Oracle® E-Business Suite
Cloud Manager Guide
Release 20.2.1
Part No. F35809-06

May 2021
Contents

Send Us Your Comments

Preface

Part 1  Overview of Oracle E-Business Suite on Oracle Cloud Infrastructure

1  Introduction to Oracle E-Business Suite Cloud Manager

   Introduction .................................................................................................................. 1-1
   Features ................................................................................................................ ...... 1-1

Part 2  Implement Oracle E-Business Suite Cloud Manager

2  Deploy Oracle E-Business Suite Cloud Manager on Oracle Cloud Infrastructure

   Overview of Deploying Oracle E-Business Suite Cloud Manager .......................... 2-1
   Before You Begin ....................................................................................................... 2-2
   Create Oracle Cloud Infrastructure Accounts and Resources ............................ 2-5
   Create Network Resources for Deploying Oracle E-Business Suite Cloud Manager .... 2-12
   Create Oracle E-Business Suite Cloud Manager Compute Instance ...................... 2-28
   Configure Oracle E-Business Suite Cloud Manager Compute Instance ............. 2-30
   Update to Latest Version of Oracle E-Business Suite Cloud Manager .................. 2-41
   Obtain the CIDR for the Oracle Cloud Infrastructure SMTP Server .................. 2-41
   Oracle E-Business Suite Cloud Manager Deployment for Demo and Test Purposes ... 2-41
3 Set Up Your Tenancy to Host Oracle E-Business Suite Environments

Overview of Setting Up Your Tenancy to Host Oracle E-Business Suite Environments........3-1
Create or Identify a Compartment to Host Oracle E-Business Suite Environments..........3-3
Create the Oracle E-Business Suite Administrators Group and Assign Policies.............3-4
Create Users in Oracle Identity Cloud Service..........................................................3-8
Create Network Resources for Deploying Oracle E-Business Suite Environments.........3-9
Create Network Profiles.........................................................................................3-34

4 Manage the Oracle E-Business Suite Cloud Manager Virtual Machine

Overview of Managing the Oracle E-Business Suite Cloud Manager Virtual Machine.......4-1
Update Oracle E-Business Suite Cloud Manager to the Latest Version (Conditional).....4-1
Perform Oracle E-Business Suite Cloud Manager Administration Tasks.....................4-11
Manage Ksplice Uptrack Actions.............................................................................4-27

Part 3 Move On-Premises Oracle E-Business Suite Instances to Oracle Cloud Infrastructure

5 Create a Backup of an On-Premises Oracle E-Business Suite Instance on Oracle Cloud Infrastructure

Overview of Creating Backups...................................................................................5-1
Verify Prerequisites for Traditional Lift and Shift.....................................................5-3
Prepare the Source Oracle E-Business Suite Environment........................................5-10
Deploy Oracle E-Business Suite Cloud Manager......................................................5-12
Install the Oracle E-Business Suite Cloud Backup Module........................................5-12
Create an Advanced Configuration Parameters File (Optional).................................5-13
Create a Backup with the Oracle E-Business Suite Cloud Backup Module.................5-15
Troubleshoot Backup Issues......................................................................................5-26

6 Create a Standby Environment on Oracle Cloud Infrastructure from an On-Premises Oracle E-Business Suite Release 12.2 Instance with Oracle Database Release 12.1.0.2

Overview......................................................................................................................6-1
Requirements for Creating a Standby Environment.....................................................6-1
Preparations for Creating a Standby Environment.....................................................6-3
Install the Oracle E-Business Suite Cloud Backup Module.........................................6-7
Create a Standby Environment for Oracle Cloud Infrastructure from an On-Premises Environment..................................................................................6-7
Part 4  Manage Oracle E-Business Suite Instances Using Oracle E-Business Suite Cloud Manager

7  Access Oracle E-Business Suite Cloud Manager
   Overview of Accessing Oracle E-Business Suite Cloud Manager ........................................ 7-1
   Log In to Oracle E-Business Suite Cloud Manager ......................................................... 7-2
   Specify Your User Details (Conditionally Required) ....................................................... 7-2
   Check Oracle E-Business Suite Cloud Manager Version .................................................. 7-4
   Navigate within Oracle E-Business Suite Cloud Manager ............................................. 7-4
   Review Environments ........................................................................................................ 7-5

8  Configure Oracle E-Business Suite Cloud Manager Features
   Set Up Network Profiles .................................................................................................... 8-1
   Set Up the Extensibility Framework ............................................................................... 8-8
   Set Up Scheduling Policies ............................................................................................. 8-14

9  Provision an Oracle E-Business Suite Instance
   Requirements for Provisioning a New Environment ...................................................... 9-1
   One-Click Provisioning ..................................................................................................... 9-6
   Advanced Provisioning ..................................................................................................... 9-8
   Perform Post-Provisioning and Post-Cloning Tasks ...................................................... 9-24

10 Oracle E-Business Suite System Administration
    Oracle E-Business Suite System Administration ............................................................... 10-1
    Access Your Oracle E-Business Suite Environment ................................................... 10-1
    Access the Fusion Middleware Control and WebLogic Server Administration Console with
    SSH Port Forwarding for Oracle E-Business Suite on Oracle Cloud Infrastructure ........ 10-4
    Review Environment Details (Standard) ......................................................................... 10-6
    Review Standby Environment Details ........................................................................... 10-12

11 Oracle E-Business Suite Lifecycle Management
    Add and Delete Nodes ..................................................................................................... 11-1
    Clone an Oracle E-Business Suite Instance ................................................................... 11-5
    Back Up an Oracle E-Business Suite Instance .............................................................. 11-10
    Promote a Standby Environment .................................................................................... 11-21
    Delete an Oracle E-Business Suite Environment .......................................................... 11-26
12 Monitor Activity Status

Monitor Activity Status........................................................................................................... 12-1

A Tasks in the Extensibility Framework

Seeded Tasks in the Extensibility Framework......................................................................... A-1
Custom Task Scripts in the Extensibility Framework.............................................................. A-3
  Create a Wrapper Script...................................................................................................... A-4
  Test the Script................................................................................................................... A-20
  Package the Script in a Zip File........................................................................................ A-21

B Time Zone Support in Oracle E-Business Suite Cloud Manager

Time Zone Support in Oracle E-Business Suite Cloud Manager............................................. B-1
Send Us Your Comments

Oracle E-Business Suite Cloud Manager Guide, Release 20.2.1
Part No. F35809-06

Oracle welcomes customers' comments and suggestions on the quality and usefulness of this document. Your feedback is important, and helps us to best meet your needs as a user of our products. For example:

- Are the implementation steps correct and complete?
- Did you understand the context of the procedures?
- Did you find any errors in the information?
- Does the structure of the information help you with your tasks?
- Do you need different information or graphics? If so, where, and in what format?
- Are the examples correct? Do you need more examples?

If you find any errors or have any other suggestions for improvement, then please tell us your name, the name of the company who has licensed our products, the title and part number of the documentation and the chapter, section, and page number (if available).

Note: Before sending us your comments, you might like to check that you have the latest version of the document and if any concerns are already addressed. To do this, access the new Oracle E-Business Suite Release Online Documentation CD available on My Oracle Support and www.oracle.com. It contains the most current Documentation Library plus all documents revised or released recently.

Send your comments to us using the electronic mail address: appsdoc_us@oracle.com

Please give your name, address, electronic mail address, and telephone number (optional).

If you need assistance with Oracle software, then please contact your support representative or Oracle Support Services.

If you require training or instruction in using Oracle software, then please contact your Oracle local office and inquire about our Oracle University offerings. A list of Oracle offices is available on our Web site at www.oracle.com.
Preface

Intended Audience


This guide assumes you have a working knowledge of Oracle E-Business Suite system administration.

If you have never used Oracle E-Business Suite, we suggest you attend one or more of the Oracle E-Business Suite training classes available through Oracle University.

See Related Information Sources on page x for more Oracle E-Business Suite product information.

Documentation Accessibility

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

Access to Oracle Support

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

Structure

1 Introduction to Oracle E-Business Suite Cloud Manager
2 Deploy Oracle E-Business Suite Cloud Manager on Oracle Cloud Infrastructure
3 Set Up Your Tenancy to Host Oracle E-Business Suite Environments
4 Manage the Oracle E-Business Suite Cloud Manager Virtual Machine
5 Create a Backup of an On-Premises Oracle E-Business Suite Instance on Oracle Cloud
Infrastructure
6 Create a Standby Environment on Oracle Cloud Infrastructure from an On-Premises Oracle E-Business Suite Release 12.2 Instance with Oracle Database Release 12.1.0.2
7 Access Oracle E-Business Suite Cloud Manager
8 Configure Oracle E-Business Suite Cloud Manager Features
9 Provision an Oracle E-Business Suite Instance
10 Oracle E-Business Suite System Administration
11 Oracle E-Business Suite Lifecycle Management
12 Monitor Activity Status
A Tasks in the Extensibility Framework
B Time Zone Support in Oracle E-Business Suite Cloud Manager

Related Information Sources

This book is included in the Oracle E-Business Suite Documentation Library.

Online Documentation

All Oracle E-Business Suite documentation is available online (HTML or PDF).

- **Online Help** - Online help patches (HTML) are available on My Oracle Support.

- **Oracle E-Business Suite Documentation Library** - This library, which is included in the Oracle E-Business Suite software distribution, provides PDF documentation as of the time of each release.


- **Release Notes** - For information about changes in this release, including new features, known issues, and other details, see the release notes for the relevant product, available on My Oracle Support.


Related Guides

You should have the following related books on hand. Depending on the requirements of your particular installation, you may also need additional manuals or guides.

*Oracle Application Management Pack for Oracle E-Business Suite Guide*
This book is intended for database administrators and system administrators who are responsible for performing the tasks associated with maintaining an Oracle E-Business Suite system using the Oracle Application Management Pack for Oracle E-Business Suite.


This book lists the target metrics for Oracle E-Business Suite that Oracle Enterprise Manager monitors.

**Oracle Cloud Infrastructure Documentation**

This documentation describes how to use Oracle Cloud Infrastructure, a set of complementary cloud services that enable you to build and run a wide range of applications and services in a highly available hosted environment. In particular, see:

- Getting Started [https://docs.cloud.oracle.com/en-us/iaas/Content/GSG/Concepts/baremetalintro.htm]
- Developer Resources [https://docs.cloud.oracle.com/en-us/iaas/Content/devtoolshome.htm]

**Oracle E-Business Suite Concepts**

This book is intended for all those planning to deploy Oracle E-Business Suite Release 12.2, or contemplating significant changes to a configuration. After describing the Oracle E-Business Suite architecture and technology stack, it focuses on strategic topics, giving a broad outline of the actions needed to achieve a particular goal, plus the installation and configuration choices that may be available.

**Oracle E-Business Suite CRM System Administrator’s Guide**

This manual describes how to implement the CRM Technology Foundation (JTT) and use its System Administrator Console.

**Oracle E-Business Suite Installation Guide: Using Rapid Install**

This book describes how to run Rapid Install to perform a fresh installation of Oracle E-Business Suite Release 12.2 or to replace selected technology stack executables in an existing instance.

**Oracle E-Business Suite System Administrator’s Guide Documentation Set**

This documentation set provides planning and reference information for the Oracle E-Business Suite system administrator.

- For Oracle E-Business Suite Release 12.2, *Oracle E-Business Suite Setup Guide* contains information on system configuration tasks that are carried out either after installation or whenever there is a significant change to the system. The activities described include defining concurrent programs and managers, enabling Oracle Applications Manager features, and setting up printers and online help. *Oracle E-Business Suite Maintenance Guide* explains how to patch an Oracle E-Business Suite
system, describing the adopt patching utility and providing guidelines and tips for performing typical patching operations. It also describes maintenance strategies and tools that can help keep a system running smoothly. Oracle E-Business Suite Security Guide contains information on a comprehensive range of security-related topics, including access control, user management, function security, data security, secure configuration, and auditing. It also describes how Oracle E-Business Suite can be integrated into a single sign-on environment.


Oracle E-Business Suite User's Guide

This guide explains how to navigate products, enter and query data, and run concurrent requests by means of the user interfaces (UI) of Oracle E-Business Suite. It includes basic information on setting preferences and customizing the UI. An introduction to Oracle Enterprise Command Centers is also included. Lastly, this guide describes accessibility features and keyboard shortcuts for Oracle E-Business Suite.

Do Not Use Database Tools to Modify Oracle E-Business Suite Data

Oracle STRONGLY RECOMMENDS that you never use SQL*Plus, Oracle Data Browser, database triggers, or any other tool to modify Oracle E-Business Suite data unless otherwise instructed.

Oracle provides powerful tools you can use to create, store, change, retrieve, and maintain information in an Oracle database. But if you use Oracle tools such as SQL*Plus to modify Oracle E-Business Suite data, you risk destroying the integrity of your data and you lose the ability to audit changes to your data.

Because Oracle E-Business Suite tables are interrelated, any change you make using an Oracle E-Business Suite form can update many tables at once. But when you modify Oracle E-Business Suite data using anything other than Oracle E-Business Suite, you may change a row in one table without making corresponding changes in related tables. If your tables get out of synchronization with each other, you risk retrieving erroneous information and you risk unpredictable results throughout Oracle E-Business Suite.

When you use Oracle E-Business Suite to modify your data, Oracle E-Business Suite automatically checks that your changes are valid. Oracle E-Business Suite also keeps track of who changes information. If you enter information into database tables using
database tools, you may store invalid information. You also lose the ability to track who has changed your information because SQL*Plus and other database tools do not keep a record of changes.
Part 1

Overview of Oracle E-Business Suite on Oracle Cloud Infrastructure
This chapter covers the following topics:

- Introduction
- Features

**Introduction**

Oracle E-Business Suite Cloud Manager is a web-based application that drives all the principal automation flows for Oracle E-Business Suite on Oracle Cloud Infrastructure, including provisioning new environments, performing lifecycle activities on those environments, and restoring environments from on-premises.

Oracle E-Business Suite Cloud Manager was designed to simplify the diverse tasks Oracle E-Business Suite database administrators (DBAs) perform on a daily basis, with the goal of reducing the effort needed to perform them.

Oracle E-Business Suite Cloud Manager offers the following benefits:

- Security, with a load balancer that works as a TLS termination point.
- Deployment on a subnet that is not directly exposed to the user's network (internet or corporate intranet).
- The ability to allow multiple database administrators to manage the same set of Oracle E-Business Suite environments.
- Full integration with Oracle Identity Cloud Service for authentication services.

**Features**

This section describes available utilities and lists all key features delivered with the
automation for provisioning, lift and shift, and lifecycle management when running Oracle E-Business Suite on Oracle Cloud Infrastructure.

**Automation Tools**

**Oracle E-Business Suite Cloud Manager**

Oracle E-Business Suite Cloud Manager is a web application that provisions and manages Oracle E-Business Suite environments on Oracle Cloud Infrastructure. It is deployed as a virtual machine within the customer tenancy. Major capabilities include One-Click Provisioning, Advanced Provisioning, and Cloning.

**Oracle E-Business Suite Cloud Backup Module**

The Oracle E-Business Suite Cloud Backup Module is a standalone tool that interviews the user to establish settings, and then uses those settings to back up an Oracle E-Business Suite on-premises environment to Oracle Cloud Infrastructure Object Storage as part of a "traditional lift and shift".

**Oracle Applications Manager**

Oracle Applications Manager (OAM) is a web-based tool that supports managing and monitoring of an Oracle Applications system from an HTML-based central control console. You can run on-premises OAM and use the new Cloud Standby feature to create a standby environment in Oracle Cloud Infrastructure as part of a "reduced downtime lift and shift".

**Separation of Duties**

Oracle E-Business Suite Cloud Manager allows for differentiated roles between different personnel in your organization: network administrators, Oracle E-Business Suite Cloud Manager administrators, and Oracle E-Business Suite administrators (DBAs). These are achieved using the following constructs:

- **Multiple Compartments** - You have the option to create and use distinct compartments.

- **Groups** - Different groups of users can be assigned different roles.

- **Network Profiles** - You will define Network Profiles, which map compartments with Oracle Cloud Infrastructure network definitions to fulfill Oracle E-Business Suite network requirements. The use of predefined Network Profiles greatly simplifies provisioning for Oracle E-Business Suite Cloud Manager users (DBAs). When you create a network profile, you can optionally designate a regional subnet for your Oracle E-Business Suite application tier, database tier, or load balancer.
**One-Click Provisioning**

Oracle E-Business Suite Cloud Manager One-Click Provisioning is used to provision new demonstration environments in which the application tier and database tier reside on a single VM.

**Advanced Provisioning**

Oracle E-Business Suite Cloud Manager Advanced Provisioning can be used to provision an environment from object storage backups as well as to provision a new environment. Advanced Provisioning includes the following features:

- Selection of network topology.
- Support of both single availability domain and multiple availability domain regions.
- Choice of one or more application tiers.
- Choice of one or more internal and external zones.
- Placement of the database on one of the following: Compute, 1-Node VM DB System (Single Instance), 2-Node VM DB System (Oracle RAC), or Exadata Cloud Service.
- Ability to upload and deploy public SSH keys during provisioning to support secure shell access.
- Choice to deploy Load Balancer as a Service (LBaaS) or optionally configure your application tier node as the web entry point for your Oracle E-Business Suite environment.
- Configuration of your web entry point as the TLS termination point for the HTTP inbound connections to your Oracle E-Business Suite environment.
- Ability to define logical host names for the database tier and application tier nodes.

**Lift and Shift**

**Traditional Lift and Shift**

Oracle E-Business Suite Cloud Manager combined with the Oracle E-Business Suite Backup Module provide this lift and shift capability.

Lift and shift automations support an Oracle E-Business Suite Release 12.2.3 or later, or Release 12.1.3 installation (with Oracle Database 19c, 12.1.0.2, or 11.2.0.4) to Oracle Cloud Infrastructure and certified Oracle Database cloud services.
Reduced Downtime Lift and Shift

You can create a standby of your on-premises Oracle E-Business Suite installation in Oracle Cloud Infrastructure, and promote that standby to accomplish your lift and shift. This capability is currently available for Oracle E-Business Suite Release 12.2.3 or later with Oracle Database 12.1.0.2, with a target of Oracle Cloud Infrastructure Compute.

Database

Database Platforms

Automated provisioning and lift and shift utilities provide the option to run your database on the following platforms:

- Oracle Cloud Infrastructure Compute VM
- 1-Node VM DB System (Single Instance)
- 2-Node VM DB System (Oracle RAC)
- Exadata Cloud Service (Oracle RAC)

Note: In Release 20.2.1.1.1 and later, Oracle E-Business Suite Cloud Manager supports the new Exadata Cloud Service resource model and Exadata X8M.

Oracle E-Business Suite and Oracle Database with a Certified Quarterly Database Patch

This feature allows you to select a certified quarterly database bundle patch when using Oracle E-Business Suite Cloud Manager to:

- Provision a new environment
- Perform a lift and shift of an existing environment

Transparent Database Encryption

Transparent Data Encryption (TDE) is automatically enabled for environments provisioned using Oracle E-Business Suite Cloud Manager if the target database is on one of the following platforms:

- 1-Node VM DB System (Single Instance)
- 2-Node VM DB System (Oracle RAC)
- Exadata Cloud Service (Oracle RAC)
In addition, you have the option to enable TDE for environments provisioned on Compute.

**Compute Virtual Machines (VMs)**

Oracle E-Business Suite Cloud Manager Advanced Provisioning allows you to choose standard Intel 2.x and AMD E2.x shapes for your application tier, as well as for your database tier when it is deployed on a Compute VM.

For more information, see Virtual Machine Shapes [https://docs.cloud.oracle.com/en-us/iaas/Content/Compute/References/computeshapes.htm].

**Time Zone Support**

When conducting Oracle E-Business Suite Cloud Manager Advanced Provisioning, you can choose the operating system time zone for your destination servers, except in the case of Oracle Cloud Infrastructure Exadata Cloud Service. This feature is not available for Exadata Cloud Service because once an Exadata infrastructure resource is created, the infrastructure time zone cannot be changed.

Note that changing to a time zone different from the one used during your initial Oracle E-Business Suite implementation can cause data corruption, so you should use caution when choosing a different time zone.

For more information about the implementation of time zone support, see Time Zone Support in Oracle E-Business Suite Cloud Manager, page B-1.

**Fault Domains**

When using Oracle E-Business Suite Cloud Manager to provision, provision from a backup, or clone, all the deployed database tier and application tier nodes will be associated with a fault domain. You can choose the fault domains yourself or accept the defaults that are provided.

**Tagging**

Tags can be used to identify all resources associated with an environment or group of environments. When using Oracle E-Business Suite Cloud Manager to provision, provision from a backup, or clone, the Installation Details page allows you to choose a pre-defined tag or specify a new (free-form) tag.

**Lifecycle Management**

**Infrastructure Optimized Clone for Oracle E-Business Suite Environments**

The Oracle E-Business Suite Cloud Manager Cloning feature takes advantage of the native Block Volume Cloning capability in Oracle Cloud Infrastructure, and can be used
for environments deployed by Oracle E-Business Suite Cloud Manager where the
database and application tiers both reside on a Compute VM. It has the following
characteristics:

• The source system boot and block volume are cloned to create a new system,
preserving operating system and application updates during the clone.

• A single logical host name is used for the source and target systems, reducing the
time to clone.

• All block volumes attached to an instance are cloned. This is helpful when users
add additional block volumes to a provisioned instance to accommodate
customizations.

• You have the option to choose different shapes for the target.

Create a Backup

You can create backups of environments running Oracle Database 19c, 12.1.0.2, or
11.2.0.4 that were provisioned using Oracle E-Business Suite Cloud Manager Advanced
Provisioning. Note that these backups can then be used to provision a new environment
across any certified cloud service combination using the Advanced Provisioning
"Provision from Object Storage Backup" capability.

Define a Scheduling Policy for Backups

You can create backups for an Oracle E-Business Suite environment automatically on a
schedule by defining scheduling policies. These can be scheduled daily, weekly,
monthly, or yearly.

Add and Delete Nodes

A new horizontal scaling capability allows you to add and delete application tier nodes.
The Oracle E-Business Suite Cloud Manager reconfigures the system to operate with the
added or deleted node or nodes and, if you are using a load balancer, modifies the
backend set accordingly.

Delete an Environment

You have the option to delete environments created using Oracle E-Business Suite
Cloud Manager, whether from a new provisioning, a provisioning from a backup, or an
infrastructure optimized clone.

Delete a Backup

You have the option to delete object storage backups that were created using Oracle E-
Business Suite Cloud automation tools. This includes backups created using one of the
following two methods:
• By running the Oracle E-Business Suite Cloud Backup Module

• By utilizing the Oracle E-Business Suite Cloud Manager "Create Backup" feature

**Extensibility Framework**

Each major activity in Oracle E-Business Suite Cloud Manager, such as provisioning or cloning, consists of a set of phases and tasks defined in a driver file and run by a processing engine. You can review the status of each phase and task, as well as the overall activity.

The Extensibility Framework provides administrators the ability to add tasks to activities for Advanced Provisioning, cloning, and promoting a standby environment. Both seeded tasks and custom tasks are supported:

• A **seeded task** is a task that is provided with the automation. Examples are running AutoConfig on the application tier nodes, changing the system administrator password, or licensing products, but there are many others.

• A **custom task** is a task of your choosing, that can be called from a shell script. One example could be setting a profile option.

In addition, you can now insert pauses between phases as you choose, and resume the activity when desired. For example, you can insert a pause if you want to perform your own manual validations after a particular phase.

**Online Help**

Online help is available for key Oracle E-Business Suite Cloud Manager flows.
Part 2

Implement Oracle E-Business Suite Cloud Manager
Deploy Oracle E-Business Suite Cloud Manager on Oracle Cloud Infrastructure

This chapter covers the following topics:

• Overview of Deploying Oracle E-Business Suite Cloud Manager
• Before You Begin
• Create Oracle Cloud Infrastructure Accounts and Resources
• Create Network Resources for Deploying Oracle E-Business Suite Cloud Manager
• Create Oracle E-Business Suite Cloud Manager Compute Instance
• Configure Oracle E-Business Suite Cloud Manager Compute Instance
• Update to Latest Version of Oracle E-Business Suite Cloud Manager
• Obtain the CIDR for the Oracle Cloud Infrastructure SMTP Server
• Oracle E-Business Suite Cloud Manager Deployment for Demo and Test Purposes

Overview of Deploying Oracle E-Business Suite Cloud Manager

This chapter describes how to deploy Oracle E-Business Suite Cloud Manager version 20.2.1 on Oracle Cloud Infrastructure.

If you are performing a demo or are testing, you may be able to leverage the procedure provided in Oracle E-Business Suite Cloud Manager Deployment for Demo and Test Purposes, page 2-41 to simplify tenancy preparation, Oracle E-Business Suite Cloud Manager deployment and configuration by taking advantage of an Oracle Marketplace stack.

Note: If you have deployed a previous version of Oracle E-Business Suite Cloud Manager and wish to upgrade to the latest version, you do not need to perform the tasks in this chapter. Instead, follow the instructions described in Update Oracle E-Business Suite Cloud
Manager to Latest Version (Conditional), page 4-1. Oracle strongly recommends that you upgrade to the latest version at your earliest convenience. To continue to use an older version of Oracle E-Business Suite Cloud Manager for a limited period, refer to the documentation included in My Oracle Support Knowledge Document 2363536.1, Oracle E-Business Suite on Oracle Cloud Tutorial Archive [https://support.oracle.com/rs?type=doc&id=2363536.1].

Before you provision your Oracle E-Business Suite environments, you must follow the instructions in Set Up Your Tenancy to Host Oracle E-Business Suite Environments, page 3-1. Setting up the tenancy includes creating a compartment, groups, policies, users, and network resources to support a specific purpose. For example, the purpose could be to support a function (such as production, development or test), to support a region, or to create any other desired tenancy segmentation (such as a business unit).

Before You Begin

To follow the instructions in this chapter successfully, you will need either an Oracle Cloud Infrastructure tenancy enabled by Oracle Identity Cloud Service, or an Identity Cloud Service account that can be used to federate an existing Oracle Cloud Infrastructure tenancy that is not Identity Cloud Service-enabled. (Note that if your Oracle Cloud Infrastructure account was issued after 2017-12-20, it is already Oracle Identity Cloud Service-enabled.) The tenancy administrator will be required to create groups and users.

The following are four distinct categories of users referenced throughout this procedure and their roles:

- **Tenancy administrator** - Creates compartments, policies, groups, and users. The tenancy administrator also creates the identity provider (IDCS) group mapping to manage authentication.

In the example shown in the following diagram, the tenancy administrator creates four compartments, one for the cloud manager deployment itself, Oracle E-Business Suite instances production, test, and development. The tenancy administrator creates groups of users to serve as cloud manager administrators and Oracle E-Business Suite administrators for the production, test, and development environments in these compartments. Their access to these compartments is governed by the policies designed by the tenancy administrator.

These compartments will use network resources to be configured by the network administrator.
**Example Tenancy Configuration Performed by Tenancy Administrators**

- **Network administrator** - Designs the network and implements the network design with the following cloud resources:
  - VCNs
    - Subnets
  - Gateways
  - Routing tables
  - Security lists/groups
  - Security rules
  - FastConnect

As shown in the following diagram, the network administrators create VCNs in the network, one or more subnet for each VCN, and create the security lists and security rules for the subnets.
Example Network Configuration by Network Administrators

- **Oracle E-Business Suite Cloud Manager administrator** - Deploys the Oracle E-Business Suite Cloud Manager and defines the network profiles to map compartments and network resources. The Oracle E-Business Suite Cloud Manager administrator also leverages the compartments and network resources.

  As shown in the following diagram, the Oracle E-Business Suite Cloud Manager administrator deploys the Oracle E-Business Suite Cloud Manager in the designated compartment and defines network profiles for the production, test, and development compartments, mapping them to subnets and associated resources in the network.

Example Deployment and Network Profile Configuration by Oracle E-Business Suite Cloud Manager Administrators

- **Oracle E-Business Suite administrators** - Also known as application administrators or DBAs, they provision and maintain the Oracle E-Business Suite environments. The Oracle E-Business Suite administrators also leverage the network profiles that are defined.
In the following diagram, the Oracle E-Business Suite administrators provision Oracle E-Business Suite environments in the production, test, and development compartments, leveraging the network profiles to designate the network resources used by those environments.

**Example Provisioning and Management by Oracle E-Business Suite Administrators**

![Diagram showing Oracle E-Business Suite administrators provisioning environments in production, test, and development compartments.](image)

**Note:** If you wish, an Oracle E-Business Suite Cloud Manager administrator can also perform the duties of the network administrator and an Oracle E-Business Suite administrator. This is appropriate if you are configuring the system for demonstration use, or in any other circumstance where a single database administrator (DBA) will be performing all these roles. To accomplish this, you will make this user a member of the network administrators group and Oracle E-Business Suite administrators group.

**Note:** Ensure you perform all the applicable instructions in each section before proceeding to the next section.

### Create Oracle Cloud Infrastructure Accounts and Resources

In this section, the tenancy administrator performs all tasks as described.

1. Create Compartments, page 2-6

2. Create and Map Groups in Oracle Cloud Infrastructure Identity and Access Management and Oracle Identity Cloud Service, page 2-7

3. Assign Policies, page 2-9
4. Create Users, page 2-10

**Create Compartments:**
In this section, you will first map out your compartment topology and then create your compartment or compartments.

There are two types of compartments that we will refer to:

- **Cloud Manager Compartment** - Compartment that holds the Oracle E-Business Suite Cloud Manager Compute instance.

- **Network Compartment** - Compartment that holds network resources.

If you are giving a demonstration, you might choose to use one compartment for all components.

Oracle E-Business Suite Cloud Manager supports the use of nested compartments. The following depicts the compartment hierarchies that have been explicitly certified:

- The first certified hierarchy consists of one shared compartment under the root compartment for the EBS Cloud Manager, EBS environments, and the network.

- Another certified hierarchy consists of multiple shared compartments under the root compartment including one compartment for the EBS Cloud Manager and EBS environments, and another for the network.

