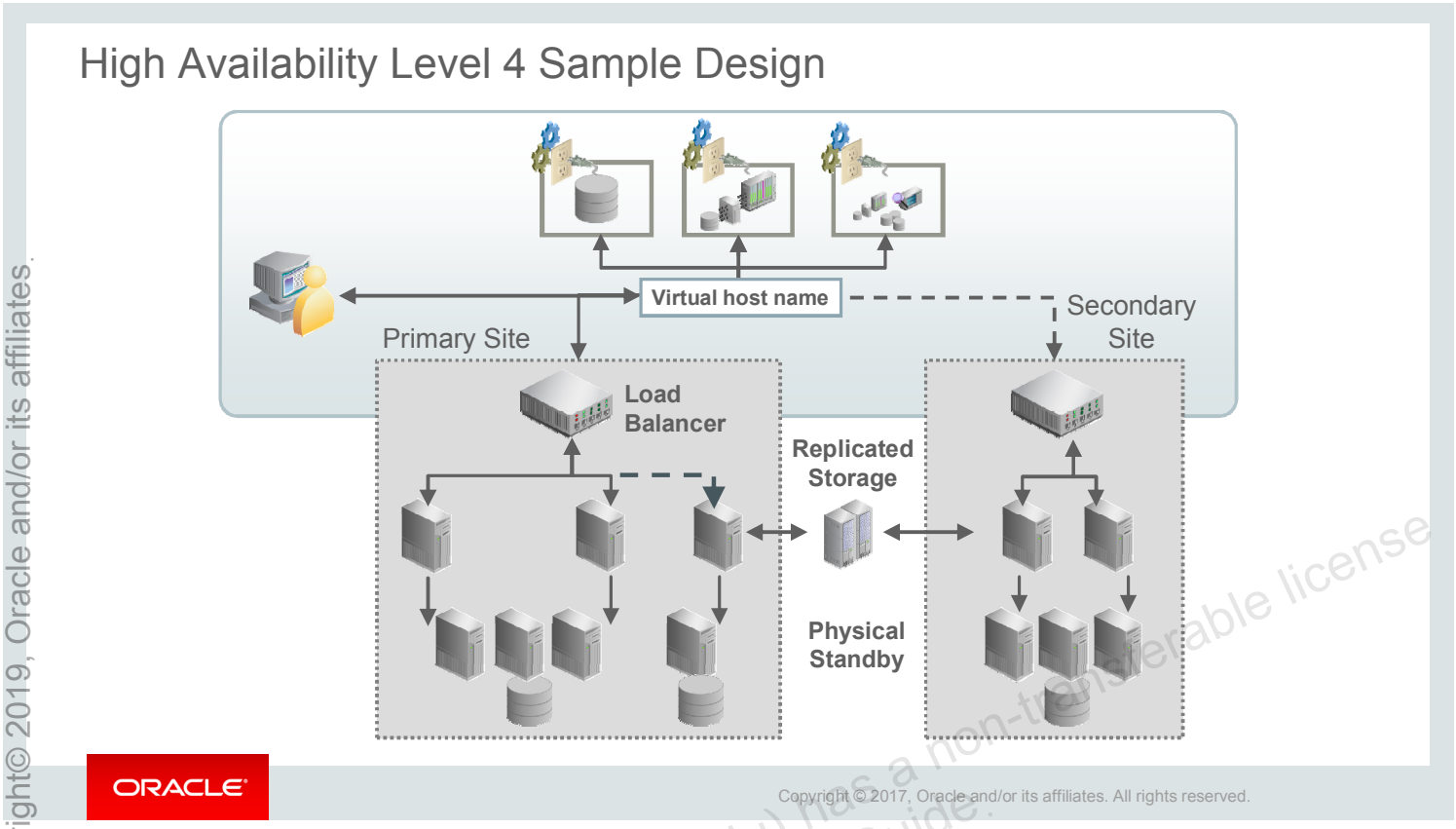


Level 3: Local HA

An Enterprise Manager High Availability Level 3 topology is characterized by active and passive redundant components at the OMS and OMR tiers, all hosted at the same physical location.

This Level 3 design consists of the following:

- Two active OMSes and one passive OMS that is fronted by a load balancer
- Shared storage for the Oracle Inventory, Oracle Homes, Software Library, and BI Publisher
- Software installed against alias host names
- Agent and Cloud Control Console connections made to the application virtual host name
- OMS failover performed by a load balancer
- OMR protected locally by RAC cluster and Data Guard