- Another certified hierarchy consists of separate non-shared compartments for the EBS Cloud Manager, each EBS environment, and the network under the root compartment.

- The final certified hierarchy consists of separate non-shared compartments for the EBS Cloud Manager, each EBS environment, and the network within a subcompartment under the root compartment.

The following diagram depicts these compartment hierarchies:
To create each compartment, perform the following:

1. While signed in to the Oracle Cloud Infrastructure Service Console, click the menu icon at the top left to open the navigation menu.

2. Under Governance and Administration, select Identity, and then click Compartments.

3. On the Compartments page, click CreateCompartment.

4. In the dialog window, enter the required details:
   - NAME: Enter the compartment name (for example, network-compartment or ebscm-compartment).
   - DESCRIPTION: Enter a description of your choice.
   - PARENT COMPARTMENT: Select the root compartment under which the new compartment will be created.
   - Click Create Compartment at the bottom of the window.

Create and Map Groups in Oracle Cloud Infrastructure Identity and Access Management and Oracle Identity Cloud Service:

In this section, you will define two groups in Oracle Cloud Infrastructure Identity and Access Management (IAM) and Oracle Identity Cloud Service (IDCS):

- The network administrators group (for example, netadmin-grp).
- The Oracle E-Business Suite Cloud Manager administrators group (for example, ebscmadmin-grp). This group will be used to configure the Oracle E-Business Suite Cloud Manager Compute instance in Configure Oracle E-Business Suite Cloud.
Perform the following steps to create and map the two groups:

1. Open the Oracle Cloud Infrastructure console navigation menu. Under **Governance and Administration**, select **Identity**, and click **Groups**.

2. Create each of your groups as follows:
   1. Click **Create Group**.
   2. In the dialog window, enter the required details:
      - **NAME**: Enter the name for the group (for example, netadmin-grp and ebscmadmin-grp).
      - **DESCRIPTION**: Enter a description of your choice.
   3. Click **Create**.

3. Create each of your groups in Oracle Identity Cloud Service as follows:
   1. In the console navigation menu, under **Governance and Administration**, select **Identity**, and click **Federation**.
   2. Click on the name of the identity provider that corresponds to Oracle Identity Cloud Service (IDCS).
   3. On the left hand side under **Resources**, click **Groups**.
   4. Click **Create IDCS Group**.
   5. In the dialog window, enter the required details:
      - **NAME**: Supply a name for the group (for example, idcs-netadmin-grp and idcs-ebscmadmin-grp).
      - **DESCRIPTION**: Enter a description of your choice.
   6. Click **Create**.

4. Within the same page, map the groups in Oracle Identity Cloud Service as follows:
   1. Click **Group Mappings** on the left hand side.
   2. Click **Add Mappings**.
   3. In the dialog window, select the Identity Provider group and the corresponding Oracle Cloud Infrastructure group from the drop-down lists (for example, idcs-
netadmin-grp maps to netadmin-grp).

4. Click **Another Mapping** to add the second map (for example, idcs-ebscmadmin-grp maps to ebscmadmin-grp).

5. Click **Add Mappings**.

**Assign Policies:**
In this section, you will assign policies that allow for the proper permissions for administrators to manage and use the necessary compartments.

1. In the Console navigation menu, under **Governance and Administration**, select **Identity**, and then click **Policies**.

2. Create a policy for the network compartment to allow network administrators to manage it and for Oracle E-Business Suite Cloud Manager administrators to use it:
   1. Select the network compartment from the **COMPARTMENT** drop-down list on the left.
   2. Click **Create Policy**.

3. In the dialog window, enter the required details:
   - **NAME**: Enter a name (for example, networkcompartment-policy).
   - **DESCRIPTION**: Enter a description of your choice.
   - In the Policy Builder section, click **Customize (Advanced)**. In the provided text field, add each of the following policy statements, substituting appropriate values for the variables designated by angle brackets.
     
     Allow group <network administrators group> to manage virtual-network-family in compartment <network compartment>
     Allow group <Oracle E-Business Suite Cloud Manager administrators group> to use virtual-network-family in compartment <network compartment>

4. Click **Create**.

3. Create a policy for the Oracle E-Business Suite Cloud Manager compartment to allow Oracle E-Business Suite Cloud Manager administrators to perform operations on Oracle Cloud Infrastructure resources within it:
   1. Select the Cloud Manager compartment from the **COMPARTMENT** drop-down list on the left.
   2. Click **Create Policy**.
3. In the dialog window, enter the required details:
   - **NAME**: Enter a name (for example, ebscmcompartment-policy).
   - **DESCRIPTION**: Enter a description of your choice.
   - In the Policy Builder section, click **Customize (Advanced)**. In the provided text field, add each of the following policy statements, substituting appropriate values for the variables designated by angle brackets.

   Allow group <Oracle E-Business Suite Cloud Manager administrators group> to manage instance-family in compartment <Oracle E-Business Suite Cloud Manager compartment>
   Allow group <Oracle E-Business Suite Cloud Manager administrators group> to manage load-balancers in compartment <Oracle E-Business Suite Cloud Manager compartment>
   Allow group <Oracle E-Business Suite Cloud Manager administrators group> to manage tag-namespaces in compartment <Oracle E-Business Suite Cloud Manager compartment>

4. **Click Create Policy.**

4. Create a policy for the tenancy to allow network administrators and Oracle E-Business Suite Cloud Manager administrators to perform operations on Oracle Cloud Infrastructure resources within it:

1. Select the Cloud Manager compartment from the **COMPARTMENT drop-down list** on the left.

2. **Click Create Policy.**

3. In the dialog window, enter the required details:
   - **NAME**: Enter a name (for example, tenancy-policy).
   - **DESCRIPTION**: Enter a description of your choice.
   - In the Policy Builder section, click **Customize (Advanced)**. In the provided text field, add each of the following policy statements, substituting appropriate values for the variables designated by angle brackets.

   Allow group <network administrators group> to inspect compartments in tenancy
   Allow group <Oracle E-Business Suite Cloud Manager administrators group> to inspect compartments in tenancy
   Allow group <Oracle E-Business Suite Cloud Manager administrators group> to inspect users in tenancy
   Allow group <Oracle E-Business Suite Cloud Manager administrators group> to inspect groups in tenancy

4. **Click Create Policy.**
Create Users:

Create Federated Users
While logged on to the Oracle Cloud Infrastructure Service Console as the tenancy administrator, create each of your users as follows.

Repeat these steps for all users of your Oracle E-Business Suite Cloud Manager administrator group and network administrator group.

1. From the navigation menu, under Governance and Administration, select Identity Federation.

2. Click on the name of an Identity Provider of type IDCS.

3. On the left hand side under Resources, click Users.

4. Click Create User.

5. In the "Create IDCS User" dialog box, enter the following:
   • NAME: Enter a user name of your choice. This name must be in the format <firstname>.<lastname>@<domain>.
   • EMAIL: A valid email ID. Confirm this email in the following field.
   • FIRST NAME: First name of the user.
   • LAST NAME: Last name of the user.
   • GROUPS: Select the appropriate Oracle Identity Cloud Service group (for example, either idcs-netadmin-grp or idcs-ebscadmin-grp).

6. Click Create.

Create Non-Federated Users
While logged on to the Oracle Cloud Infrastructure Service Console as the tenancy administrator, create the Oracle E-Business Suite Cloud Manager administrator user as follows:

1. From the navigation menu, under Governance and Administration, select Identity, and then click Users.

2. Click Create User.

3. In the corresponding dialog box, supply the following:
   • NAME: Enter a user name of your choice. This user has to match the user you defined for the first Oracle E-Business Suite Cloud Manager administrator user.
The name must be in the format <firstname>.<lastname>@<domain>.

- **DESCRIPTION**: A description of your choice (for example, "This is the Oracle E-Business Suite Cloud Manager administrator").

- **EMAIL**: A valid email ID.

4. Click **Create**.

5. Generate the user’s password and provide it to the user, who will need it to perform tasks such as uploading API signing keys and generating SMTP credentials.

6. Add the Oracle E-Business Suite Cloud Manager administrator to the Oracle E-Business Suite Cloud Manager administrators group (ebscmadmin-grp in our example).

### Create Network Resources for Deploying Oracle E-Business Suite Cloud Manager

In this section, the network administrator performs all tasks as described.

First, you will create a new Virtual Cloud Network (VCN) using the steps in Create a Virtual Cloud Network, page 2-13.

Then dependent on the subnet you intend to use, you will create associated network resources (including gateways, route tables, security lists, and subnets) that will be used by your Oracle E-Business Suite Cloud Manager Compute instance: Create Network Resources for Use with Public Subnets, page 2-14 or Create Network Resources for Use with Private Subnets, page 2-19.

In a production environment, we strongly recommend you deploy a dedicated bastion server. This bastion server will be associated with a specific subnet that will be used as a bridge between the resources outside and inside Oracle Cloud Infrastructure. See Learn About Setting Up the Basic Infrastructure for a Cloud Environment [https://docs.oracle.com/en/solutions/set-resources-to-provision-deploy-cloud-environment/index.html#GUID-F647FBA1-C61C-4EA8-872C-AAB9DDA593DB] for more information about the architecture of the bastion server.

If you are evaluating Oracle E-Business Suite Cloud Manager, you can use the Cloud Manager VM as a bastion server to connect to the Oracle E-Business Suite environments that it creates.

The following table shows the subnet types supported for Oracle E-Business Suite Cloud Manager and the associated load balancer.
### Table 2-1: Subnet Types Supported for Oracle E-Business Suite Cloud Manager and Load Balancer

<table>
<thead>
<tr>
<th></th>
<th>Availability Domain-Specific Public</th>
<th>Availability Domain-Specific Private</th>
<th>Regional Public</th>
<th>Regional Private</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle E-Business Suite Cloud Manager</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Load balancer for Oracle E-Business Suite Cloud Manager</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Create a Virtual Cloud Network:

**Note:** If you have an existing Virtual Cloud Network you want to use, skip this section and proceed to Create Network Resources for Use with Public Subnets, page 2-14 if you intend to use public subnets. If you intend to use private subnets, proceed to Create Network Resources for Use with Private Subnets, page 2-19.

To create a new Virtual Cloud Network (VCN):

1. From the Oracle Cloud Infrastructure Service Console, click the menu icon at the top left to open the navigation menu. Under **CORE INFRASTRUCTURE**, go to **Networking** and click **Virtual Cloud Networks**.

2. Click **Create VCN** and enter the required details for your VCN:
   - **NAME**: Enter a name, such as `ebscm-vcn`.
   - **CREATE IN COMPARTMENT**: Select your network compartment, created in Create Compartments, page 2-6.
   - **CIDR BLOCK**: Specify your choice of CIDR (for example, 10.0.0.0/16).

   **Note:** When creating the VCN, accept the default DNS resolver. Oracle E-Business Suite provisioning in Oracle Cloud Infrastructure does not currently support a non-default DNS resolver VCN.

3. Click **Create VCN** at the bottom of the window.
Create Network Resources for Use with Public Subnets:

Note: If you want to use private subnets for Oracle E-Business Suite Cloud Manager and load balancer, skip this section and proceed to Create Network Resources for Use with Private Subnets, page 2-19.

Create an Internet Gateway

To create an internet gateway:

1. On the Virtual Cloud Networks screen, click the link with the name of your VCN, such as ebscm-vcn.

2. Under Resources on the navigation menu at the left, select Internet Gateways.

3. Click Create Internet Gateway and enter the required details for your internet gateway:
   - NAME: Enter a name, such as ebscm-igw.
   - CREATE IN COMPARTMENT: Select your network compartment, created in Create Compartments, page 2-6.

4. Click Create Internet Gateway at the bottom of the window.

Create Route Tables

In this section, you will create two separate route tables, one for the Oracle E-Business Suite Cloud Manager Compute instance and one for the load balancer. In the following examples, we will use the names ebscm-RouteTable and lbaas-RouteTable, respectively.

Perform these steps twice - once for the Oracle E-Business Suite Cloud Manager Compute instance route tables and once for the load balancer route tables.

To create the route tables:

1. On the Virtual Cloud Networks screen, click the link with the name of your VCN, such as ebscm-vcn.

2. Under Resources in the navigation menu at the left, select Route Tables.

3. Click Create Route Table and enter the required details for your route table:
   - NAME: Specify a name, such as ebscm-RouteTable or lbaas-RouteTable.
   - CREATE IN COMPARTMENT: Select your network compartment, created in Create Compartments, page 2-6.

4. Click + Another Route Rule and enter the route rule details as follows:
• **TARGET TYPE**: Select Internet Gateway.

• **DESTINATION CIDR BLOCK**: `0.0.0.0/0`

• **COMPARTMENT**: Select your network compartment, created in Create Compartments, page 2-6.

• **TARGET INTERNET GATEWAY**: Select the previously created gateway.

5. Click **Create Route Table** at the bottom of the window.

**Create Security Lists**
In this section, you will create two separate security lists, one for the Oracle E-Business Suite Cloud Manager Compute instance and one for the load balancer. In the following examples, we will use the names `ebscmvm-seclist` and `lbaas-seclist`, respectively.

**Create the Oracle E-Business Suite Cloud Manager Security List**

1. On the Virtual Cloud Networks screen, click the link with the name of your VCN, such as `ebscm-vcn`.

2. Under **Resources** in the navigation menu on the left, select **Security Lists**.

3. Click **Create Security List** and enter the required details for the security list:
   - **NAME**: Specify a name such as `ebscmvm-seclist`.
   - **CREATE IN COMPARTMENT**: Select your network compartment, created in Create Compartments, page 2-6.

4. Under **Allow Rules For Ingress**:
   1. Click **+ Another Ingress Rule**.

   2. For the first ingress rule that is needed, modify the default rule as follows:
      - **SOURCE TYPE**: CIDR
      - **SOURCE CIDR**: Enter the CIDR of your choice.
      - **IP PROTOCOL**: TCP
      - **SOURCE PORT RANGE**: All
      - **DESTINATION PORT RANGE**: 22

   3. For the second ingress rule that is needed, click **+ Another Ingress Rule** and enter the following values:
• **SOURCE TYPE**: CIDR

• **SOURCE CIDR**: 0.0.0.0/0

• **IP PROTOCOL**: ICMP

• **TYPE**: 3

• **CODE**: 4

4. For the third ingress rule that is needed, click **+ Another Ingress Rule** and enter the following values:

• **SOURCE TYPE**: CIDR

• **SOURCE CIDR**: Enter the CIDR of your LBaaS subnet, lbaas-subnet-ad1. For example, 10.0.1.0/24. Note that the subnet is created in the next step.

• **IP PROTOCOL**: TCP

• **SOURCE PORT RANGE**: All

• **DESTINATION PORT RANGE**: 8081

5. For the fourth ingress rule that is needed, click **+ Another Ingress Rule** and enter the following values:

   **Note**: Note that the fourth ingress rule is not required if a regional subnet is chosen for your public load balancer or if you are in a single availability domain region.

• **SOURCE TYPE**: CIDR

• **SOURCE CIDR**: Enter the CIDR of your LBaaS subnet, lbaas-subnet-ad2. For example, 10.0.1.0/24. Note that the subnet is created in the next step.

• **IP PROTOCOL**: TCP

• **SOURCE PORT RANGE**: All

• **DESTINATION PORT RANGE**: 8081

5. Under **Allow Rules For Egress**, click **+ Another Egress Rule** and modify the default rule as follows.

• **DESTINATION TYPE**: CIDR
- **DESTINATION CIDR**: 0.0.0.0/0
- **IP PROTOCOL**: TCP
- **SOURCE PORT RANGE**: All
- **DESTINATION PORT RANGE**: All

6. Click **Create Security List** at the bottom of the window.

**Create the Load Balancer Security List**

1. On the Virtual Cloud Networks screen, click the link with the name of your VCN, such as ebscm-vcn.

2. Under **Resources** in the navigation menu on the left, select **Security Lists**.

3. Click **Create Security List** and enter the required details of your security list:
   - **NAME**: Specify a name such as lbaas-seclist.
   - **CREATE IN COMPARTMENT**: Select your network compartment, created in Create Compartments, page 2-6.

4. Under **Allow Rules For Ingress**, click **+ Another Ingress Rule** and enter the following values for the ingress rule that is needed:
   - **SOURCE TYPE**: CIDR
   - **SOURCE CIDR**: Enter the CIDR corresponding to the IP addresses of your client machines that will access the Cloud Manager UI.
   - **IP PROTOCOL**: TCP
   - **SOURCE PORT RANGE**: All
   - **DESTINATION PORT RANGE**: 443 or other port of your choice. This port will be used in step 5 of Run Oracle E-Business Suite Cloud Manager Configure Script for the First Time, page 2-31, when prompting for the Load Balancer Listener Port.

5. Under **Allow Rules For Egress**, click **+ Another Egress Rule** and enter the following values for the egress rule that is needed:
   - **DESTINATION TYPE**: CIDR
   - **DESTINATION CIDR**: 0.0.0.0/0
• **IP PROTOCOL**: TCP

• **SOURCE PORT RANGE**: All

• **DESTINATION PORT RANGE**: All

6. Click **Create Security List** at the bottom of the window.

**Create Subnets**
In this section, you will create the following new subnets:

• One regional or availability domain-specific public subnet where the Oracle E-Business Suite Cloud Manager Compute instance will be created. This may be referred to as the "provisioning VM subnet."

• Either one or two subnets for creating the load balancer for the Oracle E-Business Suite Cloud Manager.
  
  • Create only one subnet for the load balancer if any of the following are true:
    
    • You are using a regional subnet.

    • You are in a single availability domain region.

  
  • Alternatively, if you choose to deploy using availability domain-specific subnets in a multiple availability domain region, you will create two subnets.

You will need to specify your own names and parameters, but you can use the examples in the following two tables for guidance.

If you choose to use regional subnets, refer to the following example:

<table>
<thead>
<tr>
<th>Subnet Name</th>
<th>CIDR Block</th>
<th>Route Table</th>
<th>Subnet Access</th>
<th>Security List</th>
</tr>
</thead>
<tbody>
<tr>
<td>ebscm-subnet-phx</td>
<td>10.0.0.0/24</td>
<td>ebscm-RouteTable</td>
<td>Public subnet</td>
<td>ebscmvm-seclist</td>
</tr>
<tr>
<td>lbaas-subnet-phx</td>
<td>10.0.1.0/24</td>
<td>lbaas-RouteTable</td>
<td>Public subnet</td>
<td>lbaas-seclist</td>
</tr>
</tbody>
</table>

If you choose to use availability domain-specific subnets, refer to the following example:
Table 2-3 - Availability Domain-Specific Public Subnet Example Names and Parameters

<table>
<thead>
<tr>
<th>Subnet Name</th>
<th>Availability Domain (AD)</th>
<th>CIDR Block</th>
<th>Route Table</th>
<th>Subnet Access</th>
<th>Security List</th>
</tr>
</thead>
<tbody>
<tr>
<td>ebscm-subnet-ad1</td>
<td>AD-1</td>
<td>10.0.0.0/24</td>
<td>ebscm-RouteTable</td>
<td>Public subnet</td>
<td>ebscmvm-seclist</td>
</tr>
<tr>
<td>lbaas-subnet-ad1</td>
<td>AD-1</td>
<td>10.0.1.0/24</td>
<td>lbaas-RouteTable</td>
<td>Public subnet</td>
<td>lbaas-seclist</td>
</tr>
<tr>
<td>lbaas-subnet-ad2</td>
<td>AD-2</td>
<td>10.0.2.0/24</td>
<td>lbaas-RouteTable</td>
<td>Public subnet</td>
<td>lbaas-seclist</td>
</tr>
</tbody>
</table>

To create a new subnet:

1. On the Virtual Cloud Networks screen, click the link with the name of your VCN, such as ebscm-vcn.

2. Under Resources in the navigation menu on the left, select Subnets.

3. Click Create Subnet, specifying your choice for the following parameters:
   - NAME
   - CREATE IN COMPARTMENT
   - SUBNET TYPE: Select either the Regional (Recommended) or Availability Domain-Specific option. If you choose Availability Domain-Specific, select your availability domain.
   - CIDR BLOCK
   - ROUTE TABLE COMPARTMENT IN <COMPARTMENT>: Ensure you choose a route table that has a target type of Internet Gateway.
   - SUBNET ACCESS: Select the Public Subnet option.
   - SECURITY LISTS: Select the security list that matches the subnet you are defining based on Table 3-3.

4. Click Create at the bottom of the window.

Create Network Resources for Use with Private Subnets:
When using private subnets, you could either:
• Define a DRG (Dynamic Routing Gateway [https://docs.cloud.oracle.com/en-us/iaas/Content/Network/Tasks/managingDRGs.htm]) to establish communication between your on-premises network and the VCN.

• Leverage a public subnet associated with a bastion server to access the VMs in the private subnet.

Create a Network Address Translation (NAT) Gateway
To create a Network Address Translation, or NAT, gateway, perform the following steps:

1. On the Virtual Cloud Networks screen, click the link with the name of your VCN, such as ebscm-vcn.

2. Under Resources in the navigation menu on the left, select NAT Gateways.

3. Click Create NAT Gateway and specify the following:
   • NAME: Enter a name, such as ebscm-natgw.
   • CREATE IN COMPARTMENT: Select your network compartment, created in Create Compartments, page 2-6.

4. Click Create NAT Gateway at the bottom of the window.

Create a Service Gateway
To create a service gateway, perform the following steps:

1. On the Virtual Cloud Networks screen, click the link with the name of your VCN, such as ebscm-vcn.

2. Under Resources in the navigation menu on the left, select Service Gateways.

3. Click Create Service Gateway and specify the following:
   • CREATE IN COMPARTMENT: Select your network compartment created in Create Compartments, page 2-6.
   • NAME: Enter a name, such as ebscm-srvgw.
   • Select “All <XXX> Services In Oracle Services Network” from the Services drop-down list. (Note that XXX is a region-specific code such as IAD or LHR.)

4. Click Create Service Gateway at the bottom of the window.

Create Route Tables
In this section, you will create two separate route tables, one for the Oracle E-Business
Suite Cloud Manager Compute instance and one for the load balancer. In the following examples, we will use the names ebscm-RouteTable and lbaas-RouteTable, respectively.

**Create the Route Table for Oracle E-Business Suite Cloud Manager Compute Instance**

1. On the Virtual Cloud Networks screen, click the link with the name of your VCN, such as ebscm-vcn.

2. Under **Resources** in the navigation menu on the left, select **Route Tables**.

3. Click **Create Route Table** and specify the following:
   - **CREATE IN COMPARTMENT**: Select your network compartment, created in Create Compartments, page 2-6.
   - **NAME**: Enter a name, such as ebscm-rtbl.

4. Click **+ Another Route Rule** and enter route rule details as follows:
   - **TARGET TYPE**: Select NAT Gateway.
   - **DESTINATION CIDR BLOCK**: 134.70.0.0/17 (Note that the 134.70.0.0/17 CIDR is required in order to connect to object storage.)
   - **COMPARTMENT**: Select your network compartment created in Create Compartments, page 2-6.
   - **TARGET NAT GATEWAY**: Select the previously created NAT gateway.

5. Click **+ Another Route Rule** and enter route rule details as follows:
   - **TARGET TYPE**: Select NAT Gateway.
   - **DESTINATION CIDR BLOCK**: CIDR for the Oracle Identity Cloud Service host being used (Note that the Oracle Identity Cloud Service host is of the format "idcs-xxxxxxxxxxxxxxxxx.identity.oraclecloud.com"). Use `nslookup` for getting the IP address of the Identity Cloud Service and derive the CIDR for the IP address to add the same here. In case the Oracle Identity Cloud Service CIDR changes, this rule must be updated as well.
   - **COMPARTMENT**: Select your network compartment created in Create Compartments, page 2-6.
   - **TARGET NAT GATEWAY**: Select the previously created NAT gateway.

6. Click **+ Another Route Rule** and enter route rule details as follows:
   - **TARGET TYPE**: Select Service Gateway.
• **DESTINATION CIDR BLOCK**: Select "All <XXX> Services In Oracle Services Network" (Note: XXX is a region-specific code such as IAD or LHR etc.)

• **COMPARTMENT**: Select your network compartment, created in Create Compartments, page 2-6.

• **TARGET SERVICE GATEWAY**: Select the previously created service gateway.

7. (Optional) If you are using the Oracle Cloud Infrastructure Mailer service, click + Another Route Rule and enter route rule details as follows:
   • **TARGET TYPE**: Select NAT Gateway.
   • **DESTINATION CIDR BLOCK**: The CIDR for the Oracle Cloud Infrastructure SMTP server being used (See Obtain the CIDR for the Oracle Cloud Infrastructure SMTP Server, page 2-41 for instructions on how to obtain this CIDR)
   • **COMPARTMENT**: Select your network compartment created in Create Compartments, page 2-6.
   • **TARGET NAT GATEWAY**: Select the previously created NAT gateway.

8. Click **Create Route Table** at the bottom of the window.

**Create the Route Table for Oracle E-Business Suite Cloud Manager Load Balancer**

For this route table for the load balancer, no route rules will be added to this route table as it will be used as a placeholder in case we need to define any additional route rules at a later time. Note that for communication within the VCN, no route rules are needed.

1. On the Virtual Cloud Networks screen, click the link with the name of your VCN, such as ebscm-vcn.

2. Under Resources in the navigation menu on the left, select **Route Tables**.

3. Click **Create Route Table** and specify the following:
   • **CREATE IN COMPARTMENT**: Select your network compartment created in Create Compartments, page 2-6.
   • **NAME**: Enter a name, such as ebscm-RouteTable.

4. Click **Create Route Table** at the bottom of the window.

**Create Security Lists**

In this section, you will create two separate security lists, one for the Oracle E-Business
Suite Cloud Manager Compute instance and one for the load balancer. In the following examples, we will use the names ebscmvm-seclist and lbaas-seclist, respectively.

**Create the Oracle E-Business Suite Cloud Manager Security List**

1. On the Virtual Cloud Networks screen, click the link with the name of your VCN, such as ebscm-vcn.

2. Under Resources in the navigation menu on the left, select Security Lists.

3. Click Create Security List and specify the following:
   - **CREATE IN COMPARTMENT**: Select your network compartment, as created in Create Compartments, page 2-6.
   - **NAME**: Specify a name such as ebscmvm-seclist.

4. Under Allow Rules for Ingress, click + Another Ingress Rule:
   1. For the first rule that is needed, modify the default rule as follows:
      - **SOURCE TYPE**: CIDR
      - **SOURCE CIDR**: The CIDR matching the IP address of the machine from which you plan to connect to Oracle E-Business Suite Cloud Manager, such as a bastion server.
      - **IP PROTOCOL**: TCP
      - **SOURCE PORT RANGE**: All
      - **DESTINATION PORT RANGE**: 22
   2. For the second rule that is needed, click + Another Ingress Rule and enter the following values:
      - **SOURCE TYPE**: CIDR
      - **SOURCE CIDR**: VCN CIDR
      - **IP PROTOCOL**: ICMP
      - **TYPE**: All
      - **CODE**: All
   3. For the third rule that is needed, click + Another Ingress Rule and enter the following values:
- **SOURCE TYPE**: CIDR
- **SOURCE CIDR**: Enter the CIDR of your LBaaS subnet, lbaas-subnet-ad1. For example, 10.0.1.0/24. Note that the subnet is created in the next step.
- **IP PROTOCOL**: TCP
- **SOURCE PORT RANGE**: All
- **DESTINATION PORT RANGE**: 8081

5. Under **Allow Rules For Egress**:
   1. Click **+ Another Egress Rule** and enter the following values:
      - **DESTINATION TYPE**: CIDR
      - **DESTINATION CIDR**: 134.70.0.0/17 (134.70.0.0/17 is required to connect to object storage.)
      - **IP PROTOCOL**: TCP
      - **SOURCE PORT RANGE**: All
      - **DESTINATION PORT RANGE**: All

   2. Click **+ Another Egress Rule** and enter the following values:
      - **DESTINATION TYPE**: CIDR
      - **DESTINATION CIDR**: CIDR for the Oracle Identity Cloud Service host being used
      - **IP PROTOCOL**: TCP
      - **SOURCE PORT RANGE**: All
      - **DESTINATION PORT RANGE**: 443

3. (Optional) If you are using the Oracle Cloud Infrastructure Mailer service, click **+ Another Egress Rule** and enter the following values:
   - **DESTINATION TYPE**: CIDR
   - **DESTINATION CIDR**: CIDR for the Oracle Cloud Infrastructure SMTP service being used (See Obtain the CIDR for the Oracle Cloud Infrastructure SMTP Server, page 2-41 for instructions on how to obtain this CIDR)
• **IP PROTOCOL**: TCP

• **SOURCE PORT RANGE**: All

• **DESTINATION PORT RANGE**: The SMTP server port you want to use (for example, 25 or 587)

4. Click **+ Another Egress Rule** and enter the following values:

   • **DESTINATION TYPE**: Service

   • **DESTINATION CIDR**: "All <XXX> Services In Oracle Services Network" (Note that XXX is a region-specific code, such as IAD or LHR.)

   • **IP PROTOCOL**: TCP

   • **SOURCE PORT RANGE**: All

   • **DESTINATION PORT RANGE**: All

5. Click **+ Another Egress Rule** and enter the following values:

   • **DESTINATION TYPE**: CIDR

   • **DESTINATION CIDR**: VCN CIDR

   • **IP PROTOCOL**: ICMP

   • **TYPE**: Leave this field blank.

   • **CODE**: Leave this field blank.

6. Click **Create Security List** at the bottom of the window.

**Create the Load Balancer Security List**

1. On the Virtual Cloud Networks screen, click the link with the name of your VCN, such as ebscm-vcn.

2. Under **Resources** in the navigation menu on the left, select **Security Lists**.

3. Click **Create Security List**:

   • **CREATE IN COMPARTMENT**: Select your network compartment created in Create Compartments, page 2-6.

   • **NAME**: Specify a name, such as lbaas-seclist.
4. Under **Allow Rules For Ingress**, click + **Another Ingress Rule** and enter the following values for the ingress rule that is needed:

   - **SOURCE TYPE**: CIDR
   - **SOURCE CIDR**: The CIDR matching the IP address of the machine from which you plan to connect to Oracle E-Business Suite Cloud Manager, such as a bastion server.
   - **IP PROTOCOL**: TCP
   - **SOURCE PORT RANGE**: All
   - **DESTINATION PORT RANGE**: 443 or other port of your choice. This port will be used in step 5 of Run Oracle E-Business Suite Cloud Manager Configure Script for the First Time, page 2-31, when prompting for the Load Balancer Listener Port.

5. Under **Allow Rules For Egress**, click + **Another Egress Rule** and enter the following values for the egress rule that is needed:

   - **DESTINATION TYPE**: CIDR
   - **DESTINATION CIDR**: The CIDR matching the private IP of the Oracle E-Business Suite Cloud Manager VM’s subnet.
   - **IP PROTOCOL**: TCP
   - **SOURCE PORT RANGE**: All
   - **DESTINATION PORT RANGE**: 8081

6. Click **Create Security List** at the bottom of the window.

**Create Subnets**

In this section, you will create the following new subnets:

- One regional or availability domain-specific public subnet where the Oracle E-Business Suite Cloud Manager Compute instance will be created. This may be referred to as the "provisioning VM subnet."

- One regional or availability domain-specific private subnet for creating the load balancer for the Oracle E-Business Suite Cloud Manager.

You will need to specify your own names and parameters, but you can use the examples in the following two tables for guidance.

If you choose to use regional subnets, refer to the following example:
Table 2-4 - Regional Private Subnet Example Names and Parameters

<table>
<thead>
<tr>
<th>Subnet Name</th>
<th>CIDR Block</th>
<th>Route Table</th>
<th>Subnet Access</th>
<th>Security List</th>
</tr>
</thead>
<tbody>
<tr>
<td>ebscm-subnet-phx</td>
<td>10.0.0.0/24</td>
<td>ebscm-RouteTable</td>
<td>Private subnet</td>
<td>ebscmvm-seclist</td>
</tr>
<tr>
<td>lbaas-subnet-phx</td>
<td>10.0.1.0/24</td>
<td>lbaas-RouteTable</td>
<td>Private subnet</td>
<td>lbaas-seclist</td>
</tr>
</tbody>
</table>

If you choose to use availability domain-specific subnets, refer to the following example:

Table 2-5 - Availability Domain-Specific Private Subnet Example Names and Parameters

<table>
<thead>
<tr>
<th>Subnet Name</th>
<th>Availability Domain (AD)</th>
<th>CIDR Block</th>
<th>Route Table</th>
<th>Subnet Access</th>
<th>Security List</th>
</tr>
</thead>
<tbody>
<tr>
<td>ebscm-subnet-ad1</td>
<td>AD-1</td>
<td>10.0.0.0/24</td>
<td>ebscm-RouteTable</td>
<td>Private subnet</td>
<td>ebscmvm-seclist</td>
</tr>
<tr>
<td>lbaas-subnet-ad1</td>
<td>AD-1</td>
<td>10.0.1.0/24</td>
<td>lbaas-RouteTable</td>
<td>Private subnet</td>
<td>lbaas-seclist</td>
</tr>
</tbody>
</table>

For each of the subnets you create, perform the following steps:

1. On the Virtual Cloud Networks screen, click the link with the name of your VCN, such as ebscm-vcn.
2. Under Resources in the navigation menu on the left, select Subnets.
3. Click Create Subnet, specifying your choice for the following parameters:
   - NAME
   - SUBNET TYPE: Select either Regional (Recommended) or Availability Domain-Specific. If you choose Availability Domain-Specific, select your availability domain.
   - CIDR BLOCK
   - ROUTE TABLE
   - SUBNET ACCESS: Select Private Subnet or Public Subnet for the subnet you wish to create.
• **SECURITY LIST**: Select the security list that matches the subnet you are defining based on Table 3-5.

4. Click **Create** at the bottom of the window.

---

**Create Oracle E-Business Suite Cloud Manager Compute Instance**

In this section, the Oracle E-Business Suite Cloud Manager administrator performs all tasks as described.

**Note**: Oracle E-Business Suite Deployment on Oracle Cloud Infrastructure in a hybrid DNS configuration always requires access to a VCN DNS resolver. If you are using such a configuration, ensure that IP address 169.254.169.254 is listed as a DNS server in the DHCP options. For more information, see Hybrid DNS Configuration [https://github.com/terraform-providers/terraform-provider-oci/blob/255817f83956f1f9a3ab903e11465e8b4dde1957/docs/examples/networking/hybrid_dns/Hybrid-DNS-configuration-using-DNS-VM-in-VCN.md].

Follow the steps in this section to create and connect to a Compute instance (created using an image in the Oracle Cloud Infrastructure Console Marketplace) that will be used to host Oracle E-Business Suite Cloud Manager.

1. Log in to the Oracle Cloud Infrastructure Service Console.
   1. In the menu on the left panel under the heading, click **Solutions and Platform**, then **Marketplace**, and then **Applications**.

   2. Then, click the Oracle E-Business Suite Cloud Manager image.

   3. In the **Version** drop-down list, ensure that the default of **Oracle-EBS-Cloud-Manager-20.2.1-<date>** is selected.

   4. Select the compartment where you plan to install Oracle E-Business Suite Cloud Manager. For example, ebscm-compartment.

   5. Review and accept the Terms of Use.

   6. Click **Launch Instance**.

2. In the Create Compute Instance dialog box, specify the following:

   1. Under **NAME**, enter your choice of name for your instance. For example, ebscm-instance.
2. In **CREATE IN COMPARTMENT**, choose your compartment for your instance in the drop-down list.

3. Under **Availability Domain**, make a suitable selection (based on the subnets you created previously) from the displayed options.

4. Under **Image**, you will see the name of the Oracle Cloud Infrastructure Console Marketplace image: **Oracle E-Business Suite Cloud Manager**.

5. Under **Shape**, select a suitable shape. To do so, click **Change Shape**. Then select your desired shape (for example, select Intel Skylake and then "VM.Standard 2.2").

6. Under **Configure Networking**:
   1. Click the "CHANGE COMPARTMENT" hyperlink to select the compartment where your VCN resides. For example, network-compartment.
   2. From the **Select a Virtual Cloud Network** drop-down list, choose your VCN. For example, ebscm-vcn.
   3. Under **Subnet Compartment**, click "Change Compartment", and select the compartment where your VCN resides. For example, network-compartment.
   4. Under **Subnet**, specify the Oracle E-Business Suite Cloud Manager subnet. For example, ebscm-subnet-ad1.
   5. If the VM is associated with a public subnet and you want to assign a public IP address, select the **ASSIGN A PUBLIC IPV4 ADDRESS** radio button.

7. Under **Add SSH Keys**, choose one of the following two options, either (1) or (2):
   1. Select the **CHOOSE PUBLIC KEY FILES** radio button, and then drag and drop or browse to specify the file containing your SSH public key generated previously.
   2. Alternatively, select the **PASTE PUBLIC KEYS** radio button and paste the SSH public key content in the text field provided, using the content of the public key generated previously.

8. Leave the values in the **Configure Boot Volume** section unselected in order to accept the default volume size.

3. Click the **Create** button at the bottom of screen.
4. After the instance has been created (provisioned), it will appear in the instance list. To view its full details, including IP addresses, click the instance name in the list.

5. When the Oracle E-Business Suite Cloud Manager instance is fully provisioned and running, you can connect to it by following the instructions in Connecting to an Instance [https://docs.cloud.oracle.com/en-us/iaas/Content/Compute/Tasks/accessinginstance.htm] in the Oracle Cloud Infrastructure Documentation.

Configure Oracle E-Business Suite Cloud Manager Compute Instance

In this section, the Oracle E-Business Suite Cloud Manager administrator and tenancy administrator perform all the tasks as described.

Follow the instructions in this section to configure your Oracle E-Business Suite Cloud Manager Compute instance. You will perform many of these operations from the Oracle Cloud Infrastructure Service Console.

- Configure Authentication API Keys, page 2-30
- Identify Credential Required for Configuration Scripts, page 2-31
- Run Oracle E-Business Suite Cloud Manager Configure Script For the First Time, page 2-31
- Register Oracle E-Business Suite Cloud Manager as a Confidential Application, page 2-36
- Run Oracle E-Business Suite Cloud Manager Configure Script For the Second Time, page 2-38
- Configure Oracle Cloud Infrastructure Email Delivery Service (Optional), page 2-40

Configure Authentication API Keys:

1. If you do not have one already, generate an API signing key and associated fingerprint that will be used by the configuration and networking scripts in subsequent sections. Oracle E-Business Suite Cloud Manager does not support API signing keys with passphrases, so you must generate an API signing key with no passphrase. Reference the Oracle Cloud Infrastructure Documentation site, following the instructions under "To Generate an API Signing Key Pair [https://docs.cloud.oracle.com/en-us/iaas/Content/API/Concepts/apisigningkey.htm#]".

2. Add the public key for the Oracle E-Business Suite Cloud Manager administrator user by performing the following steps:
1. Log in to the Oracle Cloud Infrastructure Service Console as the Oracle E-Business Suite Cloud Manager administrator user created previously in Create Users, page 2-10.

2. Click the user icon.

3. Select **User Settings** from the context menu.

4. Under **Resources** in the navigation menu on the left, click **API Keys**. Then, click **Add Public Key**.

5. Select the **Paste Public Keys** radio button.

6. Paste the contents of the API public key in the dialog box and click **Add**. The key's fingerprint is displayed.

7. Copy the Oracle Cloud Infrastructure API private PEM key file to the Oracle E-Business Suite Cloud Manager Compute instance. The file must be placed in a directory owned by the **oracle** user, for example `/u01/install/APPS/.oci`. The fully qualified path to the Oracle Cloud Infrastructure API private PEM key file will be needed for running `configure.pl` in Run Oracle E-Business Suite Cloud Manager Configure Script for the First Time, page 2-31.

### Identify Credential Required for Configuration Steps:

While still logged into the Oracle Cloud Infrastructure Service Console, identify and record the OCID of your tenancy. You will need to provide this credential when you run the Oracle E-Business Suite Cloud Manager `configure.pl` script.

1. From the navigation menu, under **Governance and Administration**, select **Administration**, then **Tenancy Details**.

2. Click **Copy** to copy the OCID of the tenancy into your clipboard, and record this value for use in the next section.

### Run Oracle E-Business Suite Cloud Manager Configure Script for the First Time:

The Oracle E-Business Suite Cloud Manager administrator performs the tasks in this section.

1. Connect to your Oracle E-Business Suite Cloud Manager Compute instance using SSH.

2. As the **oracle** user, run the `configure.pl` script:

   ```
   $ sudo su - oracle
   $ cd /u01/install/APPS/apps-unlimited-ebs/bin
   $ perl configure.pl
   ```
Note the creation of the session-specific log file, which will have the format shown in the following example:

Log File : /u01/install/APPS/apps-unlimited-ebs/out/configure_<date>_<time>.log

3. When prompted, enter an Oracle E-Business Suite Cloud Manager admin password and enter your user details required for authentication:

Specify New Oracle E-Business Suite Cloud Manager Admin Password :
Re-enter New Oracle E-Business Suite Cloud Manager Admin Password :

Enter Oracle E-Business Suite Cloud Manager User OCID : ocid1.user.oc1..xxxxx
Enter Absolute Path to API Private Signing Key : /u01/install/APPS/.oci/oci_api_key.pem
Enter Tenancy OCID : ocid1.tenancy.oc1..xxxxx

Note: The password should contain at least one of these special characters: _ (underscore), # (hash), or $ (dollar). This password is used by the Oracle E-Business Suite Cloud Manager administrator to connect to the Cloud Manager database, and to run subsequent scripts.

4. You will now be prompted for the Oracle E-Business Suite Cloud Manager Administrator Group. This example shows a group called ebscmadmin-grp being selected from the list of available choices.

Available Groups from OCI for provided User:

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: ebsdbdev-grp</td>
<td>EBS Dev DBA Group</td>
</tr>
<tr>
<td>2: ebscmadmin-grp</td>
<td>EBS Cloud Manager Admin Group</td>
</tr>
<tr>
<td>3: ebsdemodb-grp</td>
<td>EBS Test DBA Group</td>
</tr>
<tr>
<td>4: ebsqa-grp</td>
<td>EBS QA DBA Group</td>
</tr>
</tbody>
</table>

Choose E-Business Suite Cloud Administrator Group from above list: 2

5. You will now be asked if you wish to use an existing load balancer:

Do you wish to use an existing load balancer?

1: Yes
2: No

Enter your choice: 1

If you choose option 1 (Yes), you will be asked to choose a load balancer from a list such as shown in this example. Note that the available load balancers reside in the same VCN and the same compartment as the Oracle E-Business Suite Cloud Manager VM.
Available Load Balancers

1: demolbaas1
2: demolbaas2

Choose a load balancer from the above list: 1

Otherwise, if you choose option 2 (No), and therefore wish to create a new load balancer, you will need to choose a load balancer visibility type, shape, and the subnets in which to place the load balancer. Example screens are shown as follows.

- Choose the load balancer visibility type:

  Choose Load Balancer Visibility Type:

  1: Public
  2: Private

  Enter your choice: 1

  Select option 1 (Public) or option 2 (Private) for the load balancer visibility type.

- Load balancer shape:

  1: 100Mbps
  2: 400Mbps
  3: 8000Mbps

  Choose Load Balancer Shape from above list: 1

- Subnets in which to place the load balancer (as defined in Create Network Resources for Use with Public Subnets, page 2-14 or Create Network Resources for Use with Private Subnets, page 2-19):

  Available List of Subnets

  Regional (recommended):
  -----------------------------
  1: lbaas-subnet-phx
  Availability Domain: CQI1:PHX-AD-1
  -----------------------------
  2: lbaas-subnet-ad1
  Availability Domain: CQI1:PHX-AD-2
  -----------------------------
  3: lbaas-subnet-ad2
  4: othersubnet1
  Availability Domain: CQI1:PHX-AD-3
  -----------------------------
  5: othersubnet2
  6: othersubnet3
  7: othersubnet4

  Choose subnet from above list: 1

  - If you are in a single availability domain region, your screen will show only two subnet groupings, one for
regional subnets and one for your single availability domain.

- When creating a public load balancer, only public subnets are listed.

If you are in a multiple availability domain region and you choose an availability domain-specific public subnet (options 2 to 7 in the previous example), and not a regional subnet (option 1 in the previous example), you will be prompted for a second availability domain-specific subnet for the HA load balancer, as shown.

Choose AD Specific HA subnet from above list: 6

- When prompted, enter the load balancer listener port:
  Enter Load Balancer Listener Port: 443

- When prompted, enter the CIDR range information to access the load balancer port:
  Enter CIDR Block (Range) from which Client can Access Load Balancer Listener Port: 192.0.2.0/24

6. Review the summary screen containing the information you specified earlier for the Oracle E-Business Suite Cloud Manager.
Deploy Oracle E-Business Suite Cloud Manager on Oracle Cloud Infrastructure

-------------------
Summary of Inputs
-------------------

Oracle E-Business Suite Cloud Manager User Name (Non Federated) : 
xxxx.xxxxx@example.com
Oracle E-Business Suite Cloud Manager User OCID (Non Federated) : 
ocid1.user.oc1..xxxxxxxxxxx
Path to Private PEM key file : /u01/install/APPS/.oci/oci_api_key.pem
Tenancy OCID : ocid1.tenancy.oc1..xxxxxxxxxxxxxx
Oracle E-Business Suite Cloud Manager VM Compartment Name : ebscm-compartment
Oracle E-Business Suite Cloud Manager VM Compartment OCID : ocid1.compartment.oc1..xxxxxxxxxxxxxx
Oracle E-Business Suite Cloud Administrator Group Name : ebscmadmin-grp
Oracle E-Business Suite Cloud Administrator Group OCID : ocid1.group.oc1..xxxxxxxxxxxxxxx
Network Compartment Name : network-compartment
Network Compartment OCID : ocid1.compartment.oc1..xxxxxxxxxxxxxxx
Network VCN Name : ebscm-vcn
Network VCN OCID : ocid1.vcn.oc1.phx-subnet.xxxxxxxxxxxxxx
Use an existing Load Balancer : false
Load Balancer Listener Port : 443
CIDR Block (Range) from which Client can Access Load Balancer Listener Port : 192.0.2.0/24
Load Balancer Visibility Type : Public
Load Balancer Shape : 100Mbps
Load Balancer Subnet Name : Public
Regional Subnet Load Balancer Subnet OCID : ocid1.subnet.oc1.phx-subnet1.xxxxxxxxxxxxxx
Load Balancer Subnet CIDR : 10.0.3.16/28

Do you wish to continue?

1: Yes
2: No

Enter your choice: 1

If you are satisfied with the values shown, enter option 1 to proceed.

7. You will then see a screen containing a success message, similar to the following example, plus the load balancer URL you will need later.
Register Oracle E-Business Suite Cloud Manager as a Confidential Application:
In this section, you will register the Oracle E-Business Suite Cloud Manager as a confidential application.

Grant the Oracle Identity Cloud Service Application Administrator Role to the Cloud Manager Administrator
As a tenancy administrator, grant the Oracle Identity Cloud Service application administrator role to the Oracle E-Business Suite Cloud Manager administrator user (created in Create Users, page 2-10).

1. From the Oracle Cloud Infrastructure console navigation menu, select Identity, and then Federation.

2. Click on the identity provider.

3. Click on the link for the Oracle Identity Cloud Service console.

4. Within the Oracle Identity Cloud Service console, click on the menu and navigate to Security, then click on Administrators.

5. Scroll down to the Application Administrator section and expand it. Within this section, perform the following:
   1. Click + Add.
   2. In the Add Users to the Administrator Role dialog window, select the user created previously created in Create Users, page 2-10.
   3. Click OK.


Register the Application
1. Open the Welcome email that was received as a result of your user created in
2. Click **Activate Your Account** in the email.

3. Enter a new password, confirm, and click **Submit**.

4. Navigate to the My Services dashboard at `https://myservices-<your tenancy name>.console.oraclecloud.com/mycloud/cloudportal/dashboard` and click **Sign In**.

5. Click your user avatar menu in the top right corner. This will display a drop-down menu.

6. Select **My Home** from the drop-down menu to display the My Oracle Services page.

7. On the My Oracle Services page, search and click **Admin Console**. This will display the Oracle Identity Cloud Service Administration Console.

8. In the top right of the Applications tile, click the icon to Add an Application.

9. Select **Confidential Application**. This takes you to the Add Confidential Application page.

10. Under Details, enter the following:
    - **Name**: Enter a name such as Oracle E-Business Suite Cloud Manager.
    - **Description**: Enter a description.

11. Click **Next**.

12. Under Client:
    1. Select **Configure this application as a client now**.
    2. Under **Allowed Grant Types**, select the following options:
       - **Client Credentials**
       - **Refresh Token**
       - **Authorization Code**

       Additionally, if you plan to create standby environments or to upgrade environments from Oracle E-Business Suite Release 12.1 to Release 12.2, select the **Resource Owner** option.

    3. **Redirect URL**: This is the load balancer URL from step 7 of Run Oracle E-Business Suite Cloud Manager Configure Script for the First Time, page 2-31 in
the following format: <Your Load Balancer URL>/cm/auth/callback.
For example: https://xxxx.xxx.xxx.xxx:xxxx/cm/auth/callback

4. **Logout URL**: Leave this field empty.

5. **Post-Logout Redirect URL**: <Your Load Balancer URL>/cm/ui/index.
   html?root=login. For example: https://xxxx.xxx.xxx.xxx:
   xxx/cm/ui/index.html?root=login

6. Select the **Introspect** option for Allowed Operations.

7. Grant the client access to Identity Cloud Service Admin APIs:
   1. Click **Add**.
   2. Select **Authenticator Client and Me**.
   3. Click **Add** again, and then click **Next**.

13. Under Resources, click **Next**.

14. Under Authorization, click **Finish**.

15. Make a note of the following values when they are displayed:
   - **Client ID**
   - **Client Secret**

16. Click **Activate** to activate the Confidential Application.

17. Record your Oracle Identity Cloud Service Client Tenant value. This can be seen as
   part of the URL in your browser’s address bar, after the "//" and before ".
   identity.oraclecloud.com". It begins with the characters "idcs-", followed
   by a string of numbers and letters in the format idcs-
   xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx. Copy the value for use in the next
   section.

**Run Oracle E-Business Suite Cloud Manager Configure Script for the
Second Time:**

1. Connect to your Oracle E-Business Suite Cloud Manager Compute instance using
   SSH.

2. As the `oracle` user, run the `configure.pl` script again:
   ```
   $ sudo su - oracle
   $ cd /u01/install/APPS/apps-unlimited-ebs/bin
   $ perl configure.pl
   ```
Note the creation of the session-specific log file, which will have the format shown in the following example:

Log File : /u01/install/APPS/apps-unlimited-ebs/out/configure_2019-07-11_10_02_09.log

3. When prompted, enter the Oracle E-Business Suite Cloud Manager administrator password and your Oracle Identity Cloud Service application details, as shown in the following example. The values you will need to enter for client ID and client secret were established when you registered the Oracle E-Business Suite Cloud Manager as a confidential application in Register Oracle E-Business Suite Cloud Manager as a Confidential Application, page 2-36.

Enter Oracle E-Business Suite Cloud Manager Admin Password :

Enter IDCS Client ID : <client id> (in a format similar to xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)
Enter IDCS Client Secret : <client secret> (in a format similar to xxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx)
Enter IDCS Client Tenant : <client tenant> (in a format similar to idcs-xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

4. You will see a summary screen containing the information you specified earlier:

--------------------------------------------------------------------
-------------------
Summary of Inputs
-------------------
--------------------------------------------------------------------

Enter IDCS Client ID : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Enter IDCS Client Secret : xxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Enter IDCS Client Tenant : client tenant
IDCS Host : https://idcs-xxxxxxxxxxxxxxxxxxxxxxxxxxxxx.identity.oraclecloud.com

--------------------------------------------------------------------
-------------------
Do you wish to continue?
1: Yes
2: No

Enter your choice: 1
Choose option 1 to continue.

5. A Login URL is then displayed on the screen, as shown in the following example. This is the URL by which users will access the Oracle E-Business Suite Cloud Manager UI.
Creating EBS Tagging Infrastructure.
Implicit Namespace created.
Implicit Tag key created.

====================================================================
Finished Configuring Oracle E-Business Suite Cloud Manager VM.
Login URL : https://xxx.xxx.xxx.xxx
Ensure the confidential application is correctly configured in IDCS
as per the documentation.
====================================================================

Note:
• If you wish to update the URL by which users will access the
  Oracle E-Business Suite Cloud Manager UI, you can do so
  using your own DNS registered host name and certificate by
  following the instructions described in "Update Oracle E-
  Business Suite Cloud Manager URL" in Managing the Oracle E-
  Business Suite Cloud Manager Virtual Machine, page 4-1.

• Oracle E-Business Suite resources will be tagged with "oracle-
  apps.purpose:EBS"

Configure Oracle Cloud Infrastructure Email Delivery Service (Optional):
This section provides instructions on how to set up the Oracle Cloud Infrastructure
Email Delivery Service to send notifications.

Steps to Perform Prior to Enabling Mailer
Before enabling the mailer, you must perform these steps:

1. Generate SMTP credentials by following the instructions in Generate SMTP
   Credentials for a User [https://docs.cloud.oracle.com/en-
   us/iaas/Content/Email/Tasks/generatesmtpcredentials.htm?tocpath=Services%7CEmail%20Delivery%7C___1] in the Oracle Cloud Infrastructure
   Documentation.

2. Create an Approved Sender by following the instructions in Managing Approved
   Senders [https://docs.cloud.oracle.com/en-
   us/iaas/Content/Email/Tasks/managingapprovedsenders.htm] in the Oracle Cloud
   Infrastructure Documentation.

Enable and Disable the Mailer
In order to enable and disable the mailer, use the command provided in Enable Mailer
Configuration, page 4-21 and Disable Mailer Configuration, page 4-21.
Update to Latest Version of Oracle E-Business Suite Cloud Manager

To obtain the latest fixes, update to version 20.2.1 by following the instructions in Update Oracle E-Business Suite Cloud Manager to the Latest Version (Conditional), page 4-1.

Obtain the CIDR for the Oracle Cloud Infrastructure SMTP Server

There are certain points within the deployment process in which you must provide the CIDR for the Oracle Cloud Infrastructure SMTP server. In order to obtain this CIDR, perform the following steps:

1. See Configure SMTP Connection [https://docs.cloud.oracle.com/en-us/iaas/Content/Email/Tasks/configuresmtconnection.htm] for the list of SMTP endpoints. Contact your tenancy administrator to determine the SMTP endpoint being used.

2. Run `nslookup` on the endpoint. For example:
   ```bash
   $ nslookup smtp.us-phoenix-1.oraclecloud.com
   ```

3. The resulting output will be the public IP address for the SMTP endpoint. The CIDR for the IP address obtained will be `<IP address>/32`. For example: 138.1.38.16/32.

Oracle E-Business Suite Cloud Manager Deployment for Demo and Test Purposes

You can leverage the procedure provided in this section to simplify tenancy preparation, Oracle E-Business Suite Cloud Manager deployment, and configuration by taking advantage of available automation. Doing so will streamline portions of the procedure documented in this chapter, as well as the instructions in Set Up Your Tenancy to Host Oracle E-Business Suite Environments, page 3-1.

This simplified procedure is most appropriate for demo purposes, as it has the following restrictions:

- The automation deploys a new VCN and subnets for the Oracle E-Business Suite Cloud Manager, load balancers, and the first set of Oracle E-Business Suite environments. The subnets are public regional subnets.

- The automation creates a new compartment for all the assets. An existing compartment cannot be used, and multiple compartments are not supported.
Identify or Create a Tenancy and Obtain Tenancy Administrator User Credentials:

If you have an existing tenancy, you must have a user with tenancy administrator privileges to run this procedure.

If you do not have an existing tenancy, you can sign up for a free trial account using the following steps:

1. From your laptop, go to https://www.oracle.com/cloud/free/ and click Start for free.

2. On the Oracle Cloud Sign Up page, enter the requested information including your desired tenancy name and tenancy password.

3. Review your details and click Submit.

   **Note:** Ensure that you use the same email address that was used when you registered.

You will be directed to the Oracle Cloud Infrastructure console where you will perform the remainder of the procedure.

4. Record your trial user name and password for future reference.

Set Up Oracle E-Business Suite Cloud Manager Authentication with Identity Cloud Service (IDCS):

Create the Oracle E-Business Suite Cloud Manager Administrator's Group and User in Oracle Identity Cloud Service

1. As the tenancy administrator, log in to the Oracle Cloud Infrastructure console.

2. In the Oracle Cloud Infrastructure console menu under Governance and Administration, select Identify, and then select Federation.

3. Click on the link next to Oracle Identity Cloud Service console.

4. From the Oracle Identity Cloud Service console, create your Oracle E-Business Suite Cloud Manager group:

   1. Click the navigation menu and select Groups.

   2. Click Add.

   3. In the Add Group dialog box under Step 1: Group Details, enter the following information:

      • **Name:** Enter the group name (for example, idcs-ebscm-group).
• **Description**: Enter a description of your choice.

4. Click **Finish**.

5. While still in the Oracle Identity Cloud Service console, create your Oracle E-Business Suite Cloud Manager administrator user.

1. Click the navigation menu and select **Users**.

2. Click **Add**.

3. In the Add User dialog box under Step 1: Add User Details, enter the following information:
   - **First Name**: Enter the first name of the new user.
   - **Last Name**: Enter the last name of the new user.
   - **User Name**: Enter the user name. (For example, `ebscm.admin@example.com`. Ensure the user name has "." in its name, as per our example.).
   - **Email**: Enter the email of the new user.
   - Deselect the Use email address as the user name check box.

4. Click **Next**.

5. In the Step 2: Assign User to Groups dialog window, select the check box for the group you just created (such as `idcs-ebscm-grp`).

6. Click **Finish**.

6. From the Oracle Identity Cloud Service console navigation menu, click **Security** to expand the menu. Then click **Administrators**.

7. On the Administrators page, expand the Application Administrators section and click **Add**.

8. In the Add Users to the Administrator Role dialog box, select the check box for the user corresponding to the newly created user in step 5 (in this example, that would be `ebscm.admin@example.com`).

9. Click **OK**.

10. Log out of the Oracle Identity Cloud Service console by clicking on your user avatar icon at the top right of your screen and then click **Sign Out**.
Register Oracle E-Business Suite Cloud Manager as a Confidential Application in IDCS

Now, register the Oracle E-Business Suite Cloud Manager as a confidential application.

1. Open the Welcome email that was received in the previous section.

2. Click **Activate Your Account** in the email.

3. Enter a new password, confirm, and click **Submit**.

4. Click **OK** to continue, which will take you to the Oracle Identity Cloud Service Login screen.

5. Enter the Oracle E-Business Suite Cloud Manager user name (for example, ebscm.admin@example.com) and password you just entered in the previous screen to log in.

6. Click on your user avatar menu in the top right corner. This will display a drop-down menu.

7. Select **Admin Console**. This will display the Oracle Identity Cloud Service Administration Console.

8. In the top right of the Applications tile, click the icon to **Add an Application**.

9. Select **Confidential Application**. This takes you to the Add Confidential Application page.

10. On the Details screen, enter the following:
    - **Name**: Enter Oracle E-Business Suite Cloud Manager.
    - **Description**: Enter a description.

11. Click **Next**.

12. On the Client screen:
    1. Select **Configure this application as a client now**.
    2. Under Allowed Grant Types, select the following check boxes:
        - **Resource Owner**
        - **Client Credentials**
        - **Refresh Token**
• **Authorization Code**

Additionally, if you plan to create standby environments or to upgrade environments from Oracle E-Business Suite Release 12.1 to Release 12.2, select the **Resource Owner** option.

3. **Redirect URL:** \https://<Cloud-Manager-web-entry>:443/cm/auth/callback\, where \(<Cloud-Manager-web-entry>\) is the name you plan to associate with your load balancer IP address. (For example, myebscm.example.com). This name resolution has to be configured in your DNS or in the local hosts file, as per instructions in Log in to Oracle E-Business Suite Cloud Manager, page 2-48.