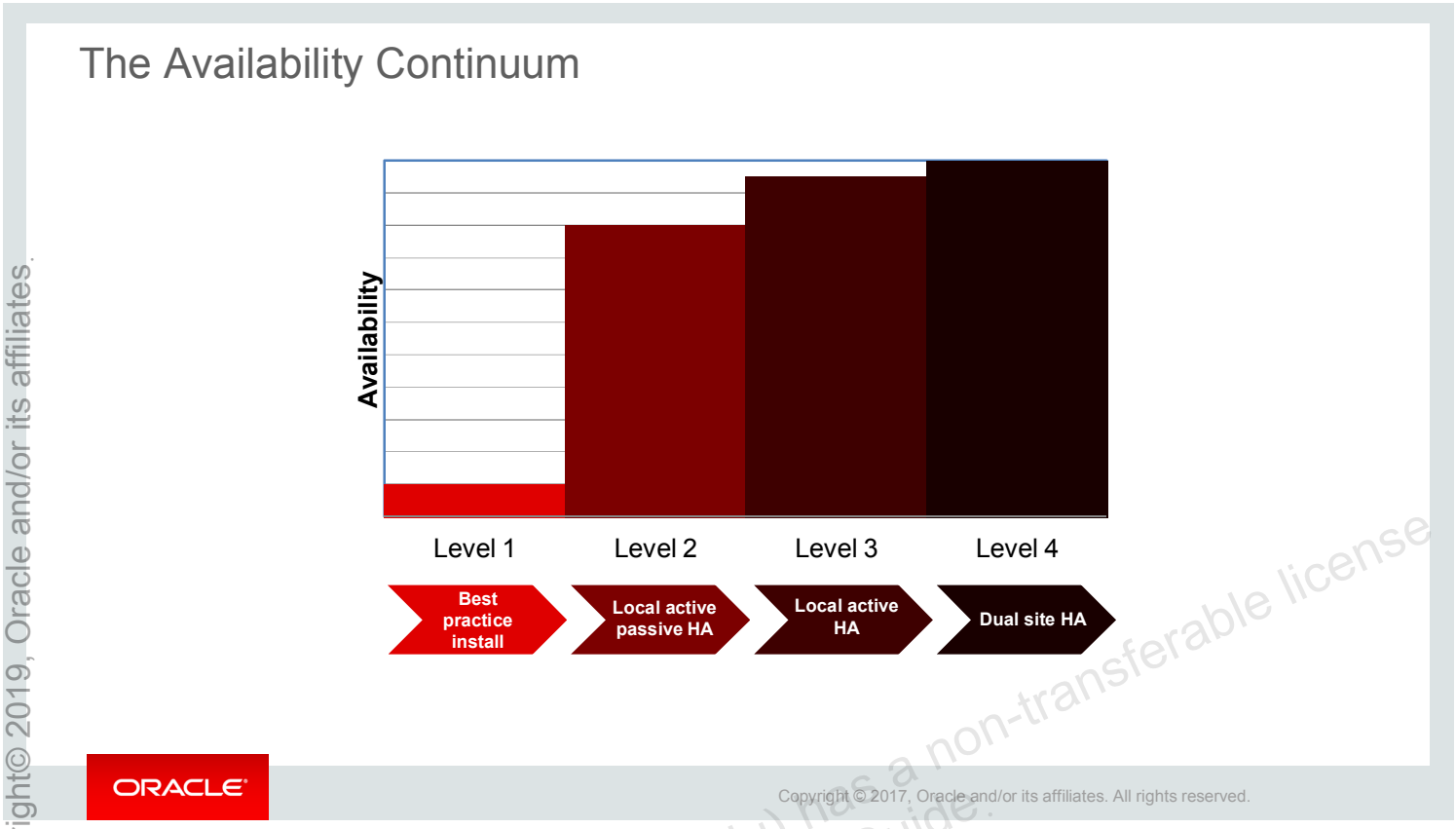


Level 4: Local HA and Remote Active/Passive DR

An Enterprise Manager High Availability Level 4 topology is characterized by active/active and active/passive HA at the primary site and active/passive DR across the primary and secondary sites. This topology is the highest level of Maximum Availability Architecture (MAA) for EM.

This Level 4 design is a multiple-site solution and consists of the following:

- A Level 3-design primary site
- A remote secondary site with a physical standby RAC cluster database for the OMR
- Replicated storage across both sites for the Oracle Inventory, Oracle Homes, Software Library, and BI Publisher
- Software installed against alias host names
- Agent and Grid Control Console connections made to the application virtual host name
- Site failover performed by a global load balancer or DNS between load balancers
- Network infrastructure and device redundancy within and between sites
- Power redundancy



The Illustrated Availability Continuum

The graph in the slide depicts the increase in availability that can be gained with the progression between levels of availability. It is not based on empirical data, and the relative values that are used are for illustrative purposes only.

Another way to interpret the y-axis scale is as a measure of acceptable down time—the lower end of the axis represents a reasonable amount of down time as being tolerable, whereas the upper end of the axis represents even the smallest amount of down time as being intolerable.

Yet another way to think of the y-axis is in terms of costs. If the demanded availability is higher and if down time becomes accordingly less acceptable, there will be higher costs in achieving the desired level of availability.

Advanced configuration of Enterprise Manager Cloud Control, including implementations of various levels of high availability, are covered in more detail in the *Oracle Enterprise Manager Cloud Control 13c Advanced Configuration Workshop* course.

Keeping Up with Current High Availability Trends

- For further information, refer to:
  - Oracle Technology Network
    - http://www.oracle.com/technetwork/oem/framework-infra/index.html
    - http://www.oracle.com/technetwork/database/features/availability/em-maa-155389.html
  - My Oracle Support (search for “maximum availability architecture”)
  - My Oracle Support community https://community.oracle.com/community/support/enterprise_manager
  - OTN Community https://community.oracle.com/community/enterprise_manager
- More details in the *Oracle Enterprise Manager Cloud Control 13c Advanced Configuration Workshop*

Summary

In this lesson, you should have learned how to:

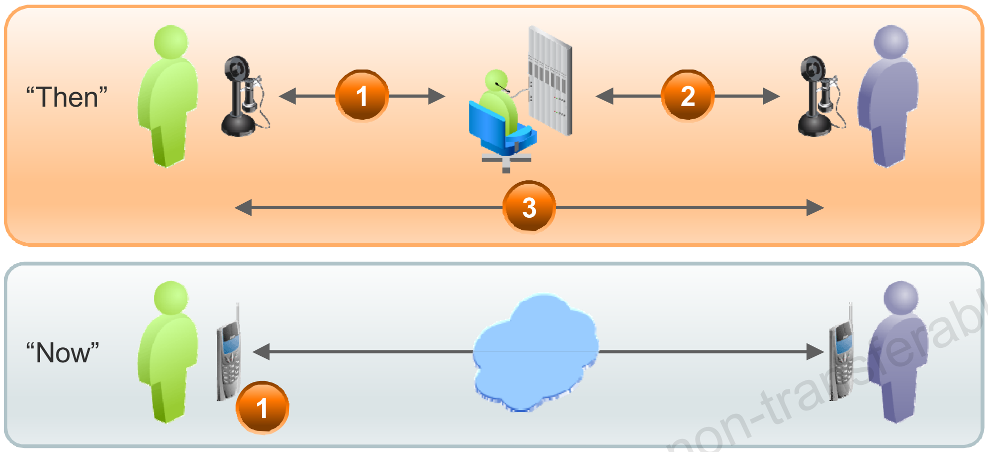
- Plan your initial Enterprise Manager Cloud Control implementation
- Prepare for your Enterprise Manager Cloud Control implementation to grow
- Maintain your Enterprise Manager Cloud Control implementation

A

Cloud Computing Fundamentals

We Are Already Consumers of the Cloud

- The cloud is a metaphor for obfuscated service provision.
- The cloud metaphor is neither new nor exclusive to IT.
  - Consider the phone call then and now.



We Consume Cloud Services Every Day

The cloud metaphor is invoked whenever the details of an implementation or provision of a service are obfuscated from the perspective of the end consumer. There are many examples of cloud-based services in everyday life, such as a phone call between two parties. Before the advent of automated exchange, making a phone call involved multiple steps that you may be aware of:

1. Call the operator and ask for a connection to the other party.
2. Wait for the operator to connect you to the other party.
3. Converse with the other party (with the possibility of the operator sniffing all voice traffic).

Therefore, when you made the phone call, you were aware of how the call was routed to the other party, and could possibly even trace the phone lines along which the call was transmitted.

These days, making a phone call requires only access to a phone service and knowledge of the other party’s phone number. How your call is actually connected to the other party is obscured within the telecommunications cloud, and in this era of voice-over-IP, mobile communication, and global roaming, the means of communication is further obfuscated.

Other cloud services in your daily life could include:

- Your milk supply. Earlier you would have known which dairy produced your milk, but today, this information is obscured by large milk producers and their distribution network.
- The electricity supply grid. The power that you consume may have been generated in another country.
- Mail delivery network. Whereas earlier your post could be guaranteed to be collected, sorted, and delivered by a single government agency, now there could be multiple independent contractors between the sender and the recipient.

In all these examples, the service or product that you consume has not altered; only the way in which it is provided has changed.

To further illustrate how cloud is already part of our everyday life, consider one more example:

- Browsing a website. You are typically unaware of the route taken by the HTTP packets between your browser and the site's web servers, or even where the web server is physically located.

Cloud Computing

- From the consumers' perspective:
  - It is an IT capability or service.
  - Its implementation is both unknown and unimportant.
  - It is available anytime, from anywhere.
- From the providers' perspective:
  - It allows them to use computing resources efficiently, wherever and however possible.
  - It allows for flexibility in resource allocation to meet varying consumer demand.
  - Meeting agreed service levels is more important than anything else.

ORACLE

The US National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Every Cloud Has a Silver Lining

Cloud computing takes on a different meaning depending on your perspective, and all present different views of the benefits that can be derived from cloud computing.

From the perspective of a consumer of cloud-based resources, the cloud is simply a capability or service that is used without having knowledge of how or where it is implemented. Indeed, knowledge of how the consumable product is provided is obscured by the very nature of it being accessed via "the cloud." Because implementation details are of no concern to the consumer, their primary interest is availability and usability.

From the perspective of a provider of cloud-based resources, the cloud allows the provider to service consumer demand by using whatever computing resources are available. This loosens the ties of physical resources to application topologies and gives the provider the flexibility and agility to deploy resources in the most efficient and timely manner possible. Like consumers of cloud-based resources, providers are also primarily interested in availability and usability because the efficacy of their offering is determined by a consumer's satisfaction with that offering, typically defined and measured through service-level agreements.