4. **Logout URL:** Leave this field empty.

5. **Post-Logout Redirect URL:** \https://<Cloud-Manager-web-entry>:443/cm/ui/index.html?root=login\, where \(<Cloud-Manager-web-entry>\) is the name you plan to associate with your load balancer IP address. (For example, myebscm.example.com). This name resolution has to be configured in your DNS or in the local hosts file, as per instructions in Log in to Oracle E-Business Suite Cloud Manager, page 2-48.

6. Select the **Introspect** option for Allowed Operations.

7. Under Grant the client access to Identity Cloud Service Admin APIs:
   1. Click **Add**.
   2. Select **Authenticator Client and Me** in the pop-up window.
   3. Click **Add** again.

8. Click **Next**.

13. On the Resources screen, click **Next**.

14. On the Web Tier Policy screen, click **Next**.

15. On the Authorization screen, click **Finish**.

16. Make note of the following values which will be used in the next section:
   - **Client ID**
   - **Client Secret**

17. Click **Close**.
18. Click **Activate** to activate the Confidential Application.

19. Click on the avatar icon the top right hand side of the screen.

20. Select the **About** option.

21. Make a note of the Instance GUID. Your Oracle Identity Cloud Service Client Tenant begins with the characters idcs- and then is followed by a string of numbers and letters. (For example, idcs-6572bfeb183b4becad9e649bfa14a488.)

**Oracle E-Business Suite Cloud Manager Deployment and Configuration:**
In this section you will deploy and configure an Oracle E-Business Suite Cloud Manager Compute instance using an Oracle Marketplace stack.

**Sign in to the Oracle Cloud Infrastructure Console**
Use the tenancy administrator credentials to sign in to Oracle Cloud Infrastructure console.

Sign in to the Oracle Cloud Infrastructure console using the following:

- **User Name:** Tenancy Admin User
- **Password:** Tenancy Admin Password

**Deploy and Configure Oracle E-Business Suite Cloud Manager**
You will now deploy and configure the Oracle E-Business Suite Cloud Manager using a Marketplace stack. The stack creates the following cloud resources:

- A compartment to contain resources required by Oracle E-Business Suite Cloud Manager

- An Oracle E-Business Suite Cloud Manager Administrators IAM (Identity and Access Management) user and group, as well as the policies required to manage the compartment

- Network resources - including a VCN, an internet gateway, subnets, route tables, security lists, and security rules

- A Compute instance for running the Oracle E-Business Suite Cloud Manager

Then, the stack will configure Oracle E-Business Suite Cloud Manager to work with your Oracle Cloud Infrastructure tenancy and the newly created Oracle Cloud Infrastructure resources.

Perform the following steps:

1. **Log in to the Oracle Cloud Infrastructure Service Console.**
1. In the menu on the left panel under the heading, click **Solutions and Platform**, then click **Marketplace**, and then click **Applications**.

2. Then, click **Oracle E-Business Suite Cloud Manager Stack for Demos**.

3. In the **Version** drop-down list, ensure that the default of **Oracle-EBS-Cloud-Manager-RM-20.1.1-2020.08.20** is selected.

4. In the **Compartment** drop-down list, select the parent compartment of the compartment where the Oracle E-Business Suite Cloud Manager Compute instance will be deployed. For example, mycompanytenancy(root).

5. Review and accept the Terms of Use.

6. Click **Launch Instance**.

2. On the Configure Variables screen, enter the following values:

   1. **Resource Prefix**: A prefix that will be added to names of all the cloud resources created by the stack.

   2. Leave the **Single Compartment Setup** check box selected.

   3. Select the compartment under which the new compartment will be created.

   4. Enter the user name corresponding to the EBS Cloud Administrator created in step 5 of Create the Oracle E-Business Suite Cloud Manager Administrator’s Group and User in Oracle Identity Cloud Service, page 2-42.

   5. Make sure the **Create New REST API** key check box is selected.

   6. Enter the web entry fully qualified domain name you entered that corresponds to the Cloud-Manager-web-entry element you entered in step 12 of Register Oracle E-Business Suite Cloud Manager as a Confidential Application in Oracle Identity Cloud Service, page 2-44.

   7. Select **VM.Standard.E2.2** for EBS Cloud Manager Shape.

   8. Enter a password which matches the following criteria: 8 to 30 characters, at least one lower character, one upper case character, one special character from _#$.

   9. Enter the contents of a public key file that will be used to connect using SSH to your Oracle E-Business Suite Cloud Manager Compute instance. For more details on how to generate the key, see Creating a Key Pair in the Oracle Cloud Infrastructure Documentation.
10. Choose the availability domain that ends in -1 from the list under EBS Cloud Manager Availability Domain.

11. Leave the Custom CIDR Ranges check box deselected.

12. Enter a CIDR block that corresponds to the IP range of the clients you plan to use to connect to the Oracle E-Business Suite Cloud Manager. For the whole internet, use 0.0.0.0/0.

13. Enter the values corresponding to Client ID, Client Secret, and IDCS Client Tenant from Register Oracle E-Business Suite Cloud Manager as a Confidential Application in Oracle Identity Cloud Service, page 2-44.

3. On the Review screen, verify the information and click Create.

4. This takes you to the Stack Details page for your newly created stack. On this page, click the Terraform Actions drop-down list and select Apply.

5. In the Apply dialog window, leave the default settings as-is and click Apply.

6. On the Job Details page, you will see the job status which will cycle through Accepted, In Progress, and Succeeded. After the job succeeds, you will have all the network resources (VCN, load balancer, subnets, and so on) required to deploy the Oracle E-Business Suite Cloud Manager Compute instance.

7. On the Application Information tab are details related to the Oracle E-Business Suite Cloud Manager instance and load balancer.

   Make a note of the Private IP, Public IP, Login URL, and LB Public IP. These variables are needed for the remainder of the procedures in this section.

**Ensure You are on the Latest Cloud Manager Version**

Check to make sure you are on the latest cloud manager version by following the instructions in Update Oracle E-Business Suite Cloud Manager to the Latest Version (Conditional), page 4-1.

**Log in to Oracle E-Business Suite Cloud Manager**

Before logging in to the Oracle E-Business Suite Cloud Manager web application, you need to add the host name in the Login URL to your local computer hosts file. Follow these instructions to perform this configuration:

1. Edit the local hosts file on your laptop and add an entry.

   **For Windows Users**

   1. Navigate to Notepad in your start menu.
2. Hover over Notepad, right-click, and select the option "Run as Administrator."

3. In Notepad, click File, then click Open.

4. Browse to C:\Windows\System32\drivers\etc.

5. Find the file hosts.

6. In the hosts file, scroll down to the end of the content.

7. Add the following entry to the very end of the file:
   
   `<LB Public IP> <Cloud-Manager-web-entry>`

8. Save the file.

2. Using the Login URL found in the Application Information tab, log into the Oracle E-Business Suite Cloud Manager using your Oracle Identity Cloud Service credentials.
   
   Once logged in, you are on the Environments page.
Set Up Your Tenancy to Host Oracle E-Business Suite Environments

This chapter covers the following topics:

• Overview of Setting Up Your Tenancy to Host Oracle E-Business Suite Environments
• Create or Identify a Compartment to Host Oracle E-Business Suite Environments
• Create the Oracle E-Business Suite Administrators Group and Assign Policies
• Create Users in Oracle Identity Cloud Service
• Create Network Resources for Deploying Oracle E-Business Suite Environments
• Create Network Profiles

Overview of Setting Up Your Tenancy to Host Oracle E-Business Suite Environments

This chapter describes how to define a new compartment and create related cloud resources in order to prepare Oracle Cloud Infrastructure tenancy for deploying a new set of Oracle E-Business Suite environments managed by a new group of Oracle E-Business Suite administrators (DBAs) using Oracle E-Business Suite Cloud Manager 19.2.1 or later.

The companion chapter, Deploy Oracle E-Business Suite Cloud Manager on Oracle Cloud Infrastructure, page 2-1, leads you through the process of deploying Oracle E-Business Suite Cloud Manager along with the compartments and resources that it requires. You must first complete the applicable steps in the companion chapter mentioned earlier before performing the tasks in this chapter.

Note: This chapter is not applicable to Oracle E-Business Suite Cloud Manager releases prior to version 19.2.1. Oracle strongly recommends upgrading Oracle E-Business Suite Cloud Manager to the latest version.
at your earliest convenience. To upgrade Oracle E-Business Suite Cloud Manager, follow the instructions in Update Oracle E-Business Suite Cloud Manager to Latest Version (Conditional), page 4-1.

If you need to continue to use an older version of Oracle E-Business Suite Cloud Manager for a limited period, refer to the documentation listed in My Oracle Support Knowledge Document 2363536.1, Oracle E-Business Suite on Oracle Cloud Tutorial Archive [https://support.oracle.com/rs?type=doc&id=2363536.1].

Before using Oracle E-Business Suite Cloud Manager to provision a new set of environments (for example, for production usage), you must prepare the tenancy by identifying or creating a new network compartment and creating a new group, users, and corresponding policies to organize and control access to that compartment.

You can create additional compartments to implement separation of duties, such as separate compartments to administer production and development environments.

The following diagram depicts the relationship between the different categories of users and the compartments that could be defined in your tenancy. In this example, three compartments are defined: Production, Development, and Network. Each compartment has a separate group of administrators associated with it: the Application Administrators Production group for the production compartment, defined by the Production Network Profile; the Application Administrators Development group for the development compartment, defined by the Development Network Profile; and the Network Administrators group for the network compartment.

**Separation of Duties Implemented with Compartments and Groups**

You may choose to define a new network compartment, or use the one that was defined while deploying the Oracle E-Business Suite Cloud Manager. This chapter assumes that the network compartment (called network-compartment in our example) that hosts the network resources is already in place. The production compartment is used as an example to explain how to prepare a tenancy specifically for the users of Oracle E-
Business Suite production environments through the following steps:

1. Identify or create the new compartment in Oracle Cloud Infrastructure, which we call ebsprod-compartment in this example.

2. Create the Oracle Identity and Access Management (IAM) group that will operate on the ebsprod-compartment compartment.

3. Create the Oracle Identity Cloud Service (IDCS) group and map it to Oracle Identity and Access Management in order to federate the authentication.

4. Create policies that allow the Oracle Identity and Access Management group to manage resources in the ebsprod-compartment compartment.

5. Create users in the Oracle Identity Cloud Service Admin Console and make them members of the Oracle Identity Cloud Service group created previously in step 3.


7. Create a new network profile in Oracle E-Business Suite Cloud Manager that maps the ebsprod-compartment compartment and the network you just defined.

Note that Oracle E-Business Suite administrators are referenced throughout this chapter. They can access the Oracle E-Business Suite Cloud Manager user interface (UI) to provision environments and conduct lifecycle management activities. These users are usually referred to as Oracle E-Business Suite DBAs.

Create or Identify a Compartment to Host Oracle E-Business Suite Environments

When preparing the tenancy to deploy your Oracle E-Business Suite production instances, first you will determine which compartment will host the compute VMs or database services and load balancer that make up your environments. You can use an existing compartment (shared compartment) or create a new compartment (non-shared compartment), as described in this section. See Deploy Oracle E-Business Suite Cloud Manager on Oracle Cloud Infrastructure, page 2-1 for diagrams outlining some compartment topology examples.

- **Shared Compartment** - You may have already established a compartment which holds the Oracle E-Business Suite Cloud Manager Compute instance, network resources, and other Oracle E-Business Suite environments. You can choose this same compartment (for instance, demo-compartment) to host your new set of environments as well.

A shared compartment is appropriate for smaller deployments or for demonstration use.
• **Non-Shared Compartment**: Oracle E-Business Suite environments and network resources are deployed in separate compartments.

Hosting your new environments in a separate (non-shared) compartment allows you to clearly separate Oracle E-Business Suite environment resources. This would allow you to use the Oracle Cloud Infrastructure Service Console to view the resource utilization for this new set of environments.

This topology option is chosen in this document to guide you through the deployment of Oracle E-Business Suite environments. A separate network compartment (called network-compartment) has already been created. You will create a new compartment (called ebsprod-compartment in this section) for hosting Oracle E-Business Suite environments.

**Note:** All these topology options can be used in nested compartments. However, in a non-shared scenario, the compartments cannot be children of each other.

To create a compartment called ebsprod-compartment for hosting the Oracle E-Business Suite Production environments:

1. In the Oracle Cloud Infrastructure Service console navigation menu, under Governance and Administration, select Identity, and click Compartments.

2. On the Compartments page, click Create Compartment.

3. In the dialog window, enter the required details:
   - **NAME**: Enter the compartment name. (For example, ebsprod-compartment)
   - **DESCRIPTION**: Enter a description of your choice.

4. Click Create Compartment at the bottom of the window.

For information on creating compartments and related policies for network resources and Oracle E-Business Suite Cloud Manager, see Deploy Oracle E-Business Suite Cloud Manager on Oracle Cloud Infrastructure, page 2-1.

---

**Create the Oracle E-Business Suite Administrators Group and Assign Policies**

In this section, you will define a group of Oracle E-Business Suite administrators that will operate on the new compartment that you previously created and assign the required policies to allow the group to manage resources in the new compartment. Throughout the examples in this chapter, we use ebsprod-compartment for the compartment name and ebscm-proddba-grp as the group name for the Oracle E-Business Suite administrators group. As shown in the following diagram, you enable
the users in this group to manage the Oracle E-Business Suite production environments by defining policies giving them access to the appropriate compartment and resources.

**Production EBS Administrators Group and Policies**

Run the following commands to create the Oracle E-Business Suite administrators group and assign the required policies:

**Create and Map Oracle E-Business Suite Administrators Groups in Oracle Identity and Access Management and Identity Cloud Service:**

Run the following commands to create the Oracle E-Business Suite and map it in Oracle Identity Access Management (IAM) and Identity Cloud Service (IDCS).

1. In the Oracle Cloud Infrastructure console navigation menu, under Governance and Administration, select Identity, and then click Groups.

2. Create the Oracle Identity Access and Management group as follows:
   1. Click Create Group.

   2. In the dialog window, enter the required details:
      
      • **NAME**: Enter the name for the group (for example, ebscm-proddb-grp).

      • **DESCRIPTION**: Enter a description of your choice.

   3. Click Create.

3. Create the Oracle Identity Cloud Service group as follows:
   1. In the console navigation menu, under Governance and Administration, select Identity, and then click Federation.

   2. Click on the name of the identity provider that corresponds to Oracle Identity Cloud Service.
3. On the left hand side under **Resources**, click **Groups**.

4. Click **Create IDCS Group**.

5. In the dialog window, enter the required details:
   - **NAME**: Supply a name for the group (for example, idcs-ebscm-proddba-grp).
   - **DESCRIPTION**: Enter a description of your choice.

6. Click **Create**.

4. Within the same page, map the groups in Oracle Identity Cloud Service as follows:
   1. Click **Group Mappings** on the left hand side.
   2. Click **Add Mappings**.
   3. In the dialog window, select the Identity Provider group and the corresponding Oracle Cloud Infrastructure group from the drop down-lists (for example, idcs-ebscm-proddba-grp and ebscm-proddba-grp).
   4. Click **Add Mappings**.

**Assign Policies:**

1. In the console navigation menu, under **Governance and Administration**, select **Identity**, and click **Policies**.

2. Create a policy for the network compartment to allow Oracle E-Business Suite administrators to use the network compartment:
   1. Select the network compartment from the **COMPARTMENT** drop-down list on the left.
   2. Click **Create Policy**.

3. In the dialog window, enter the required details:
   - **NAME**: Supply a name (for example, networkcompartment-policy).
   - **DESCRIPTION**: Enter a description of your choice.
   - Add the following policy statements, substituting your own group name in place of ebscm-proddba-grp and your own network compartment in place of network-compartment, if different from our example.
Allow group ebscm-proddba-grp to use virtual-network-family in compartment network-compartment

4. Click Create.

3. Create the policy for the Oracle E-Business Suite administrators to perform operations on Oracle Cloud Infrastructure resources at the tenancy level.

1. Select the root compartment of your tenancy from the COMPARTMENT drop-down list on the left.

2. Click Create Policy.

3. In the dialog window, enter the required details:
   
   • NAME: Enter a name (for example, ebsproddba-root-policy).
   
   • DESCRIPTION: Enter a description of your choice.
   
   • Add the following policy statements, substituting your own group name in place of ebscm-proddba-grp, if appropriate.

   - Allow group ebscm-proddba-grp to manage buckets in tenancy
   - Allow group ebscm-proddba-grp to manage objects in tenancy
   - Allow group ebscm-proddba-grp to manage app-catalog-listing in tenancy
   - Allow group ebscm-proddba-grp to inspect compartments in tenancy
   - Allow group ebscm-proddba-grp to inspect users in tenancy
   - Allow group ebscm-proddba-grp to inspect groups in tenancy
   - Allow group ebscm-proddba-grp to use tag-namespaces in tenancy where target.tag-namespace.name='Oracle-Tags'

4. Click Create Policy.

4. Create the policy for the Oracle E-Business Suite administrators to perform operations on Oracle Cloud Infrastructure resources within their own compartment.

1. Select the Oracle E-Business Suite compartment from the COMPARTMENT drop-down list on the left.

2. Click Create Policy.

3. In the dialog window, enter the required details:
   
   • NAME: Enter a name (for example, ebsproddba-policy).
   
   • DESCRIPTION: Enter a description of your choice.
   
   • Add the following policy statements, substituting your own group name
and compartment name if different from those in our example.

Allow group ebscm-proddba-grp to manage instance-family in compartment ebsprod-compartment
Allow group ebscm-proddba-grp to manage database-family in compartment ebsprod-compartment
Allow group ebscm-proddba-grp to manage load-balancers in compartment ebsprod-compartment
Allow group ebscm-proddba-grp to manage volume-family in compartment ebsprod-compartment
Allow group ebscm-proddba-grp to use tag-namespaces in compartment ebsprod-compartment
Allow group ebscm-proddba-grp to manage tag-namespaces in compartment ebsprod-compartment
Allow group <Oracle E-Business Suite Cloud Manager administrators group> to manage tag-namespaces in compartment ebsprod-compartment

4. Click Create Policy.

5. (Conditional) If you plan to use the Default Network Profiles created by the ProvisionOCINetwork.pl script described in Use a Default Network with Automated Scripts, page 3-10, then ensure that you add the corresponding policy statements for your Oracle E-Business Suite administrators group. To do so, follow the instructions in Create and Map Groups in Oracle Cloud Infrastructure Identity and Access Management and Oracle Identity Cloud Service, page 2-7.

Create Users in Oracle Identity Cloud Service

You will create users in Oracle Identity Cloud Service for the Oracle E-Business Suite administrators.

The users will create and own the Oracle Cloud Infrastructure resources that run your Oracle E-Business Suite production environments.

Oracle Identity Cloud Service is used for authenticating Oracle E-Business Suite administrators.

1. As the tenancy administrator, log in to the My Services dashboard by navigating to https://myservices-<your tenancy name>.console.oraclecloud.com/mycloud/cloudportal/dashboard and clicking Sign In.

2. Click the Users icon in the top right corner, then select My Home.

3. Search and click Admin Console. This takes you to the Oracle Identity Cloud Service Admin console.

4. For each Oracle E-Business Suite production administrator to be added (for example, members of idcs-ebscm-proddba-grp), perform the following steps:

   1. Click the navigation menu and select Users.
2. Click Add.

3. In the dialog window, supply the following information:
   - First Name
   - Last Name
   - User Name / Email

4. Select the check box **Use email address as the user name**.

5. Click Next.

6. In the dialog window, select the check box for the group you just created (for example, idcs-ebscm-proddba-grp).

7. Click Finish.

   **Note:** You can create and add further such Oracle E-Business Suite administrators at any later time.

8. At this point, Oracle Identity Cloud Service will dynamically send an email that will request the newly added Oracle E-Business Suite administrators to activate their accounts. Provide the administrators the Oracle E-Business Suite Cloud Manager link and notify them that they must now self-register by following the instructions in Access Oracle E-Business Suite Cloud Manager, page 7-2.

---

**Create Network Resources for Deploying Oracle E-Business Suite Environments**

In this section, the network administrator and Oracle E-Business Suite Cloud Manager administrator perform tasks as indicated.

Before the Oracle E-Business Suite Cloud Manager can be used to provision environments, a network and associated network profiles must be created. A network profile maps Oracle Cloud Infrastructure network definitions with Oracle E-Business Suite instances network requirements. You could have multiple Oracle E-Business Suite environments in the same network or a network designated for a specific purpose, such as production, test, etc.

When creating a network, the network administrator can start by defining the subnets associated with network resources either using the automated scripts provided through a default network or manually creating required resources with chosen topology.
• Use a Default Network with Automated Scripts, page 3-10 - This section provides guidance for the network administrator who wishes to create a default network and two default network profiles, one for One-Click Provisioning and one for Advanced Provisioning using provided scripts, and to the Oracle E-Business Suite Cloud Manager administrator who will subsequently upload the network profiles for One-Click Provisioning and Advanced Provisioning.

• Use a Custom Network, page 3-13 - The network administrator has an option to create custom network elements and subsequently use these elements in the definition of custom network profiles.

Use a Default Network with Automated Scripts:
When creating a network through a default network, the following scripts are used prior to accessing the Oracle E-Business Suite Cloud Manager UI to create and then upload two default network profiles, one for One-Click Provisioning and one for Advanced Provisioning:

• ProvisionOCINetwork.pl: This script creates required subnets and security lists and generates two network profile definitions (.json files). This script must be run by a network administrator user who has privileges to create network resources. See Create Default Network and Network Profiles Using ProvisionOCINetwork.pl, page 3-10.

• UploadOCINetworkProfile.pl: This script uploads network profile definitions (.json files) to a database so they can be viewed from the Oracle E-Business Suite Cloud Manager UI. This script must be run by an Oracle E-Business Suite Cloud Manager administrator. See Upload Network Profile Definitions Profiles Using ProvisionOCINetwork.pl, page 3-12.

Create Default Network and Network Profiles Using ProvisionOCINetwork.pl
The following script will use Oracle Cloud Infrastructure API to create the network resources required by the Oracle E-Business Suite environment. When prompted for the script, you must provide authentication credentials that belong to the network administrator. We recommend that you upload the network administrator private API keys temporarily to the Cloud Manager VM to be able to run the script.

Add API Key to the Network Administrator
1. Log in to the Oracle Cloud Infrastructure Service Console as the network administrator user. Note that this user should be a non-federated user (in the form <firstname>.<lastname>@<domain>) and not a federated user (for example, oracleidentitycloudservice/<firstname>.<lastname>@<domain>).

2. Click the user icon.

3. Select User Settings from the context menu.
4. Under Resources in the navigation menu on the left, click **API Keys**. Then, click **Add Public Key**.

5. Select the **Paste Public Keys** radio button.

6. Paste the contents of the API public key in the dialog box and click **Add**. The key’s fingerprint is displayed.

7. Copy the Oracle Cloud Infrastructure API private PEM key file to the Oracle E-Business Suite Cloud Manager Compute instance. The file must be placed in a directory owned by the oracle user, for example /u01/install/APPS/.oci. The fully qualified path to the Oracle Cloud Infrastructure API private PEM key file will be needed for running `ProvisionOCINetwork.pl`.

**Identify Credentials Required for Network Provisioning Script**

While still logged into the Oracle Cloud Infrastructure Service Console as the network administrator user, identify and record the OCID of your user. You will need to provide this credential when you run the `ProvisionOCINetwork.pl` script.

1. From the Oracle Cloud Infrastructure console, click on the user profile icon on the top right hand side of your screen, and select **User Settings**.

2. Click **Copy** to copy the OCID of the user into your clipboard, and record this value for use in Run ProvisionOCINetwork.pl, page 3-11.

**Run ProvisionOCINetwork.pl**

The network administrator performs the tasks described in this section.

**Note:** The network laid down by this script creates only public subnets, not private subnets.

1. As the oracle user, run `ProvisionOCINetwork.pl`:

   ```
   $ sudo su - oracle
   $ cd /u01/install/APPS/apps-unlimited-ebs/bin
   $ perl ProvisionOCINetwork.pl
   ```

2. The screen will display the name of the log file for this session in the format `ProvisionOCINetwork_<Date_and_Time_Stamp>.log`, as illustrated by this example:

   ```
   Log File : /u01/install/APPS/apps-unlimited-ebs/out/ProvisionOCINetwork_Thu_Jul_11_13_38_17_2019.log
   ```

3. After a list of the subnets to be created is displayed, you will be prompted to select Y to proceed or N to exit. Enter Y, as shown in this example:

   ```
   Enter Y to proceed or N to exit: Y
   ```
4. You will now enter your details, substituting your own values for the example values shown:

   Enter OCID of network administrator user              : ocid1.user.
   oc1..xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

   Enter absolute path of private key of API signing key : /u01/install/APPS/.oci/oci_api_key_network_admin.pem

   Enter tenancy ocid                                    : ocid1.
   tenancy.oc1..xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

   Validating user and fetching OCI metadata...

   Enter unique identifier for the EBS network         : ebscmnet
   Enter EBS subnet 1 CIDR (E.g. 10.0.1.0/24)          : 10.0.59.0/28
   Enter EBS subnet 2 CIDR (E.g. 10.0.2.0/24)          : 10.0.83.16/28
   Enter LBaaS subnet CIDR (E.g. 10.0.3.0/24)          : 10.0.83.32/28

5. You will now be prompted to select Y to proceed or N to exit. Enter Y, as shown in this example:

   Are you sure you want to proceed with the above inputs? [Y/N]: Y

6. When processing is complete, you will see a success screen with content similar to the following:

   Oracle EBS Cloud related network created successfully.

   List of resources created:
   ebscmnet_lbaas_subnet
   ebscmnet_lbaas_seclist
   ebscmnet_lbaas_routetable
   ebscmnet_db_subnet
   ebscmnet_db_seclist
   ebscmnet_db_routetable
   ebscmnet_apps_subnet
   ebscmnet_apps_seclist
   ebscmnet_apps_routetable

   Program: ProvisionOCINetwork.pl completed at Thu <DATE> <TIME> <YEAR>
   Advanced Network Profile JSON Path: /u01/install/APPS/apps-unlimited-ebs/build/ebscmnet/ebscmnet_DEFAULT_PROFILE_ADVANCED.json
   OneClick Network Profile JSON Path: /u01/install/APPS/apps-unlimited-ebs/build/ebscmnet/ebscmnet_DEFAULT_PROFILE_ONECLICK.json
   Execute /u01/install/APPS/apps-unlimited-ebs/bin/UploadOCINetworkProfile.pl to Upload JSON into DB

7. Remove the network administrator's private key from the Cloud Manger Compute instance after running the ProvisionOCINetwork.pl script.

   $ rm /u01/install/APPS/.oci/oci_api_key_network_admin.pem

Upload Network Profile Definitions Using UploadOCINetworkProfile.pl
The Oracle E-Business Suite Cloud Manager administrator performs the tasks described in this section.

As seen at the bottom of your success screen in step 6 of Run ProvisionOCINetwork.pl, page 3-11, the Oracle E-Business Suite Cloud Manager administrator now needs to run the upload script. The script needs to be uploaded twice, the first time for the One-Click
Provisioning default network profile and the second time for the Advanced Provisioning default network profile.

The following example illustrates running the script for the Advanced Provisioning default network profile.

1. As the oracle user, run the `UploadOCINetworkProfile.pl` script:
   
   ```
   $ sudo su - oracle
   $ cd /u01/install/APPS/apps-unlimited-ebs/bin
   $ perl UploadOCINetworkProfile.pl
   ```

2. The screen will display the name of the log file for this session in the format `ProvisionOCINetwork_<Date_and_Time_Stamp>.log`, as illustrated by this example:
   
   ```
   ```

3. Enter your details, substituting your own values for the example values shown:
   
   ```
   Enter Network profile JSON file absolute path: /u01/install/APPS/apps-unlimited-ebs/build/ebscmnet/ebscmnet_DEFAULT_PROFILE_ADVANCED.json
   Enter OCID of EBS Cloud Manager administrator user: ocid1.user.oc1..xxxxxxxxxxx
   Enter EBS Cloud Manager admin password: 
   Enter Absolute path of private key of API signing key: /u01/install/APPS/oci_api_key.pem
   Enter Tenancy OCID: ocid1.tenancy.oc1..yyyyyyyyyyyyyyyy
   Enter Oracle E-Business Suite Cloud Manager Admin Password: 
   
   **Note:** The value you enter for "Network profile JSON file absolute path" must be the same value displayed on the `ProvisionOCINetwork.pl` success screen. Refer to step 6 of Run `ProvisionOCINetwork.pl`, page 3-11.
   ```

4. When a profile has been updated, you will see a success message similar to the one shown in this example:
   
   ```
   Executing: ebscm_add_default_network_profile API for DEFAULT_PROFILE_ADVANCED
   Executing Stored Procedure: ebscm_add_default_network_profile
   RetCode: 0
   Row count: 0
   ADVANCED Network Profile uploaded successfully.
   
   **Note:** These two default network profiles are available to all users.
   ```

Use a Custom Network:
This section describes how network administrators can manually create the minimal network resources required for Oracle E-Business Suite Cloud Manager Advanced
Provisioning, which allows Oracle E-Business Suite administrators to provision an Oracle E-Business Suite instance with their chosen topology.

**Note:** Oracle E-Business Suite deployment on Oracle Cloud Infrastructure in a Hybrid DNS Configuration [https://github.com/terraform-providers/terraform-provider-oci/blob/255817f83956f1f9a3ab903e11465e8b4d8de1957/docs/examples/networking/hybrid_dns/Hybrid-DNS-configuration-using-DNS-VM-in-VCN.md](https://github.com/terraform-providers/terraform-provider-oci/blob/255817f83956f1f9a3ab903e11465e8b4d8de1957/docs/examples/networking/hybrid_dns/Hybrid-DNS-configuration-using-DNS-VM-in-VCN.md) always requires access to a VCN DNS resolver. If you are using such a configuration, ensure that IP address 169.254.169.254 is listed as a DNS server in the DHCP options.