Cloud Computing: Essential Characteristics

- On-demand self-service
  - Anytime. No human involvement is required.
- Broad network access
  - Anywhere, from any device
- Resource pooling
  - Shared resources to meet many demands
- Rapid elasticity
  - Seamless response to meet changing demands
- Measured service
  - Metering of and reporting on usage

Five Essential Characteristics of Cloud Computing

The NIST definition of cloud computing includes five essential characteristics:

- **On-demand self-service**

  Consumers can request and receive computing resources as required without human intervention by a provider.
- **Broad network access**

  The resources and self-service portals provided by the cloud can be accessed through standard network-connected devices (for example, mobile phones, tablets, laptops, and workstations).
- **Resource pooling**

  Providers use their computing resources to serve the demands of many customers in a multi-tenancy model. All customers can then benefit from the dynamic allocation of resources from the pool to meet their demands. Examples of resources include storage, processing, memory, and network bandwidth.
- **Rapid elasticity**

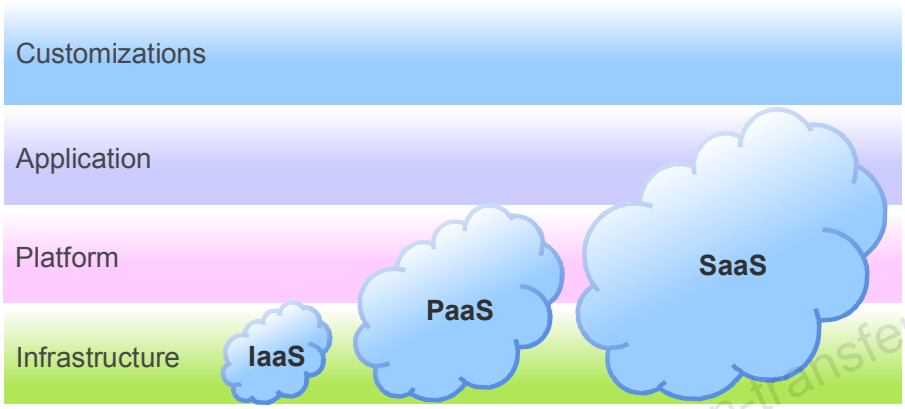
  The capacity of the cloud can be scaled up or down in response to consumer demand in a manner that appears to the consumer to provide unlimited capabilities.

- **Measured service**

  Consumption of cloud resources is measured in a manner that is appropriate to the service (for example, storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported upon by providers and consumers alike.

Cloud Computing Service Models

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)



Three Cloud Computing Service Models

The NIST definition of cloud computing includes three service models.

Infrastructure as a Service (IaaS)

The cloud computing provider makes available resources such as processing, networking, and storage that can be requested by consumers. Typically, the infrastructure that is provisioned in an IaaS cloud is virtualized, although this is not necessarily apparent to the consumer. The consumer is responsible for providing an application platform and applications to deploy on that platform, and can of course customize those applications as required.

An example of an IaaS cloud request is an Oracle Linux 5 Update 7 x86-64 virtual machine with 16 GB of RAM and 250 GB of storage.

Platform as a Service (PaaS)

The cloud computing provider makes available platforms onto which consumers can deploy their own applications, and then customize those applications as required.

Examples of platforms that might be available in a PaaS cloud are Oracle Database (both single instance and RAC) and Oracle WebLogic Server.

Software as a Service (SaaS)

The cloud computing provider makes available an application that consumers can use and customize.

Examples of software that might be available in a SaaS cloud are Oracle Fusion Applications and Oracle Social Network.

Cloud Computing Deployment Models

- Private
  - For exclusive use by a single organization
- Community
  - A common environment for use by a group of related organizations
- Public
  - Separate environments for use by multiple organizations (multi-tenancy)
- Hybrid
  - A combination of private and public clouds for a single organization

Four Cloud Computing Deployment Models

The NIST definition of cloud computing includes four deployment models:

Private Cloud

The hosting and operation of private clouds may also be outsourced to a third-party service provider, but a private cloud remains for the exclusive use of one organization.

Community Cloud

Examples of communities are all the different branches of the military, all the universities in a given region, or all the suppliers to a large manufacturer.

Public Cloud

All underlying infrastructure is owned and operated by the public cloud provider.

Hybrid Cloud

This may be to implement a “cloud bursting” scenario, where an organization might run the steady-state workload of an application on a private cloud. But when a spike in workload occurs (such as at the end of a financial quarter or during the holiday season), the application can burst out to use computing capacity from a public cloud, and then return those resources to the public pool when they are no longer needed.

Sharing the Benefits of Cloud Computing

- There is separation of provisioning resources and their usage.
  - Consumers can focus on their business needs.
  - Providers can focus on the resources to meet those needs.
- Maximum flexibility is allowed for all parties.
  - Consumers use as much or as little of the cloud as they need.
  - Providers need to only meet the demand, not exceed it.
- Consumers' capital expenses become operating expenses.
  - Hardware purchase and maintenance, machine room cooling and lighting, networking, and so on
- Providers can recoup setup costs from multiple consumers.

The Cloud Is a Win-Win Scenario for IT Providers and Consumers

The benefits of the cloud are equally distributed between providers and consumers of IT infrastructure and services.