In this example, we will configure the network settings specifically for deploying Oracle E-Business Suite production environments managed by Oracle E-Business Suite Cloud Manager.

The configuration includes the following tasks:

- Establish Your VCN, page 3-14
- Create an Internet Gateway (Conditional), page 3-15
- Create a NAT Gateway (Conditional), page 3-15
- Create a Service Gateway (Conditional), page 3-16
- Create Route Tables, page 3-16
- Create Security Lists, page 3-18
- Create Subnets, page 3-19
- Create Security Rules, page 3-21

**Note:** If you are using Exadata Cloud Service, you must have already setup required route rules, security lists, subnets required for the database tier. Review the corresponding resources created in this section for database tier and add any missing resources.

**Establish Your VCN**

Customers have the option to create their own Virtual Cloud Network (VCN) or use an existing VCN (such as the VCN where the Oracle E-Business Suite Cloud Manager is deployed). If you use a VCN separate from the Oracle E-Business Suite Cloud Manager VCN for your Oracle E-Business Suite environments, ensure that adequate network communication is established between the two.
Note: When VCNs reside in the same tenancy, local VCN peering is supported for communication between the VCN holding Oracle E-Business Suite Cloud Manager VM and the VCN holding Oracle E-Business Suite environments. With this configuration, you can have Oracle E-Business Suite Cloud Manager VM installed on one VCN and create instances on other VCNs in the same tenancy.

For more information about local VCN peering and how to set it up, see Local VCN Peering (Within Region) [https://docs.cloud.oracle.com/iaas/Content/Network/Tasks/localVCNpeering.htm].

If you decide to create a new VCN for your Oracle E-Business Suite environments, follow the instructions in Create a Virtual Cloud Network, page 2-13.

Create an Internet Gateway (Conditional)

Note: The resources created (including route tables, security lists, and subnets) must be sufficient to support your chosen topology, and therefore may need to be more extensive than the examples shown here.

The Oracle E-Business Suite provisioning and cloning flows create new Compute instances and update them to the latest OS patches using yum. Your compute instances use a gateway to access the public yum repository on the internet.

If you plan to use a public subnet for your Compute instances, and you created a new VCN, you will need to create an internet gateway for that VCN by following the instructions for either a public or private subnet, as found in Create Network Resources for Deploying Oracle E-Business Suite Cloud Manager, page 2-12.

Create a NAT Gateway (Conditional)

If you plan to use a private subnet for your Oracle E-Business Suite environments, you must use a NAT gateway. Note that there is a limit of one NAT gateway per VCN.

If you did not create a NAT Gateway previously, follow these steps to create one:

1. From the Oracle Cloud Infrastructure Service Console, click the menu icon at the top left to open the navigation menu. Under CORE INFRASTRUCTURE, go to Networking, and click Virtual Cloud Networks.

2. On the Virtual Cloud Networks screen, click the link with the name of your VCN, such as ebscm-vcn.

3. Under Resources on the navigation menu at the left, select NAT Gateway.

4. Click Create NAT Gateway:
• **CREATE IN COMPARTMENT**: Select your network compartment (for example, network-compartment).

• **NAME**: Specify a suitable name (for example, ebs-ngw).

• Click **Create NAT Gateway** at the bottom of the window.

**Create a Service Gateway (Conditional)**

If you plan to use a private subnet for your Oracle E-Business Suite environments, you can make use of a service gateway along with a NAT gateway. Note that there is a limit of one service gateway per VCN.

To create a service gateway:

1. On the **Virtual Cloud Networks** screen, click the link with the name of your VCN, such as ebscm-vcn.

2. Under **Resources** on the navigation menu at the left, select **Service Gateways**.

3. Click **Create Service Gateway**:
   - **NAME**: Specify a suitable name (for example, ebscm-srvgw).
   - **CREATE IN COMPARTMENT**: Select your network compartment (for example, network-compartment).
   - **SERVICES**: Select **All <XXX> Services In Oracle Services Network** (where XXX is a region-specific code, such as IAD or LHR).
   - Click **Create Service Gateway** at the bottom of the window.

**Create Route Tables**

In this section, you will create three separate route tables. Their roles and example names are shown in the following table:

<table>
<thead>
<tr>
<th>Component Route Table Needed For</th>
<th>Example Route Table Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load Balancer</td>
<td>ebslbaas-RouteTable</td>
</tr>
<tr>
<td>Oracle E-Business Suite Application Tier</td>
<td>apps-RouteTable</td>
</tr>
<tr>
<td>Oracle E-Business Suite Database Tier</td>
<td>db-RouteTable</td>
</tr>
</tbody>
</table>
The steps you will take depend on whether you are using a public subnet or a private subnet. Follow whichever of the two subsections below applies to you.

**Create Route Tables for a Public Subnet**
To create each of the four route tables for a public subnet, use the following steps:

1. On the Virtual Cloud Networks screen, click the link with the name of your VCN, such as ebsnetwork-vcn.

2. Under Resources on the navigation menu at the left, select Route Tables.

3. Click Create Route Table:
   1. **NAME**: Enter a name such as, ebslbaas-RouteTable, apps-RouteTable, or db-RouteTable.
   2. **CREATE IN COMPARTMENT**: Select your network compartment (for example, network-compartment).
   3. Click + Another Route Rule.

4. Enter Route Rules details as follows:
   - **TARGET TYPE**: Select Internet Gateway.
   - **DESTINATION CIDR BLOCK**: 0.0.0.0/0
   - **COMPARTMENT**: Select the previously identified compartment.
   - **TARGET INTERNET GATEWAY**: Select the previously created gateway (for example, ebscm-igw).

5. Click Create Route Table at the bottom of the window.

**Create Route Tables for a Private Subnet**
To create each of the three route tables for a private subnet, use the following steps:

1. On the Virtual Cloud Networks screen, click the link with the name of your VCN, such as ebscm-vcn.

2. Under Resources on the navigation menu at the left, select Route Tables.

3. Click Create Route Table:
   1. **NAME**: Specify a name such as ebslbaas-RouteTable, apps-RouteTable, or db-RouteTable.
Note: If you are creating a route table for subnet hosting load balancer and you are using private subnets, no route rules are required. You can directly skip to the last substep 7 and click Create Route Table at the bottom of the window. Additional rules are only required for subnet hosting Oracle E-Business Suite application tier or database tier nodes.

2. **CREATE IN COMPARTMENT**: Select your network compartment (for example, network-compartment).

3. Click + Another Route Rule.

4. Enter Route Rules details as follows:
   - **TARGET TYPE**: Select NAT Gateway.
   - **DESTINATION CIDR BLOCK**: 134.70.0.0/17
   - **COMPARTMENT**: Select the previously identified compartment.
   - **TARGET NAT GATEWAY**: Select the previously created NAT Gateway (for example, ebs-ngw).

5. Click **Create Route Table** at the bottom of the window.

6. Enter Route Rules details as follows:
   - **TARGET TYPE**: Select Service Gateway.
   - **DESTINATION SERVICE**: Select All <XXX> Services In Oracle Services Network (where XXX is a region-specific code, such as IAD or LHR).
   - **COMPARTMENT**: Select the previously identified compartment.
   - **TARGET SERVICE GATEWAY**: Select the previously created NAT Gateway (for example, ebs-srvgw).

7. Click **Create Route Table** at the bottom of the window.

**Create Security Lists**

In this section, you will create up to three separate security lists. Their roles and some example names are shown in the table below:
Table 3-2 Security Lists

<table>
<thead>
<tr>
<th>Component Security List Needed For</th>
<th>Example Security List Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load Balancer</td>
<td>ebslbaas-seclist</td>
</tr>
<tr>
<td>Oracle E-Business Suite Application Tier</td>
<td>apps-seclist</td>
</tr>
<tr>
<td>Oracle E-Business Suite Database Tier</td>
<td>db-seclist</td>
</tr>
</tbody>
</table>

To create a security list:

1. On the Virtual Cloud Networks screen, click the link with the name of your VCN, such as `ebscm-vcn`.

2. Under Resources on the navigation menu at the left, select Security Lists.

3. Click Create Security List:
   1. NAME: Specify a name such as `ebslbaas-seclist`, `apps-seclist`, or `db-seclist`.
   2. CREATE IN COMPARTMENT: Select your compartment name, such as `network-compartment`.
   3. If default rules named Ingress Rule 1 and Egress Rule 1 appear, remove these rules.
   4. Click Create Security List at the bottom of the window.

Create Subnets

In this section, you will create new subnets, specifying your own names and parameters.

The following example can be used as a reference for defining the subnets that will be used for deploying your Oracle E-Business Suite environment that could have internal and external web entry points (such as in a common DMZ configuration).
If you choose to use regional subnets, see the following table with example values for guidance:

**Table 3-3 Examples of Regional Subnets**

<table>
<thead>
<tr>
<th>Subnet Name</th>
<th>CIDR Block</th>
<th>Route Table</th>
<th>Subnet Access</th>
<th>Security List</th>
</tr>
</thead>
<tbody>
<tr>
<td>internal-ebslbaas-subnet-phx</td>
<td>10.0.3.0/24</td>
<td>ebslbaas-RouteTable</td>
<td>Public or private subnet</td>
<td>internal-ebslbaas-seclist</td>
</tr>
<tr>
<td>internal-apps-subnet-phx</td>
<td>10.0.4.0/24</td>
<td>apps-RouteTable</td>
<td>Public or private subnet</td>
<td>internal-apps-seclist</td>
</tr>
<tr>
<td>external-ebslbaas-subnet-phx (optional)</td>
<td>10.0.5.0/24</td>
<td>ebslbaas-RouteTable</td>
<td>Public or private subnet</td>
<td>external-ebslbaas-seclist</td>
</tr>
<tr>
<td>external-apps-subnet-phx</td>
<td>10.0.6.0/24</td>
<td>apps-RouteTable</td>
<td>Public or private subnet</td>
<td>external-apps-seclist</td>
</tr>
<tr>
<td>db-subnet-phx</td>
<td>10.0.7.0/24</td>
<td>db-RouteTable</td>
<td>Public or private subnet</td>
<td>db-seclist</td>
</tr>
</tbody>
</table>

To create each new subnet:

1. On the **Virtual Cloud Networks** screen, click the link with the name of your VCN, such as ebscm-vcn.

2. Under **Resources** in the navigation menu on the left, select **Subnets**.
3. Click Create Subnet, specifying your choice for the following parameters:

   - NAME

   - SUBNET TYPE: Select either Regional (Recommended) or Availability Domain-Specific. If you choose Availability-Domain Specific, select your availability domain.

   - CIDR BLOCK

   - ROUTE TABLE: When you create a subnet, you can specify it as either a Public Subnet or a Private Subnet. If you are creating a public subnet, ensure you choose a route table that has a target type of Internet Gateway. If you are creating a private subnet, ensure you choose a Route Table that has a target type of NAT Gateway.

   - SUBNET ACCESS: As mentioned in the ROUTE TABLE previously, subnet access can be either public or private. Be aware that if you select a private subnet for any VM, the corresponding VM will not have a public IP address and no inbound connections to this VM from outside the current VCN will be allowed.

     For more information, see VCNs and Subnets [https://docs.cloud.oracle.com/en-us/iaas/Content/Network/Tasks/managingVCNs.htm].

   - SECURITY LIST

4. Click Create at the bottom of the window.

Create Security Rules
In this section, you will add the mandatory security rules shown in the following tables to the security lists created in Creating Security Lists, page 3-18.

Internal Load Balancer Security List
This section includes the following security rules for the internal load balancer security list:
Table 3-4 Ingress Rules for Both Public and Private Subnets

<table>
<thead>
<tr>
<th>Source Type</th>
<th>Source</th>
<th>Protocol</th>
<th>Source Port Range / Type and Code</th>
<th>Destination Port Range / Type and Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIDR</td>
<td>CIDR that describes the IP range users will use to access your Oracle E-Business Suite environments.</td>
<td>TCP</td>
<td>All</td>
<td>Depends on the web entry port you will use during the provisioning of your environment.</td>
</tr>
</tbody>
</table>

Table 3-5 Egress Rules When Using a Public Subnet

<table>
<thead>
<tr>
<th>Destination Type</th>
<th>Destination</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIDR</td>
<td>0.0.0.0/0</td>
<td>TCP</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>CIDR</td>
<td>0.0.0.0/0</td>
<td>ICMP</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Table 3-6 Egress Rules When Using a Private Subnet

<table>
<thead>
<tr>
<th>Destination Type</th>
<th>Destination</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIDR</td>
<td>&lt;Internal application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>CIDR</td>
<td>0.0.0.0/0</td>
<td>ICMP</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

External Load Balancer Security List (Optional)

This section includes the following security rules for the external load balancer security list:
**Table 3-7 Ingress Rules for Both Public and Private Subnets**

<table>
<thead>
<tr>
<th>Source Type</th>
<th>Source</th>
<th>Protocol</th>
<th>Source Port Range / Type and Code</th>
<th>Destination Port Range / Type and Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIDR</td>
<td>CIDR that describes the IP range users will use to access your Oracle E-Business Suite environments.</td>
<td>TCP</td>
<td>All</td>
<td>Depends on the web entry port you will use during the provisioning of your environment.</td>
</tr>
</tbody>
</table>

**Table 3-8 Egress Rules When Using a Public Subnet**

<table>
<thead>
<tr>
<th>Destination Type</th>
<th>Destination</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIDR</td>
<td>0.0.0.0/0</td>
<td>TCP</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>CIDR</td>
<td>0.0.0.0/0</td>
<td>ICMP</td>
<td>N/A (leave Type and Code blank)</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Table 3-9 Egress Rules When Using a Private Subnet**

<table>
<thead>
<tr>
<th>Destination Type</th>
<th>Destination</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIDR</td>
<td>&lt;External application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>CIDR</td>
<td>0.0.0.0/0</td>
<td>ICMP</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Application Tier Security List for Internal Subnets**

This section includes the following security rules for the application tier security list for internal subnets:
<table>
<thead>
<tr>
<th>Source Type</th>
<th>Source</th>
<th>Protocol</th>
<th>Source Port Range / Type and Code</th>
<th>Destination Port Range / Type and Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIDR</td>
<td>&lt;Internal application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;EBS Cloud Manager subnet CIDR&gt;</td>
<td>ICMP</td>
<td>N/A (leave Type and Code blank)</td>
<td>N/A (leave Type and Code blank)</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Internal load balancer subnet CIDR&gt;</td>
<td>ICMP</td>
<td>N/A (leave Type and Code blank)</td>
<td>N/A (leave Type and Code blank)</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;EBS Cloud Manager subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>22</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;External application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>111</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;External application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>2049</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Database tier subnet CIDR&gt;</td>
<td>ICMP</td>
<td>N/A (leave Type and Code blank)</td>
<td>N/A (leave Type and Code blank)</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Internal application tier subnet CIDR&gt;</td>
<td>ICMP</td>
<td>N/A (leave Type and Code blank)</td>
<td>N/A (leave Type and Code blank)</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;External application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>7001-7003</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;External application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>6801-6802</td>
</tr>
<tr>
<td>Source Type</td>
<td>Source</td>
<td>Protocol</td>
<td>Source Port Range / Type and Code</td>
<td>Destination Port Range / Type and Code</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------</td>
<td>----------</td>
<td>-----------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;External application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>16801-16802</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;External application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>12345</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;External application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>36501-36550</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Internal load balancer subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>8000</td>
</tr>
</tbody>
</table>

**Table 3-11 Egress Rules When Using a Public Subnet**

<table>
<thead>
<tr>
<th>Destination Type</th>
<th>Destination</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIDR</td>
<td>0.0.0.0/0</td>
<td>TCP</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>CIDR</td>
<td>0.0.0.0/0</td>
<td>ICMP</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Table 3-12 Egress Rules When Using a Private Subnet**

<table>
<thead>
<tr>
<th>Destination Type</th>
<th>Destination</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIDR</td>
<td>134.70.0.0/17</td>
<td>TCP</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>Destination Type</td>
<td>Destination</td>
<td>Protocol</td>
<td>Source</td>
<td>Direction</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
<td>----------</td>
<td>--------</td>
<td>-----------</td>
</tr>
<tr>
<td>Service</td>
<td>All &lt;XXX&gt; Services in the Oracle Services Network</td>
<td>TCP</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>Service</td>
<td>All &lt;XXX&gt; Services in the Oracle Services Network</td>
<td>ICMP</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;External application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Internal application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Database tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>1521-1524</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;EBS Cloud Manager subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>443</td>
</tr>
<tr>
<td>CIDR</td>
<td>0.0.0.0/0</td>
<td>ICMP</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Application Tier Security List for External Subnets (Optional)**

This section includes the following security rules for the application tier security list for external subnets:
Table 3-13 Ingress Rules for Application Tier Subnet 2 (appSubnet2)

<table>
<thead>
<tr>
<th>Source Type</th>
<th>Source</th>
<th>Protocol</th>
<th>Source Port Range / Type and Code</th>
<th>Destination Port Range / Type and Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIDR</td>
<td>&lt;External application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;EBS Cloud Manager subnet CIDR&gt;</td>
<td>ICMP</td>
<td>N/A (leave Type and Code blank)</td>
<td>N/A (leave Type and Code blank)</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;External load balancer subnet CIDR&gt;</td>
<td>ICMP</td>
<td>N/A (leave Type and Code blank)</td>
<td>N/A (leave Type and Code blank)</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;EBS Cloud Manager subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>22</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Internal application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>111</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Internal application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>2049</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Internal application tier subnet CIDR&gt;</td>
<td>ICMP</td>
<td>N/A (leave Type and Code blank)</td>
<td>N/A (leave Type and Code blank)</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Database tier subnet CIDR&gt;</td>
<td>ICMP</td>
<td>N/A (leave Type and Code blank)</td>
<td>N/A (leave Type and Code blank)</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;External application tier subnet CIDR&gt;</td>
<td>ICMP</td>
<td>N/A (leave Type and Code blank)</td>
<td>N/A (leave Type and Code blank)</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Internal application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>22</td>
</tr>
<tr>
<td>Source Type</td>
<td>Source</td>
<td>Protocol</td>
<td>Source Port Range / Type and Code</td>
<td>Destination Port Range / Type and Code</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------------</td>
<td>----------</td>
<td>-----------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Internal application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>5556-5557</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Internal application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>7201-7202</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Internal application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>17201-17202</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Internal application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>7401-7402</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Internal application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>17401-17402</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Internal application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>7601-7602</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Internal application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>17601-17602</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Internal application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>7801-7802</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Internal application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>17801-17802</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Internal application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>6801-6802</td>
</tr>
<tr>
<td>Source Type</td>
<td>Source</td>
<td>Protocol</td>
<td>Source Port Range / Type and Code</td>
<td>Destination Port Range / Type and Code</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------</td>
<td>----------</td>
<td>-----------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Internal application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>16801-16802</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Internal application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>9999-10000</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Internal application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>1626</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Internal application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>12345</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Internal application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>36501-36550</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Internal application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>6100-6101</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Internal application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>6200-6201</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Internal application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>6500-6501</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;External load balancer subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>8000</td>
</tr>
</tbody>
</table>
### Table 3-14 Egress Rules When Using a Public Subnet

<table>
<thead>
<tr>
<th>Destination Type</th>
<th>Destination</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIDR</td>
<td>0.0.0.0/0</td>
<td>TCP</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>CIDR</td>
<td>0.0.0.0/0</td>
<td>ICMP</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### Table 3-15 Egress Rules When Using a Private Subnet

<table>
<thead>
<tr>
<th>Destination Type</th>
<th>Destination</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIDR</td>
<td>134.70.0.0/17</td>
<td>TCP</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;External application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Database tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>1521-1524</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;EBS Cloud Manager subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>443</td>
</tr>
<tr>
<td>CIDR</td>
<td>0.0.0.0/0</td>
<td>ICMP</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Internal application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>Service</td>
<td>All &lt;XXX&gt; Services in the Oracle Services Network (XXX is a region-specific code, such as IAD or LHR)</td>
<td>TCP</td>
<td>All</td>
<td>All</td>
</tr>
</tbody>
</table>
### Database Tier Security List

This section includes the following security rules for database tier security list:

**Table 3-16 Ingress Rules for Both Public and Private Subnets**

<table>
<thead>
<tr>
<th>Source Type</th>
<th>Source</th>
<th>Protocol</th>
<th>Source Port Range / Type and Code</th>
<th>Destination Port Range / Type and Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIDR</td>
<td>&lt;EBS Cloud Manager subnet CIDR&gt;</td>
<td>ICMP</td>
<td>N/A (leave Type and Code blank)</td>
<td>N/A (leave Type and Code blank)</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Database tier subnet CIDR&gt;</td>
<td>ICMP</td>
<td>N/A (leave Type and Code blank)</td>
<td>N/A (leave Type and Code blank)</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;EBS Cloud Manager subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>22</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Internal application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>1521-1524</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Internal application tier subnet CIDR&gt;</td>
<td>ICMP</td>
<td>N/A (leave Type and Code blank)</td>
<td>N/A (leave Type and Code blank)</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;External application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>1521-1524</td>
</tr>
<tr>
<td>Source Type</td>
<td>Source</td>
<td>Protocol</td>
<td>Source Port Range / Type and Code</td>
<td>Destination Port Range / Type and Code</td>
</tr>
<tr>
<td>-------------</td>
<td>--------</td>
<td>----------</td>
<td>-----------------------------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;External application tier subnet CIDR&gt;</td>
<td>ICMP</td>
<td>N/A (leave Type and Code blank)</td>
<td>N/A (leave Type and Code blank)</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Database tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>22</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Database tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>1521-1524</td>
</tr>
</tbody>
</table>

**Table 3-17 Egress Rules When Using a Public Subnet**

<table>
<thead>
<tr>
<th>Destination Type</th>
<th>Destination</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIDR</td>
<td>0.0.0.0/0</td>
<td>TCP</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>CIDR</td>
<td>0.0.0.0/0</td>
<td>ICMP</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Table 3-18 Egress Rules When Using a Private Subnet**

<table>
<thead>
<tr>
<th>Destination Type</th>
<th>Destination</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIDR</td>
<td>134.70.0.0/17</td>
<td>TCP</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;EBS Cloud Manager subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>443</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Database tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>1521-1524</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Database tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>22</td>
</tr>
</tbody>
</table>
Oracle E-Business Suite Cloud Manager Security List

Note: When creating a custom network, the following security rules need to be added to the Oracle E-Business Suite Cloud Manager security list. For information on creating the security list for Oracle E-Business Suite Cloud Manager, see Create Network Resources for Deploying Oracle E-Business Suite Cloud Manager., page 2-12

Table 3-19 Ingress Rules

<table>
<thead>
<tr>
<th>Source Type</th>
<th>Source</th>
<th>Protocol</th>
<th>Source Port Range / Type and Code</th>
<th>Destination Port Range / Type and Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIDR</td>
<td>&lt;Application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>443</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Database tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>443</td>
</tr>
</tbody>
</table>
Table 3-20 Egress Rules

<table>
<thead>
<tr>
<th>Destination Type</th>
<th>Destination</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIDR</td>
<td>&lt;Application tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>22</td>
</tr>
<tr>
<td>CIDR</td>
<td>&lt;Database tier subnet CIDR&gt;</td>
<td>TCP</td>
<td>All</td>
<td>22</td>
</tr>
</tbody>
</table>

Create Network Profiles

The Oracle E-Business Suite Cloud Manager administrator performs the tasks in this section.

A network profile maps Oracle Cloud Infrastructure network definitions with Oracle E-Business Suite instances network requirements. Before the Oracle E-Business Suite Cloud Manager can be used to provision environments, a network and associated network profiles must be created.

After the network administrator creates the network, the Oracle E-Business Suite Cloud Manager administrator will use the Oracle E-Business Suite Cloud Manager UI to define related network profiles that can then be selected by the Oracle E-Business Suite administrators (in our example, the administrators are members of the ebscm-proddba-grp group).

To create a new network profile, see Create a Network Profile, page 8-4.
Manage the Oracle E-Business Suite Cloud Manager Virtual Machine

This chapter covers the following topics:

- Overview of Managing the Oracle E-Business Suite Cloud Manager Virtual Machine
- Update Oracle E-Business Suite Cloud Manager to the Latest Version (Conditional)
- Perform Oracle E-Business Suite Cloud Manager Administration Tasks
- Manage Ksplice Uptrack Actions

Overview of Managing the Oracle E-Business Suite Cloud Manager Virtual Machine

This chapter describes how to manage the Oracle E-Business Suite Cloud Manager virtual machine after initial deployment.

Update Oracle E-Business Suite Cloud Manager to the Latest Version (Conditional)

Perform the following tasks to ensure you are using the latest version of Oracle E-Business Suite Cloud Manager.

Note: Unless otherwise noted, the Oracle E-Business Suite Cloud Manager administrator performs the tasks in this section.

1. Check the Oracle E-Business Suite Cloud Manager Version, page 4-2

2. Create a Backup of Oracle E-Business Suite Cloud Manager Virtual Machine, page 4-2
3. Migrate to the Latest Codelevel, page 4-2

**Check the Oracle E-Business Suite Cloud Manager Version:**
After deploying Oracle E-Business Suite Cloud Manager, you can log in to Oracle E-Business Suite Cloud Manager and check the version by following the instructions in Log In to Oracle E-Business Suite Cloud Manager, page 7-2 and Check the Oracle E-Business Suite Cloud Manager Version, page 7-4. If you see a message that a later version is available than the one you have installed, proceed with the rest of this procedure.

The latest version is 20.2.1.1.1.

**Create a Backup of Oracle E-Business Suite Cloud Manager Virtual Machine:**
Before you run the Self Update Utility, we strongly recommend that you back up your Oracle E-Business Suite Cloud Manager Virtual Machine. To do so, follow the instructions in Cloning a Boot Volume [https://docs.cloud.oracle.com/en-us/iaas/Content/Block/Tasks/cloningabootvolume.htm] to create a boot volume clone. You will also need to record key details of your provisioning VM for use during a restore process.

From the Oracle Cloud Infrastructure console on the **Instances** screen, click on your instance (for example, myebscminstance) to go to the **Instance Details** screen. Record (such as in a screenshot) the instance attributes for later use:

- Shape
- Availability Domain
- Virtual Cloud Network (VCN)
- Subnet
- Private IP address

When you restore, you will also need the SSH key and host name of the original instance.

To obtain the host name, log in to Oracle E-Business Suite Cloud Manager VM using SSH, and perform the following steps:

1. Run the **hostname** command and record the name.
2. Make a note of the contents of the **/etc/hosts** file.
Migrate to the Latest Codelevel:

**Important:** Note for Exadata Cloud Service customers:

- In Release 20.2.1.1.1 and later, Oracle E-Business Suite Cloud Manager supports the new Exadata Cloud Service resource model. If you use Exadata Cloud Service, you should convert your Exadata DB Systems to this new model, and then update Oracle E-Business Suite Cloud Manager to Release 20.2.1.1.

- Alternatively, if you are not ready to convert to the new resource model, and you need to provision Oracle E-Business Suite environments where the database is on an Exadata DB System that uses the old resource model, then you must remain on your existing Oracle E-Business Suite Cloud Manager release of 20.2.1.1 or earlier.

After you have created the backup of the virtual machine, you can proceed to migrate your deployment based on your current Oracle E-Business Suite Cloud Manager version.

- If you are on Oracle E-Business Suite Cloud Manager version 19.3.1.X or later, perform the steps in Migrate Version 19.3.1.X or Later to the Latest Codelevel (Conditional), page 4-4.

- If you are on Oracle E-Business Suite Cloud Manager version 19.2.1.2, perform the steps in Migrate Version 19.2.1.2 to the Latest Codelevel (Conditional), page 4-6.

- If you are on Oracle E-Business Suite Cloud Manager version 19.1.1 through 19.2.1.1, perform the steps in Migrate Version 19.1.1 through 19.2.1.1 to the Latest Codelevel (Conditional), page 4-9.

- If you are on a version earlier than 19.1.1, there is no predefined upgrade path. You may need to redeploy Oracle E-Business Suite Cloud Manager by following the instructions in Deploy Oracle E-Business Suite Cloud Manager on Oracle Cloud Infrastructure, page 2-1.

**Note:** For existing environments created with versions of Oracle E-Business Suite Cloud Manager prior to version 20.2.1, the expected behaviors are as follows:

- For instances created using Advanced Provisioning:
  - The Logical FQDN for both the application tier and database tier will display as "Not Configured" on the Environment.
The Add Node dialog window will not have the "Logical Hostname" field and the corresponding Logical FQDN on the Environment Details page should have "Not Configured" displayed.

For instances created using One-Click Provisioning, the DNS FQDN and Storage will display as "Not Available" on the Environment Details page.

The Logical FQDN will display as "Not Available" where applicable if the logicalHostConfigured flag is 'false' on the source.

**Migrate Version 19.3.1.X or Later to the Latest Codelevel (Conditional)**

If you are on Oracle E-Business Suite Cloud Manager version 19.3.1.X or later, and you have already created policies for tag-namespaces (such as in Define Additional Policies bring up your version to the latest version, 20.2.1.1.

Perform the following steps:

1. Connect to the Oracle E-Business Suite Cloud Manager VM using SSH and switch from the opc user to the oracle user:
   
   ```
   $ sudo su - oracle
   ```

2. Run the Self Update utility as follows:
   
   ```
   $ cd /u01/install/APPS/apps-unlimited-ebs/bin
   $ perl selfUpdate.pl
   ```

3. Review the warning for Exadata Cloud Service customers and check whether you are ready to proceed with the update to Release 20.2.1.1. If you use Exadata Cloud Service and you are not ready to convert to the new resource model, then you must enter option 2 to exit the utility and remain on your existing Oracle E-Business Suite Cloud Manager release of 20.2.1.1 or earlier.