- Resource providers can:
  - Manage the underlying infrastructure in any manner they choose, provided they meet their service-level agreements
  - Deploy resources where they are needed, as they are needed
  - Pool resources to provide scalability and multi-tenant capabilities
  - Use IT hardware to ensure optimum return on investment
- Resource consumers:
  - Need to focus only on their area of interest and expertise
  - Can leave provisioning and management of underlying infrastructure to the resource providers
  - Consume as much or as little resources as needed, when needed

An inherent benefit to IT service consumers is that the cloud is a consolidation of all the hardware, network, and software infrastructure they would otherwise be required to own to service their requirements. On the other hand, the cloud setup necessitates that IT service providers acquire an amount of adequately sized hardware resources, network components, and base software. However, the silver lining is that the provider can monitor resource usage and charge the consumer accordingly.

Cloud computing allows IT service providers to offer capabilities that may be far beyond each consumer's current reach by consolidating and sharing infrastructure across the needs and requirements of many consumers. Conversely, by servicing a wider group of consumers, the cloud service provider can offer a greater range and depth of resources by recouping the requisite IT infrastructure costs through metering and chargeback.

Why Implement a Cloud?

- Standardization
- Consolidation
- Centralization
- Optimization
- Abstraction
- Flexibility
- Self-service

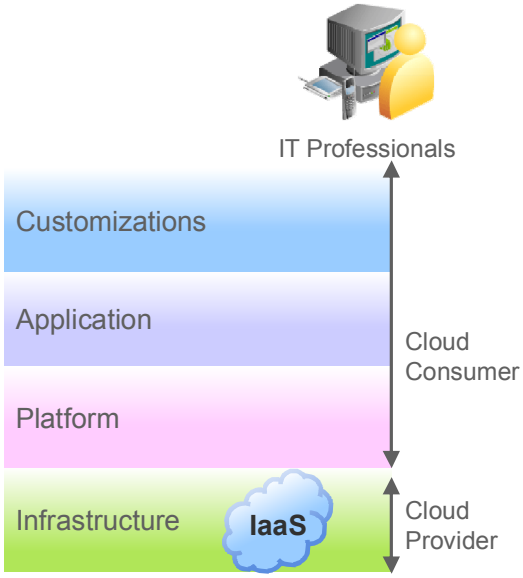
A Cloud Over Your Head Is Not Always Bad

The move to a computing cloud can be compelling for an organization on many fronts:

- Standardization
  - The cloud model naturally lends itself to the adoption of standards, including hardware, application platforms, and integration technologies.
- Consolidation
  - Combining physical infrastructure and IT budgets across multiple departments
  - More efficient purchasing, installation, maintenance, and operation processes
  - Reduced operational overhead with fewer physical pieces of infrastructure to manage
  - Potential gains per application deployment in terms of available compute resources
- Centralization
  - Consolidation may result in co-location of previously distributed infrastructure.
  - Operations may be simplified through the reduction of infrastructure.

- Optimization
  - Taking advantage of all available computing resources on any given server
  - Potential for reduced workload on operations or systems staff with fewer resources to manage
- Abstraction
  - The host and application platforms in a cloud deployment become an abstraction of physical servers with installed software, breaking ties to specific physical resources.
- Flexibility
  - As long as any service-level agreements that are in place are not breached, IT resources can be deployed and used in whatever configuration and manner as desired.
  - Applications can be deployed on any environments that meet their current resource needs.
- Self-service
  - Where suitable, you can allow end users (for example, developers) to request for resources and have the cloud management system provide the resources, thereby freeing system administrators and the operations teams from servicing such requests.
  - End users need to be concerned only with any quotas and other restrictions that may be imposed upon them, not with where they might be able to find the resources they need because these will be provided by the private cloud.

Cloud Service Models: IaaS



- Provider offers compute and storage resources, and O/S.
- Consumer provides everything else.
- Use cases:
  - Relocating existing workloads
  - Building highly customized platforms and applications

IaaS Cloud Service Model

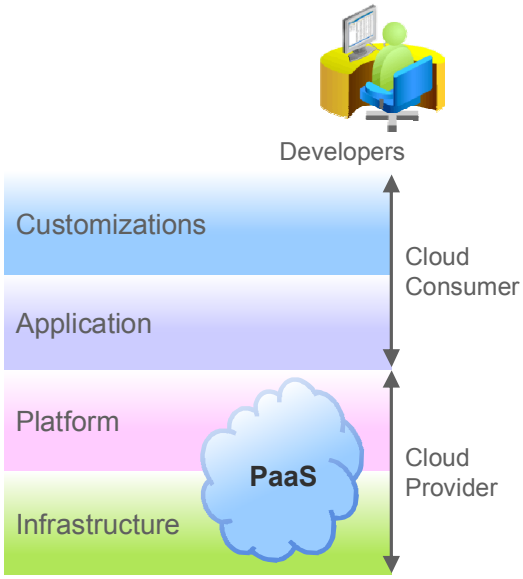
The three cloud service models defined by NIST (IaaS, PaaS, SaaS) are suited to different types of users due to the level of control each model allows for the cloud provider and the cloud consumer.

As a cloud consumer, you are attracted to the IaaS provider's cloud because you do not want to own and manage your own hardware but you do want to control everything from the operating system upwards. In the IaaS service model, cloud consumers use self-service to request compute, memory, and storage resources together with a base operating system. They then install application servers, databases, and other platforms, followed by the applications that they want along with the customizations they need.