If you use Exadata Cloud Service and you have converted your existing Exadata DB Systems to the new resource model, or if you do not use Exadata Cloud Service, then you can proceed with the update. In this case, you can enter option 1 to continue.
WARNING

Oracle E-Business Suite Cloud Manager Release 20.2.1.1.1 supports the new Exadata Cloud Service resource model. You should convert your Exadata DB Systems to this new model. Be aware that if you have not yet converted to the new model, and plan to provision Oracle E-Business Suite environments where the database is on an Exadata DB System that uses the old resource model, you must choose 2 to exit and remain on your existing Cloud Manager release.

Do you wish to continue??
1: yes
2: no

Enter your choice: 1

4. Choose the Oracle E-Business Suite Cloud Manager release from the choices provided:

Available Oracle E-Business Suite Cloud Manager release versions:
1: 20.2.1.1.1

Choose release version to upgrade from the above list: 1

5. When prompted, enter your Oracle E-Business Suite Cloud Manager administrator password:

Enter Oracle E-Business Suite Cloud Manager Admin Password:

Note: You will have already followed the steps in Configure Oracle E-Business Suite Cloud Manager Compute Instance, page 2-30, to configure your VM. At this prompt, enter the Oracle E-Business Suite Cloud Manager administrator password you specified at that time.

6. Before continuing with the upgrade, you should ensure that there are no activities in your Oracle E-Business Suite Cloud Manager with a status of In Progress, Scheduled, Paused, or Failed. Refer to Monitor Activity Status, page 12-1.

It is recommended that you allow In Progress and Scheduled activities to complete before continuing, resume any Paused activities, and restart any Failed activities that you want to try again. You can also choose to delete an incomplete installation or an incomplete backup to clean up any resources instead of restarting the Failed activity. If there are still any activities with a status of Failed when you perform the upgrade, their status will be changed to Aborted. In this case, you must manually clean up any incomplete resources from the activity after the upgrade.

When prompted, enter y to confirm that you want to continue:
Ensure that there are no Running, Scheduled or Failed Activities before upgrade. Failed activities will be marked as aborted and user has to do failed resource cleanup manually or user can finish cleanup of failed instances before proceeding.

Do you wish to continue [y/n]? y

7. The utility then displays several messages recording the actions it performs. Finally, it displays a screen containing a success message, similar to the following. You can optionally review the log file to verify further details about the upgrade.

====================================================================
==========================================
Oracle E-Business Suite Cloud Manager VM setup successful. Version: 20.2.1.1.1
Refer to /u01/install/APPS/apps-unlimited-ebs/out/self-update-
<date>_<time>.log for complete details.
====================================================================
==========================================

Migrate Version 19.2.1.2 to the Latest Codelevel (Conditional)
If you are on Oracle E-Business Suite Cloud Manager version 19.2.1.2, prior to running the Self Update utility to bring your version to the latest codelevel, you need to define additional policy statements. Then run the Self Update utility.

Define Additional Policies for Using "tag-namespaces"
The tenancy administrator performs the tasks in this section.

To accommodate the addition of tags, create new policies or add the following policy statements to existing policies:

Allow group <Oracle E-Business Suite Cloud Manager administrators group> to manage tag-namespaces in compartment <Oracle E-Business Suite Cloud Manager compartment>
Allow group <Oracle E-Business Suite administrators group> to use tag-namespaces in compartment <Oracle E-Business Suite Cloud Manager compartment>
Allow group <Oracle E-Business Suite Cloud Manager administrators group> to manage tag-namespaces in compartment <Oracle E-Business Suite compartment>
Allow group <Oracle E-Business Suite administrators group> to use tag-namespaces in compartment <Oracle E-Business Suite compartment>
Allow group <Oracle E-Business Suite Cloud Manager administrators group> to use tag-namespaces in tenancy where target.tag-namespace.name='Oracle-Tags'

For example, create a new policy using the following steps:

1. From the Oracle Cloud Infrastructure console navigation menu, under Governance and Administration, select Identity, and then click Policies.

2. Select the desired compartment from the drop-down list on the left.

3. Click Create Policy.
4. In the dialog window, enter the required details as follows:
   - **NAME**: Enter a name. For example, ebstag-policy.
   - **DESCRIPTION**: Enter a suitable description.
   - Add your desired policy statements.

5. Click **Create Policy**.

**Perform the Migration Tasks**

Perform the following steps:

1. Connect to the Oracle E-Business Suite Cloud Manager VM using SSH and switch from the opc user to the oracle user.
   
   `sudo su - oracle`

2. Run the Self Update utility as follows:
   
   `$ cd /u01/install/APPS/apps-unlimited-ebs/bin
   $ perl selfUpdate.pl`

3. Review the warning for Exadata Cloud Service customers and check whether you are ready to proceed with the update to Release 20.2.1.1.1. If you use Exadata Cloud Service and you are not ready to convert to the new resource model, then you must enter option 2 to exit the utility and remain on your existing Oracle E-Business Suite Cloud Manager release of 20.2.1.1 or earlier.

   If you use Exadata Cloud Service and you have converted your existing Exadata DB Systems to the new resource model, or if you do not use Exadata Cloud Service, then you can proceed with the update. In this case, you can enter option 1 to continue.

   ************************************************************ WARNING
   Oracle E-Business Suite Cloud Manager Release 20.2.1.1.1 supports the new Exadata Cloud Service resource model. You should convert your Exadata DB Systems to this new model. Be aware that if you have not yet converted to the new model, and plan to provision Oracle E-Business Suite environments where the database is on an Exadata DB System that uses the old resource model, you must choose 2 to exit and remain on your existing Cloud Manager release.

   Do you wish to continue??
   1: yes
   2: no

   Enter your choice: 1
4. Choose the Oracle E-Business Suite Cloud Manager release from the choices provided:

Available Oracle E-Business Suite Cloud Manager release versions:

1: 20.2.1.1.1

Choose release version to upgrade from the above list: 1

5. When prompted, enter your Oracle E-Business Suite Cloud Manager administrator password:

Enter Oracle E-Business Suite Cloud Manager Admin Password :

Note: You will have already followed the steps in Configure Oracle E-Business Suite Cloud Manager Compute Instance, page 2-30, to configure your VM. At this prompt, enter the Oracle E-Business Suite Cloud Manager administrator password you specified at that time.

6. Before continuing with the upgrade, you should ensure that there are no activities in your Oracle E-Business Suite Cloud Manager with a status of In Progress, Scheduled, or Failed. Refer to Monitor Activity Status, page 12-1.

It is recommended that you allow In Progress and Scheduled activities to complete before continuing, and restart any Failed activities that you want to try again. You can also choose to delete an incomplete installation or an incomplete backup to clean up any resources instead of restarting the Failed activity. If there are still any activities with a status of Failed when you perform the upgrade, their status will be changed to Aborted. In this case, you must manually clean up any incomplete resources from the activity after the upgrade.

When prompted, enter y to confirm that you want to continue:

Ensure that there are no Running, Scheduled or Failed Activities before upgrade.
Failed activities will be marked as aborted and user has to do failed resource cleanup manually or user can finish cleanup of failed instances before proceeding.

Do you wish to continue [y/n]? y

7. The utility then displays several messages recording the actions it performs. Finally, it displays a screen containing a success message, similar to the following. You can optionally review the log file to verify further details about the upgrade.

====================================================================
==========================================
Oracle E-Business Suite Cloud Manager VM setup successful.
Version: 20.2.1.1.1
Refer to /u01/install/APPS/apps-unlimited-ebs/out/self-update-<date>_<time>.log for complete details.
====================================================================
==========================================
Migrate Version 19.1.1 through 19.2.1.1 to the Latest Codelevel (Conditional)

If you are on Oracle E-Business Suite Cloud Manager version 19.1.1 or later, up to and including 19.2.1.1, you must first upgrade to version 19.3.1.2. Then you can migrate from that version to the latest codelevel.

Prior to running the Self Update utility to bring your version to 19.3.1.2, you need to define additional policy statements. Then, run the Self Update utility to migrate to version 19.3.1.2.

If you are upgrading from 19.1.1.X, you must then complete the 19.3.1.2 configuration by running the `UpdateOCINetwork.pl` script to update the network profile for Oracle E-Business Suite Cloud Manager.

Finally, you can migrate from version 19.3.1.2 to the latest codelevel.

Define Additional Policies for Using "tag-namespaces"

The tenancy administrator performs the tasks in this section.

To accommodate the addition of tags, create new policies or add the following policy statements to existing policies:

- Allow group `<Oracle E-Business Suite Cloud Manager administrators group>` to manage tag-namespaces in compartment `<Oracle E-Business Suite Cloud Manager compartment>`
- Allow group `<Oracle E-Business Suite administrators group>` to use tag-namespaces in compartment `<Oracle E-Business Suite Cloud Manager compartment>`
- Allow group `<Oracle E-Business Suite Cloud Manager administrators group>` to manage tag-namespaces in compartment `<Oracle E-Business Suite compartment>`
- Allow group `<Oracle E-Business Suite administrators group>` to use tag-namespaces in compartment `<Oracle E-Business Suite compartment>`
- Allow group `<Oracle E-Business Suite Cloud Manager administrators group>` to use tag-namespaces in tenancy where `target.tag-namespace.name='Oracle-Tags'`

For example, create a new policy using the following steps:

1. From the Oracle Cloud Infrastructure console navigation menu, under Governance and Administration select Identity and then click Policies.

2. Select the desired compartment from the drop-down list on the left.

3. Click Create Policy.

4. In the dialog window, enter the required details as follows:
   - NAME: Enter a name (for example, ebstag-policy).
   - DESCRIPTION: Enter a suitable description.
   - Add your desired policy statements.

5. Click Create Policy.
Perform the Migration Tasks

Perform the following steps:

1. Connect to the Oracle E-Business Suite Cloud Manager VM using SSH and switch from the opc user to the oracle user.
   
   $ sudo su - oracle

2. Run the Self Update utility as follows:
   
   $ cd /u01/install/APPS/apps-unlimited-ebs/bin
   
   $ perl selfUpdate.pl

3. Choose the Oracle E-Business Suite Cloud Manager release from the choices provided:

   Available Oracle E-Business Suite Cloud Manager release versions:
   
   1: 19.3.1.2

   Choose release version to upgrade from the above list: 1

4. When prompted, enter your Oracle E-Business Suite Cloud Manager administrator password:

   Enter Oracle E-Business Suite Cloud Manager Admin Password :

   Note: You will have already followed the steps in Configure Oracle E-Business Suite Cloud Manager Compute Instance, page 2-30 to configure your VM. At this prompt, enter the Oracle E-Business Suite Cloud Manager administrator password you specified at that time.

5. Before continuing with the upgrade, you should ensure that there are no activities in your Oracle E-Business Suite Cloud Manager with a status of In Progress, Scheduled, or Failed. Refer to Monitor Activity Status, page 12-1.

   It is recommended that you allow In Progress and Scheduled activities to complete before continuing, and restart any Failed activities that you want to try again. You can also choose to delete an incomplete installation or an incomplete backup to clean up any resources instead of restarting the Failed activity. If there are still any activities with a status of Failed when you perform the upgrade, their status will be changed to Aborted. In this case, you must manually clean up any incomplete resources from the activity after the upgrade.

   When prompted, enter y to confirm that you want to continue:
Ensure that there are no Running, Scheduled or Failed Activities before upgrade. Failed activities will be marked as aborted and user has to do failed resource cleanup manually or user can finish cleanup of failed instances before proceeding.

Do you wish to continue [y/n]? y

6. The utility then displays several messages recording the actions it performs. Finally, it displays a screen containing a success message, similar to the one below. You can optionally review the log file to verify further details about the upgrade.

====================================================================
Oracle E-Business Suite Cloud Manager VM setup successful. Version: 19.3.1.2
Refer to /u01/install/APPS/apps-unlimited-ebs/out/self-update-<date>_<time>.log for complete details.
====================================================================

Run UpdateOCINetwork.pl (Conditional)

**Note:** The Oracle E-Business Suite Cloud Manager administrator performs the tasks described in this section.

If you are upgrading from 19.1.1.X, the Oracle E-Business Suite Cloud Manager administrator, you must run the UpdateOCINetwork.pl script to update the network profile for Oracle E-Business Suite Cloud Manager.

1. As the oracle user, run the UpdateOCINetwork.pl script using the following commands:

```
$ sudo su - oracle
$ cd /u01/install/APPS/apps-unlimited-ebs/bin
$ perl UpdateOCINetwork.pl
```

Run the Self Update Utility to Migrate from 19.3.1.2 to the Latest Codelevel

Complete the migration by following the steps in Migrate Version 19.3.1.X or Later to the Latest Codelevel, page 4-4.

Perform Oracle E-Business Suite Cloud Manager Administration Tasks

This section covers how to perform administrative tasks on the Oracle E-Business Suite Cloud Manager VM, categorized into three sections:

- **Manage Services** - The ebscloudmgrctl.sh script is used to manage services, which include the following tasks:
  - Start Services, page 4-13
  - Stop Services, page 4-13
• Review or Change Configurations - The ebscmadmin utility is used to review or change configurations, which include the following tasks:
  • Check the Oracle E-Business Suite Cloud Manager Version, page 4-14
  • Change the Oracle E-Business Suite Cloud Manager Administration Password, page 4-15
  • Change the Oracle E-Business Suite Cloud Manager Administrator Group, page 4-16
  • View a List of Compatible Load Balancers, page 4-17
  • Change the Load Balancer Associated with Your Oracle E-Business Suite Cloud Manager VM, page 4-17
  • Update the Oracle E-Business Suite Cloud Manager Load Balancer URL, page 4-14
  • Update the Oracle E-Business Suite Cloud Manager Load Balancer Fully Qualified Domain Name (FQDN), page 4-18
  • Update the Oracle Identity Service Cloud Configuration, page 4-19
  • Change the Parallel Worker Count, page 4-20
  • Create a User Profile, page 4-20
  • Enable Mailer Configuration, page 4-21
  • Disable Mailer Configuration, page 4-21
  • Tag an Oracle E-Business Suite Environment, page 4-21

• Standalone Tasks
  • Replace the Self-Signed Certificate for the Oracle E-Business Suite Cloud Manager Load Balancer with a Certificate Authority Issued Certificate, page 4-22
  • Refresh Metadata for an Environment Upgraded to Oracle Database 19c, page 4-23
  • Rediscover an Environment Upgraded to Oracle E-Business Suite Release 12.2, page 4-25
**Note:** Apart from Start Services and Stop Services, these tasks are optional.

**Common Command Line Arguments:**
The following are common arguments to many of the commands described in this section.

**Passwords**
In many instances, the command line help will indicate that a password is required. The following is an example of how to securely provide a password to a command line utility such as `ebscmadmin`:

```bash
$ { echo <EBSCM_admin_password>; } | ebscmadmin <command> [arguments]
```

**Configuration File**
The configuration file refers to a file created as part of the user profile. This file is typically located in the Oracle E-Business Suite Cloud Manager Compute instance in the directory `/u01/install/APPS/.oci`. Take note of the configuration file for your user, as this is a required argument for some commands.

**Manage Services:**
Use `ebscloudmgrctl.sh` for managing services.

**Start Services**
Perform the following steps to start services.

1. As the `oracle` user, run `ebscloudmgrctl.sh` with the `startall` command.
   ```bash
   $ sudo su - oracle
   $ cd /u01/install/APPS/apps-unlimited-ebs/bin
   $ sh ebscloudmgrctl.sh startall
   ```

2. Enter the Oracle E-Business Suite Cloud Manager administrator password when prompted.
   
Enter Oracle E-Business Suite Cloud Manager Admin Password:

**Stop Services**
Perform the following steps to stop services.

1. As the `oracle` user, run `ebscloudmgrctl.sh` with the `stopall` command.
   ```bash
   $ sudo su - oracle
   $ cd /u01/install/APPS/apps-unlimited-ebs/bin
   $ sh ebscloudmgrctl.sh stopall
   ```

2. Enter the Oracle E-Business Suite Cloud Manager administrator password when prompted.
Enter Oracle E-Business Suite Cloud Manager Admin Password:

Abort Running Jobs
Perform the following steps to abort all jobs and stop all services.

1. As the oracle user, run ebscloudmgrctl.sh with stopall force.
   
   ```
   $ sudo su - oracle
   $ cd /u01/install/APPS/apps-unlimited-ebs/bin
   $ sh ebscloudmgrctl.sh stopall force
   ```

2. Enter the Oracle E-Business Suite Cloud Manager administrator password when prompted.

   Enter Oracle E-Business Suite Cloud Manager Admin Password:

Review or Change Configurations:
Use the ebscmadmin utility for reviewing or changing configurations.

For help with ebscmadmin, run $ ./ebscmadmin -h.

To get detailed help on a particular command, run $ ./ebscmadmin <command> -h.

Check the Oracle E-Business Suite Cloud Manager Version
Use this command to check what version of Oracle E-Business Suite Cloud Manager you currently have deployed.

As the oracle user, change to the appropriate directory, and run ebscmadmin with the ebscm-version-details command.

For example:

```
$ sudo su - oracle
$ cd /u01/install/APPS/apps-unlimited-ebs/bin
$ ./ebscmadmin ebscm-version-details
```

This will display your current version Oracle E-Business Suite Cloud Manager, the latest version that is available, as well as a brief message summarizing whether or not you need to or are able to upgrade.

Update the Oracle E-Business Suite Cloud Manager Load Balancer URL
Use this command if you wish to use a DNS-registered host name instead of a public IP address in the Oracle E-Business Suite Cloud Manager UI URL.

For example, if the Oracle E-Business Suite Cloud Manager UI is already configured, the load balancer URL is `https://192.0.2.1:443`, and you have registered the IP address `192.0.2.1` in your DNS server as `example.com`, then you can pass the URL `https://example.com:443` as the LBaaS URL to the utility by using the steps shown in the following example.

1. As the oracle user, change to the appropriate directory, and run ebscmadmin with the update-load-balancer-url command followed by an argument.
For example:

```
$ sudo su - oracle
$ cd /u01/install/APPS/apps-unlimited-ebs/bin
$ ./ebscmadmin update-load-balancer-url --load-balancer-url=https://example.com:443
```

Run `./ebscmadmin update-load-balancer-url -h` to review all available arguments for this command.

2. When prompted, enter the Oracle E-Business Suite Cloud Manager administrator password.

   Enter Oracle E-Business Suite Cloud Manager Administration Password:

3. You will then see a confirmation screen indicating that the configuration of the Oracle E-Business Suite Cloud Manager VM is complete. The following is an example of the confirmation message.

   Oracle E-Business Suite Cloud Manager Load Balancer URL updated successfully.
   Ensure the confidential application is correctly configured in IDCS as per the documentation.

4. Now, sign on to the Oracle Identity Cloud Service Console.

5. Expand the menu located in the top left corner, and select Applications.

6. Search for the confidential application that needs to be updated.

7. Click Confidential Application.

8. Navigate to the Configuration tab.


10. Review and update the values of the Redirect URL and Post Logout Redirect URL fields.

11. Click Save.

**Change the Oracle E-Business Suite Cloud Manager Administration Password**

Use this command if you wish to change the Oracle E-Business Suite Cloud Manager administration password.

1. As the oracle user, change to the appropriate directory, and run `ebscmadmin` with the `change-admin-password` command.

   For example:

   ```
   $ sudo su - oracle
   $ cd /u01/install/APPS/apps-unlimited-ebs/bin
   $ ./ebscmadmin change-admin-password
   ```
Run `. /ebscmadmin change-admin-password -h` to review all available arguments for this command.

2. When prompted, enter your current Oracle E-Business Suite Cloud Manager administration password, specify the new password, and then re-enter the new password to confirm it.

   Enter Current Oracle E-Business Suite Cloud Manager Administration Password:

   Enter New Oracle E-Business Suite Cloud Manager Administration Password:

   Re-enter New Oracle E-Business Suite Cloud Manager Administration Password:

3. The following message appears indicating that you have successfully changed the Oracle E-Business Suite Cloud Manager administration password.

   Oracle E-Business Suite Cloud Manager administration Password changed successfully.

Change the Oracle E-Business Suite Cloud Manager Administrator Group

Use this command if you wish to change the Oracle E-Business Suite Cloud administrator group.

1. As the `oracle` user, change to the appropriate directory, and run `ebscmadmin` with the `change-admin-group` command.

   For example:

   ```
   $ sudo su - oracle
   $ cd /u01/install/APPS/apps-unlimited-ebs/bin
   $ ./ebscmadmin change-admin-group <argument>
   
   Run `. /ebscmadmin change-admin-group -h` to review the appropriate arguments for this command.
   ```

2. Once you run the command, the following screen appears indicating that you have successfully changed the Oracle E-Business Suite Cloud Manager administrator group.

   Created log file: /u01/install/APPS/apps-unlimited-ebs/out/ebscmadmin/change-admin-group_20201120_022249.log

   Validating if user is authorized member of Oracle E-Business Suite Cloud Administrator Group
   User is part of Oracle E-Business Suite Cloud Manager Administrator Group OCID: ocid1.group.oc1.
   xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

   Validating Group OCID
   Changing Oracle E-Business Suite Cloud Manager Admin Group..
   Stopping Node and Job Server if running.
   Starting Node and Job Server.
   Oracle E-Business Suite Cloud Manager Admin Group changed successfully.
View a List of Compatible Load Balancers
Use this command to view a list of all load balancers that can be configured with your specific orchestration VM.

1. As the oracle user, run ebscmadmin with the list-compatible-load-balancers command.

For example:

```bash
$ sudo su - oracle
$ cd /u01/install/APPS/apps-unlimited-ebs/bin
$ ./ebscmadmin list-compatible-load-balancers <argument>
```

Run ./ebscmadmin list-compatible-load-balancers -h to review the appropriate arguments for this command.

2. A log file is created and a list of available load balancers is displayed.

Created log file: /u01/install/APPS/apps-unlimited-ebs/out/ebscmadmin/list-compatible-load-balancers_20201120_022822.log

Getting list of available Load Balancers. Please wait.

Available Load Balancers:
1: ebs-prov-vm-lbaas -- ocid1.loadbalancer.oc1.uk-london-1.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
2: ebs1-lbaas -- ocid1.loadbalancer.oc1.uk-london-1.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
3: ebs2-lbaas -- ocid1.loadbalancer.oc1.uk-london-1.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Change the Load Balancer Associated with Your Oracle E-Business Suite Cloud Manager VM
Use this command if you wish to reconfigure the Oracle E-Business Suite Cloud Manager VM with a different load balancer. The utility will allow you to choose from a list of existing load balancers within your compartment.

1. As the oracle user, run ebscmadmin with the change-load-balancer command.

For example:

```bash
$ sudo su - oracle
$ cd /u01/install/APPS/apps-unlimited-ebs/bin
$ ./ebscmadmin change-load-balancer <argument>
```

Run ./ebscmadmin change-load-balancer -h to review the appropriate arguments for this command.

The following is an example of the confirmation message that is displayed.

Ensure the confidential application is correctly configured in IDCS as per the documentation.
Oracle E-Business Suite Cloud Manager URL: https://xxx.xxx.xxx.xxx:
Use "ebscmadmin update-load-balancer-url" command to update Oracle E-Business Suite Cloud Manager URL (Optional)
2. Now, sign on to the Oracle Identity Cloud Service Console.

3. Expand the menu located in the top left corner, and select Applications.

4. Search for the confidential application that needs to be updated.

5. Click Confidential Application.

6. Navigate to the Configuration tab.

7. Expand Client Configuration.

8. Review and update the values of the Redirect URL and Post Logout Redirect URL fields.

9. Click Save.

Update the Oracle E-Business Suite Cloud Manager Load Balancer Fully Qualified Domain Name

Use this command to update the fully qualified domain name (FQDN) of your Oracle E-Business Suite Cloud Manager load balancer.

1. As the oracle user, change to the appropriate directory, and run ebscmadmin with the update-load-balancer-fqdn command.

   For example:

   ```
   $ sudo su - oracle
   $ cd /u01/install/APPS/apps-unlimited-ebs/bin
   $ ./ebscmadmin update-load-balancer-fqdn <argument>
   ```

   Run ./ebscmadmin update-load-balancer-fqdn -h to review the appropriate arguments for this command.

   After running the command with the proper arguments, the output will look similar to the following:
Created log file: /u01/install/APPS/apps-unlimited-ebs/out/ebscadmin/update-load-balancer-fqdn_<date>_<time>.log

Validating if user is an authorized member of Oracle E-Business Suite Cloud Administrator Group
User is part of Oracle E-Business Suite Cloud Manager Administrator Group OCID: ocid1.group.oc1..<xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Deriving load balancer details of Oracle E-Business Suite Cloud Manager VM.
Creating OCI certificate resource.
Updating OCI Listener, yc3-ashburn-prov-vm-listener resource.
Updating load balancer frontend host in database.
Starting Node and Job Server if running.

Following public certificate is used for OCI certificate resource.
Public certificate: /u01/install/APPS/apps-unlimited-ebs/orcvm-state/signedcertificates/example.com_exdemocert.crt
Oracle E-Business Suite Cloud Manager URL: https://example.com:8082
Note: Ensure the confidential application is correctly configured in IDCS as per the Oracle E-Business Suite Cloud Manager Guide.

2. Now, sign on to the Oracle Identity Cloud Service Console.

3. Expand the menu located in the top left corner, and select Applications.

4. Search for the confidential application that needs to be updated.

5. Click Confidential Application.

6. Navigate to the Configuration tab.

7. Expand Client Configuration.

8. Review and update the values of the Redirect URL and Post Logout Redirect URL fields.

9. Click Save.

Update the Oracle Identity Service Cloud Configuration
Use this command if you wish to change your Oracle Identity Cloud Service configuration.

1. As the oracle user, change to the appropriate directory, and run ebscadmin with the update-idcs-configuration command.

For example:

$ sudo su - oracle
$ cd /u01/install/APPS/apps-unlimited-ebs/bin
$ ./ebscadmin update-idcs-configuration <argument>

Run ./ebscadmin update-idcs-configuration -h to review the appropriate arguments for this command.
After running the command with the proper arguments, a confirmation message is displayed:

Oracle E-Business Suite Cloud Manager IDCS details updated successfully.
Ensure the confidential application is correctly configured in IDCS as per the documentation.

2. Now, sign in to the Oracle Identity Cloud Service Console.

3. Expand the menu located in top left corner, and select Applications.

4. Search for the confidential application that needs to be updated.

5. Click Confidential Application.

6. Navigate to the Configuration tab.

7. Expand Client Configuration.

8. Review and update the values of the Redirect URL and Post Logout Redirect URL fields.

9. Click Save.

**Change the Parallel Worker Count**

Use this command to specify the number of jobs that will be run in parallel, by updating the parallel worker count.

As the oracle user, change to the appropriate directory, and run ebscmadmin with the update-worker-count command.

For example:

```
$ sudo su - oracle
$ cd /u01/install/APPS/apps-unlimited-ebs/bin
$ ./ebscmadmin update-worker-count <argument>
```

Run ./ebscmadmin update-worker-count -h to review the appropriate arguments for this command.

After running the command with the proper arguments, a confirmation message is displayed:

Worker count updated successfully.

**Create a User Profile**

Use this command to create a user profile.

As the oracle user, change to the appropriate directory, and run ebscmadmin with the create-user-profile command.

For example:
$ sudo su - oracle
$ cd /u01/install/APPS/apps-unlimited-ebs/bin
$ ./ebscmdadmin create-user-profile <argument>

Run ./ebscmdadmin create-user-profile -h to review the appropriate arguments for this command.

After running the command with the proper arguments, the output will look similar to the following:

Created/Updated user specific OCI configuration file <configuration file location> successfully.
User profile creation completed successfully.

Enable Mailer Configuration
Use this command to enable mailer configuration for Oracle E-Business Suite Cloud Manager.

As the oracle user, change to the appropriate directory, and run ebscmdadmin with the enable-mailer command.

For example:
$ sudo su - oracle
$ cd /u01/install/APPS/apps-unlimited-ebs/bin
$ ./ebscmdadmin enable-mailer <argument>

Run ./ebscmdadmin enable-mailer -h to review the appropriate arguments for this command.

After running the command with the proper arguments, a confirmation message is displayed.
Successfully enabled mailer configuration.

Disable Mailer Configuration
Use this command to disable mailer configuration for Oracle E-Business Suite Cloud Manager.

As the oracle user, change to the appropriate directory, and run ebscmdadmin with the disable-mailer command.

For example:
$ sudo su - oracle
$ cd /u01/install/APPS/apps-unlimited-ebs/bin
$ ./ebscmdadmin disable-mailer <argument>

Run ./ebscmdadmin disable-mailer -h to review the appropriate arguments for this command.

After running the command with the proper arguments, a confirmation message is displayed.
Successfully disabled mailer configuration.

Tag Oracle E-Business Suite Environments
Use this command to tag all Oracle E-Business Suite environments associated with your Oracle E-Business Suite Cloud Manager.
As the oracle user, change to the appropriate directory, and run ebscmadmin with the tag-ebs-environments command.

For example:

```
$ sudo su - oracle
$ cd /u01/install/APPS/apps-unlimited-ebs/bin
$ ./ebscmadmin tag-ebs-environments <argument>
```

Run ./ebscmadmin tag-ebs-environments -h to review the appropriate arguments for this command.

After running the command with the proper arguments, you will see output similar to the following example:

```
Created log file: /u01/install/APPS/apps-unlimited-ebs/out/ebscmadmin/tag-ebs-environments_20201111_173423.log
```

Creating Namespace oracle-apps
Creating Tag key purpose
Tagging all EBS instances.
Tagging EBSCM.

**Standalone Tasks:**

**Replace the Self-Signed Certificate for the Oracle E-Business Suite Cloud Manager Load Balancer with a Certificate Authority Issued Certificate**

When you configure Oracle E-Business Suite Cloud Manager, the listener of the Load Balancer as a Service (LBaaS) is TLS enabled for HTTP inbound connections to Oracle E-Business Suite Cloud Manager. The certificate that is deployed by default for this configuration is a self-signed certificate. You can update the self-signed certificate with a certificate authority (CA) issued certificate using the following steps:

1. By default the Oracle E-Business Suite Cloud Manager URL uses an IP address rather than a host name. The first step is to map the Oracle E-Business Suite IP address to a host name.

   **Note:** Oracle Cloud Infrastructure provides a public IP address but does not provide a public host name; therefore, you should ensure that appropriate DNS entries are present to resolve host name to the public IP address.