An IaaS cloud may be suitable in a number of circumstances, such as the following:

- You want to divest yourself of the cost of purchasing and maintaining your own infrastructure.
- Your existing infrastructure is unable to meet the current or projected demands, and the IaaS cloud allows you to use as much computing power as you require.
- Your internal infrastructure requirements can be best met by consolidating your existing IT hardware into a private IaaS cloud.

Cloud Service Models: PaaS



- Provider offers a deployment platform.
- Consumer provides applications.
- Use cases:
  - Building highly customized applications on standard platforms
  - Running applications that you own on a scalable platform

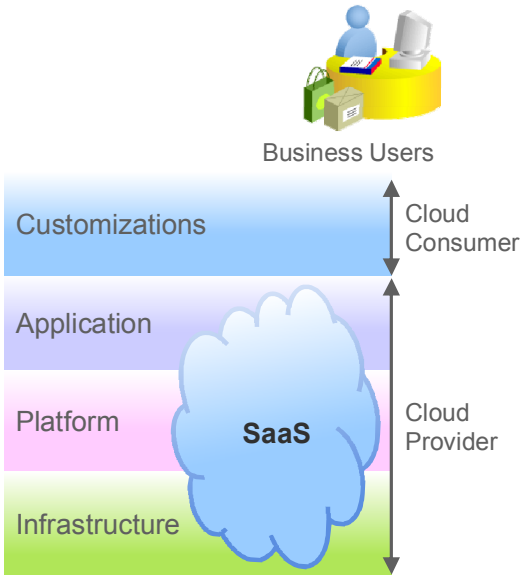
PaaS Cloud Service Model

As a cloud consumer, you are attracted to the PaaS provider's cloud because you want somewhere that you can deploy applications and start using them. You may be an application developer or a licensed application owner. In the PaaS service model, cloud consumers use self-service to request for a deployment platform such as an application server or database. They then install their applications on that platform and customize them to suit their needs.

A PaaS cloud may be suitable in a number of circumstances, such as the following:

- Your organization has the skills to build an application, but you do not want to invest in the underlying platform and computing resources. You also want the flexibility to scale your platform up or down as required.
- You own licenses for an application but do not want to invest and maintain the underlying platform and computing resources yourself.
- You are an IT development shop that specializes in J2EE and database applications, and a private PaaS cloud will allow you to consolidate existing resources and service the needs of all your development projects.

Cloud Service Models: SaaS



- Provider offers access to a running application.
- Consumer can customize as required.
- Use cases:
  - Implementing business processes without any IT acquisition
  - Building complex business flows with publicly available services

SaaS Cloud Service Model

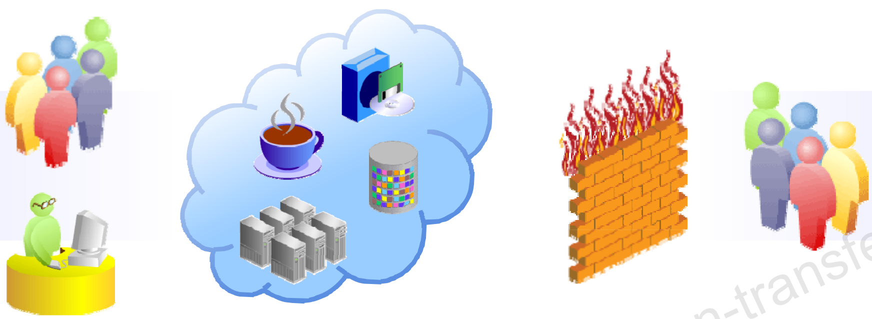
As a cloud consumer, you are attracted to the SaaS provider's cloud because you just want to use an application without owning the hardware or platform that it runs on, nor do you want to own software licenses. In the SaaS service model, cloud consumers use self-service to request access to an application such as Oracle Fusion Purchasing or Oracle Social Network that they can then customize to suit their needs.

A SaaS cloud may be suitable in a number of circumstances, such as the following:

- Your organization needs to implement a business process but cannot justify the cost of investing in and maintaining a technology stack and application licenses.
- Your organization uses the services of a number of SaaS providers and wants to link them together.
- Different departments within your organization generate unsynchronized fluctuating demand and a private SaaS cloud will allow you to consolidate and scale up or down across globally distributed data centers.

Deployment Models: Private Cloud

- This is used exclusively by one consumer.
- It can be hosted and managed internally or externally.
- Savings depend on the ability to exploit pooled resources, elasticity, and self-service automation.
- It is a simple model for the initial transition to cloud.



Private Cloud for Complete Peace of Mind

The private cloud deployment model dictates that the entire cloud is solely used by one cloud consumer, and this exclusivity can be traced to the underlying hardware that is being used to provide the cloud resources. A private cloud may be owned and operated by an organization from its own or a leased data center, or it may be owned, operated, and managed by a third party in an exclusive arrangement.

A primary advantage of an internal private cloud is the ability for the cloud consumer to control every aspect of the implementation, thereby ensuring compliance with security, naming, and other standards that may be key requirements of the consuming organization.

Deployment Models: Community Cloud

- Are used by consumers with common requirements, owners, or regulators
- Can be hosted and managed internally or externally
  - For example: Interrelated government organizations or a business conglomerate

Community Cloud for Shared Compliance

The community cloud deployment model is appropriate for multiple organizations with common security, privacy, and compliance considerations. Often these shared facets arise due to a common owner and a common regulator. A community cloud may be owned and operated by the community from its own or a leased data center, or it may be owned, operated, and managed by a third party.

Community clouds offer each member of the community the benefit of being able to share the costs of investing in and operating technologies and controls that may be required by rules and regulations.

Deployment Models: Public Cloud

- Available to the general public
- Hosted and managed by a cloud provider
- Transfer of costs that may motivate the move to the cloud
- Typically a pay-per-use or subscription basis

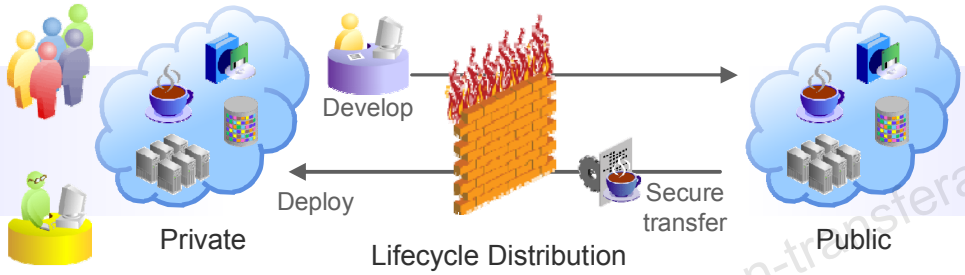
Public Cloud for General Access

The public cloud deployment model is appropriate for organizations or individuals wishing to avail themselves of computing or software resources without the associated costs and requirements of ownership and maintenance. A public cloud is owned by an organization selling cloud services. There is no exclusivity in the public cloud model—consumers have no control over whether the cloud resources they are using are shared with any other consumer, or even with which other consumers they are shared.

Public clouds relieve an individual organization of the burden of owning and maintaining computing and software resources, including the infrastructure and services required to operate a data center such as power, cooling, and lighting. Another potential benefit is the ability to operate a business in geographical locations that were previously untenable due to the cost of expanding the organization's network and general IT infrastructure—in the public cloud model, the onus of global accessibility falls on the shoulders of the cloud provider.

Deployment Models: Hybrid Cloud

- This is a combination of two or more private, community, or public clouds.
- The clouds remain distinct.
- Three use-cases exist:
  - Lifecycle distribution
  - Functional distribution
  - Workload distribution (also known as cloud bursting)



Hybrid Cloud for Total Flexibility

The hybrid cloud deployment model involves two or more private, community, or public clouds that are separate entities but are bound by common technologies. These common technologies allow applications to scale, migrate, or communicate between the clouds.

The three use-cases for implementing a hybrid cloud deployment model are:

- **Lifecycle distribution:** Your organization may be developing its own application, but does not wish to own and maintain a development environment, including the source code control system, development platform, and other development resources. An example of the hybrid cloud model would be using resources in a public cloud to develop and test code, which is then deployed to an internal private cloud where your production environment is running.
- **Functional distribution:** Your organization may have a business process, such as an insurance claim workflow, where some client interaction is unregulated but the regulatory or privacy compliance part of the process needs to be strictly controlled and monitored. The hybrid cloud model allows you to take advantage of the benefits of a public SaaS cloud, while ensuring regulatory compliance by protecting sensitive operations and information in your internal private cloud.

- **Workload distribution:** Also known as cloud bursting, workload distribution implies that the applications that you are using in a cloud model can be scaled across multiple clouds as required. You may have a business process such as an online store, which, for most of the year, is serviced by an internal private cloud, but during periods of peak demand needs to be supplemented with additional compute resources. By bursting to a public cloud to cater to peak demand, you can minimize your organization's investment in infrastructure, yet ensure that sales are maximized by servicing all customers to your site.

Cloud Type Formula

Service Host	Service Owner	Tenancy Model	Cloud Type
Enterprise	Enterprise	Single tenant	Private
Enterprise	Cloud provider	Single tenant	Managed private
Cloud provider	Cloud provider	Single tenant	Virtual private
Cloud provider	Cloud provider	Multiple tenants	Public
Any	Any	Community	Community
Any	Any	Any	Hybrid

Calculating the Cloud Type

With four basic cloud types to choose from, deciding which cloud type best meets your organization's needs requires thorough planning. One suggested approach is to start with a private cloud that will allow you to assess if your organization can realize the benefits of cloud computing. Choosing which cloud is best suited to your needs depends on three factors:

- **Service host:** Where will your cloud infrastructure be hosted? Internally in your own data center, in a leased data center, or in a cloud provider's data center? Regardless of the cloud service model you use (IaaS, PaaS, or SaaS), there is a need for basic computing resources (CPU, memory, and storage), as well as the supporting networking, power, lighting, cooling, and other elements that comprise a modern data center.
- **Service owner:** Regardless of where the cloud infrastructure is hosted, who will own the cloud service that you use? Will your organization set up its own cloud service or use that of a cloud provider? The service owner will also need to bear the costs of the entire infrastructure underpinning the cloud, as well as perform the role of a service operator and ensure that service-level agreements are met (for example).
- **Tenancy model:** Do your organization's regulatory and privacy needs dictate that you are the sole tenant of the cloud, or can you share the cloud with other consumers?