2. Update the Oracle E-Business Suite Cloud Manager VM by following the instructions in Update the Oracle E-Business Suite Cloud Manager URL, page 4-14.

3. Obtain a certificate for the host name from a certificate authority.

4. Log in to the Oracle Cloud Infrastructure console. From the navigation menu, select **Networking**, then **Load Balancers**, and then select the load balancer you want to configure.

   Add your certificate bundle to the load balancer. See To upload an SSL certificate
bundle to your load balancing system [https://docs.cloud.oracle.com/iaas/Content/Balance/Tasks/managingcertificates.htm#add] in the Oracle Cloud Infrastructure Services documentation.

If you have multiple certificates that form a single certification chain, such as one or more intermediate certificates together with a root certificate, then you must include all relevant certificates in one file before you upload them to the system. Refer to "Uploading Certificate Chains" in Working with SSL Certificates [https://docs.cloud.oracle.com/iaas/Content/Balance/Tasks/managingcertificates.htm#working] in the Oracle Cloud Infrastructure Documentation.

5. While still on the Load Balancer page, click the **Listeners** link under the Resources menu on the left.

6. Search for the Oracle E-Business Suite Cloud Manager’s listener. Note that there can be multiple listeners associated, as the same load balancer can be used by more than one Oracle E-Business Suite Cloud Manager. Ensure to pick the listener corresponding to the Oracle E-Business Suite Cloud Manager you are using.

7. Click the **Actions** icon (three dots) associated with the Oracle E-Business Suite Cloud Manager’s listener’s row, select **Edit** from the context menu.

8. In the Edit Listener dialog window, select the certificate bundle added above in the **Certificate Name** drop-down list. Click **Save Changes** and wait for the listener to be updated.

**Refresh Metadata for an Environment Upgraded to Oracle Database 19c**

If you use Oracle E-Business Suite Cloud Manager to deploy an environment with Oracle Database 12.1.0.2 or 11.2.0.4, and you manually upgrade that environment to Oracle Database 19c, then Oracle E-Business Suite Cloud Manager can no longer recognize that environment.

For the following types of environments, you can run a script to refresh the metadata for the upgraded environment within Oracle E-Business Suite Cloud Manager.

- Environments with the database tier on Compute, upgraded from Oracle Database 12.1.0.2 or 11.2.0.4 to Oracle Database 19c

- Environments with the database tier on Exadata Cloud Service, upgraded from Oracle Database 12.1.0.2 or 11.2.0.4 to Oracle Database 19c

After the environment metadata has been refreshed, you can once again manage the environment through the Oracle E-Business Suite Cloud Manager UI.

**Refresh Metadata for an Environment Upgraded to Oracle Database 19c on Compute**

To refresh the Oracle E-Business Suite Cloud Manager metadata for an environment upgraded to Oracle Database 19c on Compute, perform the following steps:
1. Ensure you are using at minimum Oracle E-Business Suite Cloud Manager Version 20.1.1.2.1. If you need to update your version, follow the instructions in Update Oracle E-Business Suite Cloud Manager to the Latest Version, page 4-1.

2. Run the `refreshComputeDBMetadata.pl` script using the following command. Specify the database context file and environment name for the environment, and specify the location and name for the log file.

   ```
   $ cd /u01/install/APPS/apps-unlimited-ebs/bin
   $ perl refreshComputeDBMetadata.pl --contextfile=<full path to database context file on the database node> --environment=<environment name> --logfile=<full path to log file>
   ```

3. When prompted, enter the Oracle E-Business Suite Cloud Manager administrator password and the password for the APPS user for the environment.

   ```
   Enter the Oracle E-Business Suite Cloud Manager Admin password: 
   Enter the APPS user password:
   ```

4. After the script completes, log into Oracle E-Business Suite Cloud Manager and verify the updated information for the environment in the environment details.

---

**Refresh Metadata for an Environment Upgraded to Oracle Database 19c on Exadata Cloud Service**

To refresh the Oracle E-Business Suite Cloud Manager metadata for an environment upgraded to Oracle Database 19c on Exadata Cloud Service, perform the following steps:

1. Ensure you are using at minimum Oracle E-Business Suite Cloud Manager Version 20.1.1.2.1. If you need to update your version, follow the instructions in Update Oracle E-Business Suite Cloud Manager to the Latest Version, page 4-1.

2. Run the `refreshExaDbMetadata.pl` script using the following command. Specify the database context file and environment name for the environment, and specify the location and name for the log file.

   ```
   $ cd /u01/install/APPS/apps-unlimited-ebs/bin
   $ perl refreshExaDbMetadata.pl --contextfile=<full path to database context file on the database node> --environment=<environment name> --logfile=<full path to log file>
   ```

3. When prompted, enter the Oracle E-Business Suite Cloud Manager administrator password and the password for the APPS user for the environment.

   ```
   Enter the Oracle E-Business Suite Cloud Manager Admin password: 
   Enter the APPS user password:
   ```

4. After the script completes, log into Oracle E-Business Suite Cloud Manager and verify the updated information for the environment in the environment details.
Rediscover an Environment Upgraded to Oracle E-Business Suite Release 12.2

If you use Oracle E-Business Suite Cloud Manager to deploy an Oracle E-Business Suite Release 12.1 environment, and you manually upgrade that environment to Oracle E-Business Suite Release 12.2, then you must run scripts to rediscover the upgraded environment and update its metadata within Oracle E-Business Suite Cloud Manager. After performing rediscovery, you can continue managing the environment through the Oracle E-Business Suite Cloud Manager UI.

The following scripts are provided to enable rediscovery:

- **unregister-environment.js** - This script end dates the existing metadata entry for the environment and deletes it from the Chef repository.

- **discover-environment.js** - This script performs prediscovery validation, and, if the validation succeeds, submits a discovery job to rediscover the upgraded environment.

- **discovery-status.js** - This script lets you check the status of a discovery job submitted through the discover-environment.js script.

- **withdraw-discover.js** - This script withdraws a failed discovery request to enable you to retry the discovery. You must withdraw a failed discovery request to clean up its registration metadata before you can submit a new discovery request for the same environment.

These scripts are located in the `/u01/install/APPS/apps-unlimited-ebs/bin/rediscovery` directory. The log file for the scripts is stored in the following location: `/u01/install/APPS/apps-unlimited-ebs/out/NodeJSClient.log`

**Important**: Before performing rediscovery, ensure that the Resource Owner option is selected under Allowed Grant Types in the registration of Oracle E-Business Suite Cloud Manager as an application in Oracle Identity Cloud Service (IDCS). See Register Oracle E-Business Suite Cloud Manager as a Confidential Application, page 2-36.

Additionally, if you upgraded your Oracle E-Business Suite environment from Release 12.1.3 to Release 12.2 using a new VM, separate from the VM where the Release 12.1.3 environment is located, then you must perform the corresponding load balancer configuration after the upgrade. You should complete the load balancer configuration before performing rediscovery. See “Upgrading to Oracle E-Business Suite Release 12.2” in My Oracle Support Knowledge Document 2517025.1, Getting Started with Oracle E-Business Suite on Oracle Cloud.
If you performed the Oracle E-Business Suite upgrade on the same VM as the Release 12.1.3 environment, then you do not need to change the load balancer configuration.

To rediscover an environment upgraded to Oracle E-Business Suite Release 12.2, perform the following steps:

1. Ensure you are using at minimum Oracle E-Business Suite Cloud Manager Version 20.2.1.1. If you need to update your version, follow the instructions in Update Oracle E-Business Suite Cloud Manager to the Latest Version, page 4-1.

2. Run the `unregister-environment.js` script using the following commands.

   ```bash
   $ cd /u01/install/APPS/apps-unlimited-ebs/bin/rediscovery
   $ node unregister-environment.js
   ``

   When prompted, specify the name of the upgraded environment, your Oracle Identity Cloud Service user name and password, and your Oracle E-Business Suite Cloud Manager administrator password.

3. Create a stage directory on the database node of the upgraded environment to store metadata gathered during the discovery job. For example: `/tmp/stage`

4. Run the `discover-environment.js` script using the following commands.

   ```bash
   $ cd /u01/install/APPS/apps-unlimited-ebs/bin/rediscovery
   $ node discover-environment.js
   ``

   When prompted, specify the following details:
   - A name for the discovery request.
   - The name of the network profile used to provision the environment.
   - The IP address for the environment’s database node.
   - The stage directory you created for the discovery job on the database node.
   - The file path for the environment's database context file.
   - The APPS password for the environment.
   - Your Oracle Identity Cloud Service user name.
   - Your Oracle Identity Cloud Service password.
   - Your Oracle E-Business Suite Cloud Manager administrator password.
   - The load balancer configured for the environment. The script displays a list of
the load balancers that are registered in the load balancer subnet within the specified network profile. If this environment uses multiple zones for the application tier and has more than one load balancer, enter the list of load balancer names separated by commas.

- The listener for the environment. The script displays a list of the listeners configured for the specified load balancer. If this environment uses more than one listener, enter the list of listener names separated by commas.

5. If you need to check the status of a discovery job, run the discovery-status.js script using the following commands.

   ```
   $ cd /u01/install/APPS/apps-unlimited-ebs/bin/rediscovery
   $ node discovery-status.js
   ```

   When prompted, specify the discovery job ID assigned by the discover-environment.js script and your Oracle E-Business Suite Cloud Manager administrator password.

   **Tip:** The discover-environment.js script may take some time to complete. If you want to check the progress of a discovery job that is still running, open a separate terminal window to run the discovery-status.js script without disrupting the running discovery job.


7. If a discovery job failed, you must withdraw the failed discovery request before retrying discovery. To withdraw a request, run the withdraw-discover.js script using the following commands.

   ```
   $ cd /u01/install/APPS/apps-unlimited-ebs/bin/rediscovery
   $ node withdraw-discover.js
   ```

   When prompted, specify the name of the failed discovery request, your Oracle Identity Cloud Service user name and password, and your Oracle E-Business Suite Cloud Manager administrator password.

   After you have withdrawn the previous discovery request and corrected any issues that caused the discovery to fail, you can retry discovery by rerunning the discover-environment.js script.

### Manage Ksplice Uptrack Actions

Your Oracle E-Business Suite Cloud Manager virtual machine is installed with Ksplice
Uptrack software that allows you to enable automatic Linux kernel updates.

To configure Ksplice Uptrack to install updates automatically, enable the `autoinstall` option in `/etc/uptrack/uptrack.conf`.

For more information, including other Ksplice Uptrack capabilities, refer to the *Oracle Linux Ksplice User’s Guide* [https://docs.oracle.com/cd/E37670_01/E39380/html/ol_about_ksplice.html].
Part 3

Move On-Premises Oracle E-Business Suite Instances to Oracle Cloud Infrastructure
Create a Backup of an On-Premises Oracle E-Business Suite Instance on Oracle Cloud Infrastructure

This chapter covers the following topics:

- Overview of Creating Backups
- Verify Prerequisites for Traditional Lift and Shift
- Prepare the Source Oracle E-Business Suite Environment
- Deploy Oracle E-Business Suite Cloud Manager
- Install the Oracle E-Business Suite Cloud Backup Module
- Create an Advanced Configuration Parameters File (Optional)
- Create a Backup with the Oracle E-Business Suite Cloud Backup Module
- Troubleshoot Backup Issues

Overview of Creating Backups

You can use automated tools to create a backup of an on-premises source Oracle E-Business Suite environment on Oracle Cloud Infrastructure Object Storage, and to provision an environment on Oracle Cloud Infrastructure from that backup. We call this procedure a "traditional lift and shift".

This chapter describes how to begin this "traditional lift and shift" by using the Oracle E-Business Suite Cloud Backup Module to create the backup of your source environment on Oracle Cloud Infrastructure Object Storage. After you have created the backup of the source environment, you subsequently complete the lift and shift by using Oracle E-Business Suite Cloud Manager Advanced Provisioning to provision an environment on Oracle Cloud Infrastructure from the backup. See Advanced Provisioning, page 9-8.
Note: Although this process is intended primarily for on-premises source instances, you can also run the Oracle E-Business Suite Cloud Backup Module as part of a lift and shift in certain cases when the source environment is already in Oracle Cloud Infrastructure with optional database services. These cases include the following:

- You initially used a manual procedure, such as a platform migration, to migrate an environment to Oracle Cloud Infrastructure, and now would like to leverage Oracle E-Business Suite Cloud Manager to manage that environment going forward.

- You want to migrate your environment from one tenancy to another. The lift and shift procedure can be used for this purpose whether or not you are currently using Oracle E-Business Suite Cloud Manager.

Related Procedures

- Use the backup feature within Oracle E-Business Suite Cloud Manager to back up environments on Oracle Cloud Infrastructure that you previously provisioned through Oracle E-Business Suite Cloud Manager. See Create a Backup of a Cloud-Based Oracle E-Business Suite Instance, page 11-11.

- As an alternative to a traditional lift and shift, consider performing a “reduced downtime lift and shift” for your on-premises environment by creating a standby environment in Oracle Cloud Infrastructure and then promoting that standby environment. For more information and prerequisites, see Create a Standby Environment for Oracle Cloud Infrastructure from an On-Premises Environment, page 6-1.

Backup Procedure

Perform the following tasks to create a backup of an on-premises Oracle E-Business Suite instance on Oracle Cloud Infrastructure using the Oracle E-Business Suite Cloud Backup Module:

1. Verify prerequisites for traditional lift and shift., page 5-3

2. Prepare the source Oracle E-Business Suite environment., page 5-10

3. Deploy Oracle E-Business Suite Cloud Manager., page 5-12

4. Install the Oracle E-Business Suite Cloud Backup Module., page 5-12

5. Create an advanced configuration parameters file (optional)., page 5-13
6. Create a backup with the Oracle E-Business Suite Cloud Backup Module., page 5-15

7. Troubleshoot backup issues., page 5-26

Related Topics

Back up a Database to Object Storage Using RMAN [https://docs.cloud.oracle.com/en-us/iaas/Content/Database/Backup/backupOsRman.htm]


Oracle Database Backup and Recovery User’s Guide 12c Release 1 (12.1) [https://docs.oracle.com/database/121/BRADV/toc.htm]

Oracle Database Backup and Recovery User’s Guide 11g Release 2 (11.2) [https://docs.oracle.com/cd/E11882_01/backup.112/e10642/toc.htm]

Verify Prerequisites for Traditional Lift and Shift

You must have the following prerequisites to create a backup with the Oracle E-Business Suite Cloud Backup Module as part of a traditional lift and shift procedure:

- An Oracle E-Business Suite Cloud Manager instance set up as described in Deploy Oracle E-Business Suite Cloud Manager on Oracle Cloud Infrastructure, page 2-1.

- A source Oracle E-Business Suite instance that meets all prerequisites for the lift and shift automation including certified Oracle E-Business Suite and Oracle Database release versions as well as required patches based on the target database location. See Source Environment Requirements, page 5-4.

- A Linux server on which to run the Oracle E-Business Suite Cloud Backup Module. This server, which will be referred to in this section as the backup module server, can be located either on-premises or in OCI Compute. It can be a separate server that resides on your intranet, or can be one of the Oracle E-Business Suite nodes. Check with your network administrator and system administrator to see what is the most appropriate option for your organization. The backup module server must have at least 500 MB of free space, must have the wget libraries installed, and must have Perl 5.14 or later with the JSON module, either as the default Perl installation or through the Perl binary provided in the Oracle E-Business Suite Cloud Backup Module patch.

- Cloud resources that match or exceed the minimum recommendations specified in Cloud Services Minimum Resource Recommendations, page 5-7.

- An Oracle Cloud user who is a member of the Oracle E-Business Suite
administrators group that you defined according to Create and Map Groups in Oracle Cloud Infrastructure Identity and Access Management and Oracle Identity Cloud Service, page 2-7 or Create the Oracle E-Business Suite Administrators Group and Assign Policies, page 3-4.

- The user OCID for that user and your tenancy OCID. See Where to Get the Tenancy’s OCID and User’s OCID [https://docs.cloud.oracle.com/en-us/iaas/Content/API/Concepts/apisigningkey.htm#Other]. Copy and paste the user OCID and tenancy OCID to a file that you can reference when instructed to enter them later in these steps.

- An RSA key pair in PEM format, which must not be a passphrase protected key, uploaded to your user settings in the Oracle Cloud Infrastructure console. You will also need the fingerprint for the key. Ensure that you generate the key for your local Oracle Cloud Infrastructure user created in Oracle Cloud Infrastructure Identity and Access Management (IAM), not for an Oracle Identity Cloud Service user. See:
  
  - How to Generate an API Signing Key [https://docs.cloud.oracle.com/iaas/Content/API/Concepts/apisigningkey.htm#How]
  
  - How to Get the Key’s Fingerprint [https://docs.cloud.oracle.com/iaas/Content/API/Concepts/apisigningkey.htm#How3]
  
  - "To Upload an API Signing Key" in Using the Console [https://docs.cloud.oracle.com/iaas/Content/Identity/Tasks/managingcredentials.htm#three]

Copy and paste the PEM file location and the fingerprint to a file that you can reference when instructed to enter them later in these steps.

**Source Environment Requirements**

The source environment for a backup must be at a certified Oracle E-Business Suite release version as well as a certified Oracle Database release version, and must have the appropriate required patches applied. For a list of the certified Oracle E-Business Suite releases, certified Oracle Database releases, and required patches, refer to My Oracle Support Knowledge Document 2517025.1, Getting Started with Oracle E-Business Suite on Oracle Cloud Infrastructure [https://support.oracle.com/rs?type=doc&id=2517025.1], Section 4.2: Capabilities of Oracle E-Business Suite Automation Tools. These requirements vary depending on the target database tier location.

Additionally, the following are mandatory requirements for the on-premises systems which host your Oracle E-Business Suite source environment. These requirements must be met before you can create a backup of the source environment onto object storage as part of the lift and shift:

- You must have an NTP service configured on the on-premises application and database servers from which the backup will be taken. For Oracle Linux Release 7,

- You must have the `wget` library installed on the on-premises server where you plan to run the Oracle E-Business Suite Cloud Backup Module.

- The source database must be in ARCHIVELOG mode in order to perform a hot backup.

- If Transparent Data Encryption (TDE) is enabled for the source environment, then you should verify that all the pluggable databases (PDBs) pdbs are in an open state with an appropriate wallet type (autologin or password).

- If you plan to enable TLS for the target environment automatically - that is, if you plan to select the HTTPS protocol for the target environment's web entry point during provisioning - then you must apply the required updates and patches for TLS to the source environment before you create the backup.


**Additional Notes**

- For creating a backup with the target database tier on Oracle Cloud Infrastructure Compute VM, note that Compute supports only single-node databases. It does not support Oracle RAC databases.

- For creating a backup with a target database tier on a 1-Node or 2-Node VM DB System, you can choose from the following database edition options:
  - 1-Node VM DB System (Single Instance):
    - Enterprise Edition
    - Enterprise Edition High Performance
    - Enterprise Edition Extreme Performance
• 2-Node VM DB System (Oracle RAC)
  • Enterprise Edition Extreme Performance

• For creating a backup with the target database tier on Exadata Cloud Service:
  Exadata Cloud Service provides Oracle RAC support.

Beginning with Release 20.2.1.1.1 of the Oracle E-Business Suite Cloud Automation Tools, the only supported model for provisioning an environment on Exadata Cloud Service is the new resource model in which the Exadata infrastructure resource and the VM cluster resource are managed separately. If you are planning to provision an environment on Exadata Cloud Service, you must be on this new resource model. If you have existing Exadata DB systems in Oracle Cloud Infrastructure, you must switch them to the new resource model before you use them to provision new environments. See The New Exadata Cloud Service Resource Model [https://docs.oracle.com/en-us/iaas/Content/Database/Concepts/exaflexsystem.htm#exaflexsystem_topic-resource_model] and Switching an Exadata DB System to the New Resource Model and APIs [https://docs.oracle.com/en-us/iaas/Content/Database/Concepts/exaflexsystem_topic-resource_model_conversion.htm].

• The automated tools support lift and shift for a Linux source system to an Oracle Linux target system. If your environment is not currently running on Linux, see the question “Can I migrate my Oracle E-Business Suite instances on any operating system to Oracle Cloud?” in My Oracle Support Knowledge Document 2517025.1, Getting Started with Oracle E-Business Suite on Oracle Cloud Infrastructure [https://support.oracle.com/rs?type=doc&id=2517025.1]. Also refer to Create a Backup of an On-Premises Oracle E-Business Suite Instance on Oracle Cloud Infrastructure, page 5-2.

• The Oracle E-Business Suite Cloud Backup Module creates a backup of your primary application tier.

• Refer to Bare Metal and Virtual Machine DB Systems [https://docs.cloud.oracle.com/en-us/iaas/Content/Database/Concepts/overview.htm#StorageConsiderations] to determine the maximum database size supported by this procedure.

• For adequately low latency between the application and database tiers, your Oracle Cloud Infrastructure Compute and Oracle Database Cloud Service should be co-located in the same availability domain.

• You must provision the same database options in VM DB System or Exadata Cloud Service as on your source database, and the versions of the database options must be at the same level. Also, you should not provision any additional database options on the target database tier. The Oracle E-Business Suite Cloud Backup Module validates whether the database options in the source environment and in
the target database tier meet these requirements, and reports any mismatches.

- Cloning or deleting multiple databases on the same Exadata Cloud Service resource simultaneously is currently not recommended.

- You can download the E-Business Suite Technology Codelevel Checker tool, or ETCC, for Release 12.2 from My Oracle Support as Patch 17537119. Unzip this patch in the database Oracle home under $ORACLE_HOME/appsutil/etcc. You must run ETCC before running the Oracle E-Business Suite Cloud Backup Module to determine whether there are any important database fixes required by Oracle E-Business Suite to function properly.

- When you provision an environment on Oracle Cloud Infrastructure from a backup of a source environment, the storage type used depends on the database version, as follows:
  - Oracle Database Release 12.1.0.2 and Oracle Database Release 19c use Automatic Storage Management (ASM).
  - Oracle Database Release 11.2.0.4 uses ASM Cluster File System (ACFS).

**Cloud Services Minimum Resource Recommendations**

To provision an environment from backup, we recommend that you have cloud service resources that match or exceed those specified in the following table.

For information regarding Virtual Private Network (VPN) options, see the Oracle Cloud Infrastructure Networking website at [https://www.oracle.com/cloud/networking/](https://www.oracle.com/cloud/networking/)

<table>
<thead>
<tr>
<th>Description</th>
<th>Machine Type</th>
<th>Number of Nodes</th>
<th>OCPUs Allocated</th>
<th>Memory</th>
<th>Storage</th>
<th>External IPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Cloud Infrastructure Backup Service</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Size of application tier backup + database backup (object)</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Description</td>
<td>Machine Type</td>
<td>Number of Nodes</td>
<td>OCPUs Allocated</td>
<td>Memory</td>
<td>Storage</td>
<td>External IPs</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>--------------</td>
<td>-----------------</td>
<td>-----------------</td>
<td>--------</td>
<td>------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Oracle E-Business Suite Cloud Manager</td>
<td>VM</td>
<td>1</td>
<td>1</td>
<td>7 GB</td>
<td>Required: 55 GB (block)</td>
<td>1</td>
</tr>
<tr>
<td>A load balancer (You can use your own load balancer or Load Balancer as a Service [LBaaS])</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>1</td>
</tr>
<tr>
<td>Description</td>
<td>Machine Type</td>
<td>Number of Nodes</td>
<td>OCPUs Allocated</td>
<td>Memory</td>
<td>Storage</td>
<td>External IPs</td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------------</td>
<td>-----------------</td>
<td>-----------------</td>
<td>--------------</td>
<td>----------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Application tier</td>
<td>VM</td>
<td>n (where 'n' is the number of application tier nodes in the target environment)</td>
<td>n*m (where 'm' is the number of OCPUs in the shape selected for the application tier; the minimum for 'm' is 1)</td>
<td>Release 12.2 = 14 GB per VM Release 12.1 = 7 GB per VM</td>
<td>Strictly dependent on your on-premises environment. The minimum requirements are as follows:</td>
<td>n</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Shared application tier: 170 GB + 40 GB for each additional application tier (block) Non-shared application tier: 170 GB x n (block) Per language: 16 GB (block)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Database tier on Oracle Cloud Infrastructure Compute</th>
<th>VM</th>
<th>1</th>
<th>2</th>
<th>14 GB</th>
<th>Vision demo: 300 GB</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Database tier on 1-Node VM DB System (Single Instance)</th>
<th>VM</th>
<th>1</th>
<th>1</th>
<th>15 GB</th>
<th>Vision demo: 256 GB</th>
</tr>
</thead>
</table>

Total storage: 712 GB
<table>
<thead>
<tr>
<th>Description</th>
<th>Machine Type</th>
<th>Number of Nodes</th>
<th>OCPUs Allocated</th>
<th>Memory Allocation</th>
<th>Storage</th>
<th>External IPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database tier on 2-Node VM DB System</td>
<td>VM</td>
<td>2</td>
<td>2 per VM</td>
<td>30 GB per VM</td>
<td>Vision demo: 256 GB</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Total storage: 912 GB</td>
<td></td>
</tr>
<tr>
<td>Database tier on Exadata Cloud Service Oracle RAC</td>
<td>Bare Metal</td>
<td>2</td>
<td>11 x 2</td>
<td>720 GB x 2</td>
<td>84 TB</td>
<td>2</td>
</tr>
</tbody>
</table>

Footnotes for Table 5-4:

1. The Available Storage Size and Total Storage Size are different. For more information, see Bare Metal and Virtual Machine DB Systems [https://docs.cloud.oracle.com/en-us/iaas/Content/Database/Concepts/overview.htm#virtualmachine].

2. These are the minimum specifications provided by an Exadata Cloud Service Quarter Rack.

Prepare the Source Oracle E-Business Suite Environment

1. Copy the API signing key files to both the application tier primary node and the database tier for the source Oracle E-Business Suite environment. If you plan to run the Oracle E-Business Suite Cloud Backup Module on a separate server, copy the key files to that server as well. The key files must be placed in a directory with the same name and path on each server, in a location where they can be referenced by the Oracle E-Business Suite Cloud Backup Module. For example: /u01/install/APPS/.oci/

2. Create a stage area directory on the source application tier. This directory will hold temporary files used during the application tier backup process as well as the application tier backup file in zip or tar format that is created locally before it is uploaded to Oracle Cloud Infrastructure Object Storage. Ensure that the application tier has free space equal to 30% of the size of the application tier file system or greater. More space may be required in the following cases:
• The database tier and the application tier are on the same host.

• You specify a large number of threads for the upload in the Backup Thread Count parameter of the Oracle E-Business Suite Cloud Backup Module.

• You set the Backup Archive Type parameter of the Oracle E-Business Suite Cloud Backup Module to `tar`, which does not compress the backup files, instead of `tgz`.

The method you use to calculate the size of the application tier file system varies according to your release.

• For Oracle E-Business Suite Release 12.2, obtain the size of the run file system as shown in this example.
  
  ```
  $ cd /u02/ebs122
  $ . EBSapps.env run
  $ cd $RUN_BASE
  $ du -sh
  40G .
  ```

  In this example, the size of the run file system on the application tier is 40 GB. Therefore, the minimum space required for the stage area on the application tier is 30% of 40 GB, or 12 GB.

• For Oracle E-Business Suite Release 12.1.3, the size of the application tier file system is the sum of the size of the following directories: `$APPL_TOP`, `$COMMON_TOP`, `$ORACLE_HOME`, and `$IAS_ORACLE_HOME`. As an example, if that sum total is 30 GB, then the minimum space required for the stage area on the application tier is 30% of 30 GB, or 9 GB.

If you have not allocated enough free space, then the Oracle E-Business Suite Cloud Backup Module will exit with a message indicating how much is required.

3. Create a stage area directory on the source database tier. This directory will hold the backup utilities and the temporary files used to process the backup. Ensure that it has at least 20 GB of free space.

4. Verify the following to ensure that the Oracle E-Business Suite Cloud Backup Module can connect to all required nodes:
   • All nodes must have SSH enabled.
   • SSH equivalence must be set up between the backup module server and the primary application tier node, and between the backup module server and the database tier node, if you plan to run the Oracle E-Business Suite Cloud Backup Module on a separate server.
   • On the application tier server and the database tier server, the SSH configuration files (`~/.ssh/config`) must have the entry "ServerAliveInterval
Additionally, if you plan to run the Oracle E-Business Suite Cloud Backup Module on a separate server, then the same entry must be set in the SSH configuration file for that server.

- The Oracle Cloud Infrastructure Backup Service must be reachable either directly from the source database server and primary application tier server or through a proxy server.

## Deploy Oracle E-Business Suite Cloud Manager

If you have not already done so, deploy Oracle E-Business Suite Cloud Manager as described in Deploy Oracle E-Business Suite Cloud Manager on Oracle Cloud Infrastructure, page 2-1.

## Install the Oracle E-Business Suite Cloud Backup Module

This section describes how to install the Oracle E-Business Suite Cloud Backup Module on the Linux server that you have chosen to use as the backup module server, which can be located either on-premises or in OCI Compute. It can be one of the Oracle E-Business Suite nodes or another server that resides in your intranet. The backup module server must have at least 500 MB of free space and must have the wget libraries installed.

The Oracle E-Business Suite Cloud Backup Module requires Perl version 5.14 or later with the JSON module installed. You must either ensure that the default Perl installation on the backup module server meets these requirements, or run the Oracle E-Business Suite Cloud Backup Module using the Perl binary provided in the patch.


2. Using the following commands, change to the directory where you downloaded the patch file and extract the downloaded patch.

   $ cd <download_folder>
   $ unzip p32232832_R12_Generic.zip

   Unzipping the patch zip file creates a directory named RemoteClone.

3. Change to the RemoteClone directory and change the permission to "execute" for all the downloaded scripts.

   $ cd RemoteClone
   $ chmod +x *.pl
   $ chmod +x lib/*.sh
Create an Advanced Configuration Parameters File (Optional)

Before running the Oracle E-Business Suite Cloud Backup Module, you can optionally create a file to specify advanced configuration parameters to address special situations. If you do not need to specify these parameters, you can skip this section.