The result of combining a service host, a service owner, and a tenancy model is a type of cloud that will deliver the desired characteristics:

- **Private:** Your organization hosts the cloud infrastructure, owns and manages the cloud, and is the sole consumer of the cloud.
- **Managed private:** Your organization hosts the cloud infrastructure that may actually be rented from a cloud provider. A cloud provider owns and operates the cloud, but you are the sole consumer of the cloud.
- **Virtual private:** A cloud provider externally hosts, owns, and manages the cloud, but for exclusive use by your organization.
- **Public:** A cloud provider hosts, owns, and manages the cloud for multiple cloud consumers.
- **Community:** Regardless of where the cloud service is hosted or who owns it, the community cloud type is defined purely by the fact that a community of organizations is consuming the resources of the cloud.
- **Hybrid:** Being a combination of two or more clouds, the hybrid cloud is not defined by where the cloud is located, who owns and operates it, or who is using it.

From Zero to Cloud

- Adopting a cloud model:
  - Is a business transformation, not just another IT project
  - Affects people and processes, as well as technology
  - Must make life easier for administrators and end users
  - Must satisfy security and compliance requirements
  - Must be acceptable to management
- Consider starting with a private cloud before moving to any other cloud type.

ORACLE

Make Haste Not Speed

Adopting a cloud model will have ramifications far beyond the boundaries of your IT enterprise, and a successful transition to cloud depends on these being established and understood early in the move to the cloud. Although an IT enterprise may be the initial driver of the move to the cloud in any given organization, the ultimate benefactors should be the business system owners and users, and they should be considered at every decision point.

The cloud model introduces new behaviors and processes for your end users to adopt, and these changes should help rather than hinder the core activities of these people. Similarly, your system and software administrators must benefit from the changes introduced by adopting the cloud—introducing an IaaS private cloud where your system administrator now has to maintain the operating systems on hundreds, if not thousands of virtual machines, would not be seen as beneficial by the system administrator.

Regardless of the cloud model you choose to use, you cannot ignore or abandon the security and compliance requirements of both your IT enterprise and your business. IT security standards must continue to be observed, as should any compliance standards that you have in place for infrastructure and software configuration. Upholding business process security standards and regulatory compliance are also paramount to the success of any transformation to a cloud model.

Finally, your CIO and other upper management teams must find the cloud model an acceptable means of powering the business because they will most likely be the business sponsor of your cloud transformation project.

Managing Internal Stakeholders

- Enterprise architects
  - Want platform standardization in order to reduce the number of technologies
- Procurement managers
  - Want platform standardization in order to reduce the number of vendors
- Application owners
  - Want self-service in order to provision systems faster
- Chief Financial Officer
  - Wants a public cloud in order to move capital expenditure to operating expenditure
- Security and risk managers
  - Want an internal private cloud to preserve data security

Walking the Tightrope

When you embark on a cloud implementation project, you will find that different stakeholders perceive different benefits that can be derived from the ensuing transformation. Managing and meeting the expectations of your stakeholders may be challenging, but the success of a cloud implementation ultimately rests on its acceptance by the business sponsors. Therefore, you will need to work toward satisfying each of their needs.

There are quantifiable benefits in standardization, consolidation, and self-service automation. Conversely, there are quantifiable costs involved in moving any or all of your existing IT enterprise to a cloud model. You may find that it is a fine line between acceptance and rejection of a cloud model, and ultimately the benefits must outweigh the costs for you to transform your business.

To the Cloud or Not? Scenario 1

- A software development organization offers support from globally distributed centers to customers worldwide.
- Support engineers are constantly requesting extra hardware to create test environments.
- Customers are increasingly spread over various platforms and versions.
- Should the support group move to a cloud? If so, what type and why?

Ask Yourself …

Who are my stakeholders?

Who stands to benefit from a cloud?

What cloud service model would be best?

What cloud type would be best?

How could I sell my chosen cloud service model and type to my stakeholders?

To the Cloud or Not? Scenario 2

- A financial services company uses a third-party application that is always being customized with new product offerings.
- The cost of development licenses and maintaining the development environments is draining the IT budget.
- They want to move some development offshore but cannot justify the infrastructure expenditure.
- Should the development group move to a cloud? If so, what type and why?

ORACLE

Ask Yourself …

Who are my stakeholders?

Who stands to benefit from a cloud?

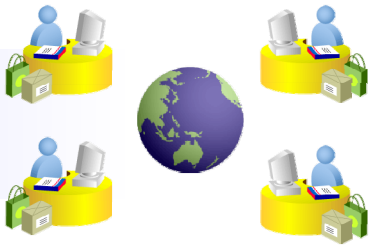
What cloud service model would be best?

What cloud type would be best?

How could I sell my chosen cloud service model and type to my stakeholders?

To the Cloud or Not? Scenario 3

- An online retailer has attracted more and more customers to its site through a number of marketing campaigns.
- Your next campaign will be 24 hours of exclusive deals.
- You are pretty sure that the online store can handle the load, and IT is putting a strain on your profits anyway.
- Should the online store move to a cloud? If so, what type and why?



ORACLE

Ask Yourself …

Who are my stakeholders?

Who stands to benefit from a cloud?

What cloud service model would be best?

What cloud type would be best?

How could I sell my chosen cloud service model and type to my stakeholders?