If you create an advanced configuration parameter file, then ensure that you specify the location of the file when you run the Oracle E-Business Suite Cloud Backup Module, as described in the next section.

1. Make a copy of the advanced-config-param.template file in the RemoteClone/EBS-METADATA/template directory. Place the new file in a directory location where it can be accessed by the Oracle E-Business Suite Cloud Backup Module.

2. Open your new advanced configuration parameter file in a text editor and specify values for the parameters you want to use, as described in the following steps.

3. In the RMAN_CHANNEL_COUNT parameter, specify the number of Recovery Manager (RMAN) staging channels to allocate for creating the backup. The default value used by RMAN is 75% of the number of CPUs. The minimum value is one channel. The maximum value is 255 channels.

4. In the RMAN_COMPRESSION_ALGORITHM parameter, specify the binary compression algorithm to use for RMAN backup. The values you can specify are BASIC, LOW, MEDIUM, and HIGH. The default value is BASIC. Note that the LOW, MEDIUM, and HIGH compression algorithms fall under Advanced Compression. You must have or acquire a license for the Advanced Compression option to use these compression algorithms. The Advanced Compression option is included in all Exadata cloud service subscriptions, and in VM DB Systems subscriptions with Enterprise Edition High Performance and Extreme Performance options.

5. In the RMAN_SECTION_SIZE parameter, specify the section size for multisection backups. The default value is 64G. Valid values are 2G, 4G, 8G, 16G, 32G, 64G, 128G, or 256G.

6. As part of RMAN backup, in the copy phase database blocks will be validated implicitly, and any corruption or missing object will be reported at that time. If you want to enforce the database validation before the RMAN backup, then set the RMAN_VALIDATE_DATABASE parameter to true. The default value is false.

7. The following parameters are set automatically to default values by RMAN unless you enter specific values for them here. You should only set values for these parameters if you fully understand their effects, as inappropriate settings can reduce backup performance.
   - In the RMAN_FILESPERSET parameter, specify the maximum number of data
files to place in each backup set. The default value is 64. To determine the number of data files in each backup set, RMAN uses either the value you specify in this parameter or the number of files read by each channel, whichever is lower. If you allocate only one channel, then you can use this parameter to make RMAN create multiple backup sets.

- In the RMAN_MAXOPENFILES parameter, specify the maximum number of input files that a backup or copy can have open at a given time. The default value used by RMAN is 8.

- In the RMAN_RATE parameter, specify the rate of bytes per second that RMAN can read on this channel. Use this parameter to set an upper limit for bytes to read so that RMAN does not consume excessive disk bandwidth and degrade online performance. Specify the rate as an integer followed by the abbreviation for the unit of measurement: <rate_as_integer>[K|M|G]

- It is not recommended to use the RMAN_DATAFILE_ID_ALLOWED_MAXCORRUPT parameter for normal processing. However, if necessary, you can set this parameter to specify the maximum number of corruptions permitted in a data file during the backup job. Specify the parameter value as a list showing each data file ID and the maximum number of corruptions for that data file, in the following format: <DATA_FILE_ID_1>:<MAX_CORRUPTIONS_1>, <DATA_FILE_ID_2>:<MAX_CORRUPTIONS_2>, ...

8. Use the following parameter only if you have already run the Oracle E-Business Suite Cloud Backup Module and it has returned any Oracle WebLogic Server validation warnings. The Oracle E-Business Suite Cloud Backup Module validates the Oracle WebLogic Server domain size and the number of Oracle WebLogic Server backup configuration files and exits with a warning if the default threshold values are exceeded. You should review these warnings as described in Review Oracle WebLogic Server Validation Warnings, page 5-26. If you have determined that you can safely ignore these warnings, then you can specify that you want to skip the Oracle WebLogic Server validation when you rerun the Oracle E-Business Suite Cloud Backup Module by setting the SKIP_WLS_DOMAIN_VALIDATION_THRESHOLD parameter to true. The default value is false.

9. If you need to skip any files or directories during database tier upload, then specify a list of the absolute file or directory paths in the EXCLUDE_FILE_OR_DIR_FOR_UPLOAD.DB parameter, separated by commas. For example, you might want to exclude custom log locations if you are certain that the directory does not need to be included in the backup.

10. If you need to skip any files or directories during application tier upload, then specify a list of the absolute file or directory paths in the
EXCLUDE_FILE_OR_DIR_FOR_UPLOAD.APPS parameter, separated by commas.

11. Save the updated advanced configuration parameter file.

Create a Backup with the Oracle E-Business Suite Cloud Backup Module

In this section, you will run the Oracle E-Business Suite Cloud Backup Module, EBSCloudBackup.pl, to create a backup of your source Oracle E-Business Suite environment on Oracle Cloud Infrastructure Backup Service.

Ensure that your instance and resources meet all the requirements and that you have performed all the required actions listed in Verify Prerequisites for Traditional Lift and Shift., page 5-3. The EBSCloudBackup.pl script validates key requirements before beginning the actual backup, including checking the available space, checking connections, verifying that archive logging is enabled, and verifying that mandatory patches have been applied. Check that these requirements are in place before you start running the script, so that the script can proceed with creating the backup after performing the validations.

Additionally, if Transparent Data Encryption (TDE) is enabled for the source environment, then you should verify that all the pluggable databases (PDBs) are in an open state with an appropriate wallet type (autologin or password).

To ensure a successful backup, avoid activities that could interfere with the backup process while EBSCloudBackup.pl is running.

• Do not apply patches. Note that this restriction applies not only to Oracle E-Business Suite patches, but to application technology stack and database patches as well. If you are running Oracle E-Business Suite Release 12.2, you must complete any active patching cycle before you begin the backup process.

• Do not remove or move archive logs.

• Do not shut down application tier or database tier services.

• Do not perform configuration updates.

Note that if the EBSCloudBackup.pl script fails, you can rerun the script and it will restart and continue from the point of failure. However, if you interrupt the script’s processing with Ctrl-C, the restart capability may not function as expected.

1. Before you start running EBSCloudBackup.pl, inform users that a backup is being taken, and request that they do not perform any destructive operation on the file system, such as removing directories, until the backup is complete.

2. Temporarily stop any application tier or database backup cron jobs that are scheduled.
3. If you have not already done so, change to the RemoteClone directory on the backup module server.

4. Run the EBSCloudBackup.pl script using the following command.

   
   $ perl EBSCloudBackup.pl
   
   As an alternative, if the backup module server does not already have the required Perl version with the JSON module installed, you can run the script using the Perl binary provided in the Oracle E-Business Suite Cloud Backup Module patch files, with the following command.

   
   $ /opt/perl/bin/perl EBSCloudBackup.pl
   
   If you are using an Oracle E-Business Suite application tier node or database tier node as the backup module server, note that you should not source the Oracle E-Business Suite environment before running the Oracle E-Business Suite Cloud Backup Module.

5. On the first screen, choose option 1, Create E-Business Suite Backup and Upload to Oracle Cloud Infrastructure.

   
   Migrate Oracle E-Business Suite - Options
   
   Migrate Oracle E-Business Suite - Enter Selection:
   
   1: Create E-Business Suite Backup and Upload to Oracle Cloud Infrastructure
   
   2: Exit
   
   Enter your choice from above list: 1

6. Next, indicate whether communication between the source database server and Oracle Cloud Infrastructure Object Storage takes place through a proxy and you need to specify the proxy details.

   
   Enter Source Database Tier - Proxy Details
   
   [Ctrl-B: Back, Ctrl-H: Main Menu]

   1: Yes
   2: No
   
   Enter your choice from above list: 1
   
   If you enter option 1, then in the following screen, specify the proxy details used to establish communication between the source database server and Oracle Cloud Infrastructure Object Storage.
Enter Source Database Tier - Proxy Details

[Ctrl-B: Back, Ctrl-H: Main Menu]

Proxy Protocol : https
Proxy Host : www-proxy.example.com
Proxy Port : 443
Proxy User Name :
Proxy User Password :

7. Enter the details for the database tier of the source Oracle E-Business Suite environment.

- When entering the host name for the source database server, ensure that you enter the fully qualified domain name.

- You must specify an operating system user name with which to connect to the source database server using SSH. You can choose to authenticate the OS user with either a password, a custom private SSH key and passphrase, or the default SSH key ($HOME/.ssh/id_rsa) on the backup module server. The prompts for the custom private key and passphrase appear only if you do not enter an OS user password. If you do not enter either a password or a custom private key, then the script indicates that the default SSH key will be used and prompts you to confirm that you want to continue with the SSH key at the indicated location.

- Enter the location of the context file on the database tier, including the complete file path.

- Optionally enter the operating system time zone for the source database server. This time zone value is used to help determine the default time zone for environments provisioned from this backup if the Server Timezone profile option is not set within the source environment. For more information, see Advanced Provisioning, page 9-8.

Specify the operating system time zone in the named region format as follows: <time_region>/<time_zone_city>

For example: America/Los_Angeles

For instructions on checking the time zone set for the source database server, refer to the documentation for your on-premises Linux installation. For example, on Oracle Linux, use the timedatectl command as described in Check the current configuration [https://docs.oracle.com/en/operating-systems/oracle-linux/8/obe-datetime-cli/index.html#Check-the-current-configuratio] in the Oracle Linux documentation.

- Specify whether Transparent Data Encryption (TDE) is enabled for the source database. If TDE is enabled, then you must also enter the password for the TDE wallet.
Finally, specify the location of the stage area directory you prepared to hold the temporary files that will be created on the database tier during the backup creation process.

---

Migrate Oracle E-Business Suite - Enter Source Database Tier Details

---

Enter Fully Qualified Hostname                      : demo.example.com
OS User Name                                        : oracle
OS User Password [skip if not applicable]           :
OS User Custom Private Key [skip if not applicable] :
OS User Passphrase [skip if not applicable]         :

Context File                                        :
/article12.1.0/appsutils/DBDBXML_apps.xml
OS Time Zone                                        : America/Los_Angeles
Database Transparent Data Encrypted ( TDE ) : ( Yes | No ) yes
Wallet Password                                     :

You have not entered Password or Custom Private Key location
We will be using default SSH key at /home/oracle/.ssh/id_rsa
Do you want to continue (Yes | No)                  :

Validating the details...
Stage Directory                                     :
/article/install/stage/dbStage

8. Next, indicate whether communication between the source application tier and Oracle Cloud Infrastructure Object Storage takes place through a proxy and you need to specify the proxy details.

---

Enter Source Application Tier Proxy Details

---

[Ctrl-B: Back, Ctrl-H: Main Menu]

1: Yes
2: No
Enter your choice from above list: 1

If you enter option 1, then in the following screen, specify the proxy details used to establish communication between the source application tier and Oracle Cloud Infrastructure Object Storage.
Enter the details for the application tier of the source Oracle E-Business Suite environment.

- When entering the host name for the source application tier server, ensure that you enter the fully qualified domain name.

- You must specify an operating system user name with which to connect to the source application tier server using SSH. You can choose to authenticate the OS user with either a password, a custom private SSH key and passphrase, or the default SSH key ($HOME/.ssh/id_rsa) on the backup module server. The prompts for the custom private key and passphrase appear only if you do not enter an OS user password. If you do not enter either a password or a custom private key, then the script indicates that the default SSH key will be used and prompts you to confirm that you want to continue with the SSH key at the indicated location.

- Additionally, specify the location of the context file on the application tier, including the complete file path, the password for the Oracle E-Business Suite APPS schema, and the location of the stage area directory you created to hold the temporary files created on the application tier during the backup creation process.

- For Oracle E-Business Suite Release 12.2 only, you must also specify the Oracle WebLogic Server administrator password for the source environment.
Enter Fully Qualified Hostname  
: demo.example.com

OS User Name  
: oracle

OS User Password [skip if not applicable]  
:

OS User Custom Private Key [skip if not applicable]  
:

OS User Passphrase [skip if not applicable]  
:

Context File  
: /u01/install/APPS/fs1/inst/apps/EBSDB_apps/appl/admin/EBSDB_apps.xml

APPS Password  
: password

You have not entered Password or Custom Private Key location

We will be using default SSH key at /home/oracle/.ssh/id_rsa

Do you want to continue (Yes | No)  
: yes

Validating the details...

Stage Directory  
: /u01/install/stage/appsStage

WebLogic Server Admin Password  
: password

10. Enter details to specify how you want to create the backup on Oracle Cloud Infrastructure Object Storage.

- Backup Identifier Tag - Enter a name to uniquely identify your backup. The script adds this tag as a prefix when creating the containers to store objects in a compartment within an Oracle Cloud Infrastructure Object Storage namespace, known as buckets. The generic bucket for the application tier and database tier Oracle home backup is named $<Backup_IDENTIFIER_TAG>Generic$. The database bucket for the database RMAN backup is named $<Backup_IDENTIFIER_TAG>DB$.

- Backup Thread Count - Specify the number of threads used to upload the application tier and database tier file system backups. The default value is 1. If your CPU count is less than 8, then the maximum value for the backup thread count is 2 times the CPU count. If your CPU count is 8 or more, then the maximum value for the backup thread count is 1.5 times the CPU count.
• Backup Archive Type - Specify **tgz** to compress the backups before the upload, or **tar** if you do not want to compress the backups. We recommend that you specify **tgz**.

• RMAN Advanced Configuration Parameter File Path - If you created an advanced configuration parameter file in Create an Advanced Configuration Parameters File, page 5-13, then specify the directory path and file name for the file in this parameter. Otherwise, leave this parameter blank.

• Backup Encryption Password - Specify a password to encrypt the application tier file system and database tier file system. If Transparent Data Encryption (TDE) is not enabled in the source database, then this password is also used to encrypt the database RMAN backup.

• Confirm Backup Encryption Password - Re-enter the same backup encryption password to confirm it.

---

**Enter OSS - Backup Details**

---

[Ctrl-B: Back, Ctrl-H: Main Menu]

Backup Identifier Tag : EBS122EXAMPLE
Backup Thread Count : 4
Backup Archive Type ( tar | tgz ) : tgz
RMAN Advanced Configuration Parameter File Path : /u01/install/APPS/RC06/RemoteClone/EBS-METADATA/template/advanced-config-param.txt
Backup Encryption Password : password
Confirm Backup Encryption Password : password

11. Next, indicate whether you access the cloud service through a proxy and need to specify the proxy details.

---

**Enter Oracle Cloud Infrastructure Proxy Details**

---

[Ctrl-B: Back, Ctrl-H: Main Menu]

1: Yes
2: No

Enter your choice from above list: 1

If you enter option 1, then in the following screen, specify the proxy details used to establish communication between the backup module server and the cloud service.
12. Enter your Oracle Cloud Infrastructure details.

- The user who performs the backup must be a member of the Oracle E-Business Suite administrators group defined according to Create and Map Groups in Oracle Cloud Infrastructure Identity and Access Management and Oracle Identity Cloud Service, page 2-7 or Create the Oracle E-Business Suite Administrators Group and Assign Policies, page 3-4. For this user, enter your user OCID, the fingerprint for your Oracle Cloud Infrastructure API signing key, the location for your PEM key file on the database tier, and the location for your PEM key file on the application tier.

- Enter the OCID for your tenancy, the region identifier of the region where you plan to provision an environment from this backup, your tenancy name, and the OCID of the compartment where the backup buckets should be created.

- For environments with Oracle Database Release 12.1.0.2 or Release 19c, you must also specify the Cloud database service on which you plan to provision the target environment based on this backup.
  - For a Compute VM, enter **Compute**.
  - For 1-Node VM DB System (Single Instance) or 2-Node VM DB System (Oracle RAC), enter **VM DB System**.
  - For Exadata Cloud Service, enter **Exadata DB System**.
Create a Backup of an On-Premises Oracle E-Business Suite Instance on Oracle Cloud Infrastructure

Migrate Oracle E-Business Suite - Enter Oracle Cloud Infrastructure Details

---

[Ctrl-B: Back, Ctrl-H: Main Menu]

Oracle Cloud User OCID : ocid1.user.oc1..xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Oracle Cloud User Private Key Path on Database Tier : /u01/install/APPS/.oci/oci_api_key.pem
Oracle Cloud User Private Key Path on APPS Tier : /u01/install/APPS/.oci/oci_api_key.pem
Oracle Cloud Tenancy OCID : ocid1.tenancy.oc1..xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Oracle Cloud Region : xx-xxxxxx-1
Oracle Cloud Tenant Name : example
Oracle Cloud Compartment OCID : ocid1.compartment.oc1..xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Target Database Type - (Compute | VM DB System | Exadata DB System): VM DB System

13. Review the values specified for the backup creation. The mode is set automatically based on your database release and target database type.

   • BMCS - Environments with Oracle Database Release 11.2.0.4, or environments with Oracle Database Release 12.1.0.2 or 19c where the target database service is Compute

   • BMCS_CDB - Environments with Oracle Database Release 12.1.0.2 or 19c where the target database service is Virtual Machine DB System or Exadata Cloud Service

The custom private key locations for the source database tier and source application tier are shown only if you chose to authenticate the OS user on those tiers with a custom private SSH key.

If you are satisfied with the values shown, enter option 1 to proceed.
Migrate Oracle E-Business Suite - Review

Mode                           : BMCS_CDB

Source Database Details:
Host Name                      : demo.example.com
OS User Name                   : oracle
Custom Private Key Location    : /home/oracle/.ssh/id_rsa
Stage Directory                : /u01/install/stage/dbStage
Context File                   : /u01/install/APPS/12.1.0
/appsutil/EBSDB_apps.xml
OS Time Zone                   : America/Los_Angeles

Source Application Tier Details:
Hostname                        : demo.example.com
OS User Name                    : oracle
Custom Private Key Location     : /home/oracle/.ssh/id_rsa
Stage Directory                 : /u01/install/stage/appsStage
Context File                    : /u01/install/APPS/fs1/inst/apps/EBSDB_apps/appl/admin/EBSDB_apps.xml

OSS - Backup Details:
Backup Identifier Tag                           : EBS122EXAMPLE
Backup Thread Count                             : 4
Backup Archive Type                             : tgz
RMAN Advanced Configuration Parameter File Path : /u01/install/APPS/RC06/RemoteClone/EBS-METADATA/template/advanced-config-param.txt

Oracle Cloud Infrastructure Details:
Oracle Cloud User OCID                        : ocid1.user.oc1..
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Oracle Cloud Tenancy OCID : ocid1.tenancy.oc1..
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Oracle Cloud Region : xx-xxxxxx-1
Oracle Cloud Tenant Name : example
Oracle Cloud Compartment OCID : ocid1.compartment.
oc1..xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Target Database Type : VM DB System

==================================================================
Proceed With Selected Action
==================================================================

[Ctrl-B: Back, Ctrl-H: Main Menu]
1: Yes
Enter your choice from above list: 1

The script performs the following tasks:

- Validates OS level authentications.
- Validates whether the Oracle Database version is certified.
- Validates whether the database is archivelog enabled.
- Validates whether mandatory patches are present.
- Creates a database backup.

- Performs remote calls to the application tier to create a tar package containing the application files. For Oracle E-Business Suite Release 12.2, the tar package includes the contents of the EBSapps directory on the run file system, including the APPL_TOP directory, the COMMON_TOP directory, the OracleAS 10.1.2 directory, and a packaged version of the Oracle Fusion Middleware home. For Oracle E-Business Suite Release 12.1.3, the tar package includes the contents of the APPL_TOP, COMMON_TOP, OracleAS 10.1.2, and OracleAS 10.1.3 directories.
- Transfers the application tier tar package and database backup to a new bucket in your Oracle Cloud Infrastructure Backup Service account associated with your Oracle Cloud Infrastructure tenancy.

If the script indicates that a validation failed, you can press Ctrl-B to return to previous screens and provide a corrected value. You can review the log files in the RemoteClone/logs directory to help identify which value failed validation. It is recommended that you do not exit the script; instead, use another UNIX window to view the log file, so that you can return to the previous screens of the script and correct the failed value without needing to re-enter all the values you previously entered.

14. After the script finishes and the backup is complete, you should notify users that they can resume normal file system activities. You should also restart any application tier or database backup cron jobs that you stopped before you began running the script, and resume patching and maintenance activities as needed.


16. You can also use Oracle E-Business Suite Cloud Manager to delete a backup that you no longer need, or use a command-line API to delete a failed backup. See
Troubleshoot Backup Issues

Review Oracle WebLogic Server Validation Warnings:
The Oracle E-Business Suite Cloud Backup Module performs certain validations on the Oracle WebLogic Server domain and exits with a warning if the default threshold values are exceeded. If the script returns one of these warning messages, then you should review the source environment to decide whether you will make changes to resolve the issue or whether you can safely ignore the warning and skip the validation to proceed with the backup.

- WLS domain size is higher than EBS default threshold: 5120 MB - Check what factors are causing the Oracle WebLogic Server domain size to be greater than 5120 MB (5 GB). If the domain size is due to large log files or temporary files, then you should first clean up those files to reduce the domain size, and then rerun the Oracle E-Business Suite Cloud Backup Module. However, if you determine that the contents of the Oracle WebLogic Server domain are valid, such as if the domain includes a large number of managed servers that add to the overall domain size, then you can choose to skip this validation.

- ERROR : Backup config.xml file count is higher than EBS default threshold : 500. Please cleanup some of the backup config.xml file available in <EBS_DOMAIN_HOME>/config directory. - Check the <EBS_DOMAIN_HOME>/config directory to determine whether you can delete any older Oracle WebLogic Server backup configuration files (backup_config*.xml) before rerunning the Oracle E-Business Suite Cloud Backup Module. If you want to retain all the backup configuration files, then you can choose to skip this validation.

If you determine that you can safely ignore any Oracle WebLogic Server warning messages, then you can skip these validations by setting the SKIP_WLS_DOMAIN_VALIDATION_THRESHOLD parameter according to the following steps.

1. Follow the instructions in Create an Advanced Configuration Parameters File, page 5-13 to create an advanced configuration parameter file and set the SKIP_WLS_DOMAIN_VALIDATION_THRESHOLD parameter to true.

2. If you choose to skip the Oracle WebLogic Server validations, ensure that you tune the JVM heap memory size accordingly using the CONFIG_JVM_ARGS environment variable. Otherwise, the preclone process for the Oracle WebLogic Server domain may run successfully, but the apply clone may later fail with an error due to the heap space being exceeded.

3. Finally, rerun the Oracle E-Business Suite Cloud Backup Module following the
Create a Backup of an On-Premises Oracle E-Business Suite Instance on Oracle Cloud Infrastructure

instructions in Create a Backup with the Oracle E-Business Suite Cloud Backup Module, page 5-15, and specify the location of your advanced configuration parameter file at the RMAN Advanced Configuration Parameter File Path prompt.

Troubleshoot Known Issue for Custom Log Locations:

This workaround resolves a known issue that can occur if a utility writes to a directory such as a log file within the Oracle home on the database tier of your Oracle E-Business Suite instance during the backup process. This issue can occur because the database is online while the backup is being created, so log entries might be generated while the backup is in progress. The Oracle E-Business Suite Cloud Backup Module skips standard log locations, but if you have configured any custom log locations and the logs are updated while the script is running, you may encounter errors such as the following:

Error:
tar: custom_logs/sqlnet_server_1586.trc: file changed as we read it
tar: custom_logs: file changed as we read it

If you identify custom log locations to exclude from the backup before you begin running the Oracle E-Business Suite Cloud Backup Module, you can create an advanced configuration parameter file specifying the directories or files to exclude. See Create an Advanced Configuration Parameters File, page 5-13.

If you encounter such errors while running the Oracle E-Business Suite Cloud Backup Module, then as a workaround, if you are certain that the directories do not need to be included in the backup, perform the following steps to specify the directories that should be skipped and then restart the backup process.

1. Review the database tier upload log file `<STAGE_DIRECTORY>/session/<SESSION_ID>/logs/<TIMESTAMP>/dbTierUpload.log` on the database node to determine the directory for which the backup failed.

2. Locate the following file in the stage area directory on the database node:
   `<STAGE_DIRECTORY>/session/<SESSION_ID>/db_manifest.json`
   Make a backup copy of this file, and then open the `db_manifest.json` file in a text editor.

3. Search for the directory for which the backup failed.

4. Specify that this directory should be skipped during the backup process by adding the directory under the "excludes" array. For example, if you have a directory named `custom_logs` within the Oracle home directory, look for the lines similar to the following in the `db_manifest.json` file:
<db_manifest.json>
{
    "sourcePath": "/scratch/oracle/12.1.0",
    "binName": "s_db_ohBin1",
    "contents": [
        "custom_logs"
    ],
    "excludes": [],
    "sizeInBytes": 15838395906,
    "objectNameInBucket": "db/s_db_oh/s_db_ohBin1.tar.enc",
    "targetPath": "s_db_oh"
}

Change these lines by adding the directory to be skipped under the "excludes" array. Note that the directory paths in the "excludes" array are relative to your Oracle home directory. Then save your changes to the db_manifest.json file. Ensure that the modified file does not contain any syntax errors. For example:

{
    "sourcePath": "/scratch/oracle/12.1.0",
    "binName": "s_db_ohBin1",
    "contents": [
        "custom_logs"
    ],
    "excludes": [
        "custom_logs"
    ],
    "sizeInBytes": 15838395906,
    "objectNameInBucket": "db/s_db_oh/s_db_ohBin1.tar.enc",
    "targetPath": "s_db_oh"
}

5. Restart the Oracle E-Business Suite Cloud Backup Module. It will continue from the point where it previously failed.
Create a Standby Environment on Oracle Cloud Infrastructure from an On-Premises Oracle E-Business Suite Release 12.2 Instance with Oracle Database Release 12.1.0.2

Overview

This chapter describes how you can use Oracle E-Business Suite automation (and in particular, the on-premises Oracle Applications Manager combined with the Oracle E-Business Suite Cloud Manager) to create a standby environment in Oracle Cloud Infrastructure.

Promotion of the standby environment accomplishes a "lift and shift". We refer to this as a "reduced downtime lift and shift", due to the reduction of overall downtime that is required with the more traditional lift and shift method described in Create a Backup of an On-Premises Oracle E-Business Suite Instance on Oracle Cloud Infrastructure, page 5-1.

The standby creation and reduced downtime lift and shift features are available for Oracle E-Business Suite Release 12.2 with Database Release 12.1.0.2, with the target of Compute.

Requirements for Creating a Standby Environment

The following are requirements for creating a standby environment.

Oracle E-Business Suite Cloud Manager in Your Tenancy

You must have Oracle E-Business Suite Cloud Manager in your tenancy.
Cloud Services Minimum Resource Recommendations

To create a standby environment, we recommend that you have cloud service resources that match or exceed those specified in the following table.

<table>
<thead>
<tr>
<th>Description</th>
<th>Machine Type</th>
<th>Number of Nodes</th>
<th>OCPUs Allocated</th>
<th>Memory</th>
<th>Storage</th>
<th>External IPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Cloud Infrastructure Backup Service</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Size of the database Oracle home in the source environment (object)</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Oracle E-Business Suite Cloud Manager</td>
<td>VM</td>
<td>1</td>
<td>1</td>
<td>7 GB</td>
<td>Required: 55 GB (block)</td>
<td>1</td>
</tr>
<tr>
<td>Application tier</td>
<td>VM</td>
<td>1</td>
<td>1</td>
<td>14 GB per VM</td>
<td>Strictly dependent on your on-premises environment. The minimum requirements are as follows: 170 GB</td>
<td>1</td>
</tr>
<tr>
<td>Database tier on Oracle Cloud Infrastructure Compute</td>
<td>VM</td>
<td>1</td>
<td>2</td>
<td>14 GB</td>
<td>Vision demo: 300 GB</td>
<td>1</td>
</tr>
</tbody>
</table>
Preparations for Creating a Standby Environment

Follow the steps below to prepare to create a standby environment.

**Set Up Certificates for Oracle E-Business Suite Cloud Manager:**

Oracle E-Business application tier nodes will invoke web services exposed by the Oracle E-Business Suite Cloud Manager. In order for Oracle E-Business Suite application tier nodes to invoke these REST services, they need to establish secure communication using TLS. The application tier nodes use a Java framework to invoke REST APIs, and the Java toolkit establishes the secure handshake after validating the certificate coming from the Cloud Manager. This validation requires that the Java toolkit recognizes the certificate authority (CA) that issued the Cloud Manager certificate.

The certificate status of the Oracle E-Business Cloud Manager load balancer will fall into one of these two categories:

- A valid certificate issued by a CA with a properly DNS-registered, resolvable name.
- A self-signed certificate generated during Cloud Manager configuration and associated with the IP address of the load balancer.

**Steps for a Certificate Issued by a Certification Authority (Conditionally Required)**

If you have a valid certificate issued by a Certificate Authority (CA) with a properly DNS-registered, resolvable name, then perform the following:

1. Obtain the certificate from your certificate authority.
2. Import the certificate to your source application tier nodes:
   - Copy the `cacerts` file to each application tier node in your source system.
   - Add the certificate to the keystore following the example commands below, one for each file system:
     ```
     $ keytool -import -trustcacerts -keystore /u01/install/APPS/fs1/EBSapps/comn/util/jdk64/jre/lib/security/cacerts -file democert.crt -alias sample2021webentry
     $ keytool -import -trustcacerts -keystore /u01/install/APPS/fs2/EBSapps/comn/util/jdk64/jre/lib/security/cacerts -file democert.crt -alias sample2021webentry
     ```
3. Stop and start the Oracle E-Business Suite instance.

**Steps For a Self-Signed Certificate Using the Cloud Manager Administration Utility (Conditionally Required)**

Use the Cloud Manager Administration Utility (`ebscmadmin`) if you are using a self-signed certificate generated during Cloud Manager configuration and you want to use...
the FQDN as the web entry point. Do not use the ebscmdadmin utility if you are using the IP address as the web entry point.

To learn more about running the ebscmdadmin utility to update the FQDN, see: Update the Oracle E-Business Suite Cloud Manager Load Balancer Fully Qualified Domain Name, page 4-18.

1. Run the ebscmdadmin command from the Oracle E-Business Suite Cloud Manager VM to update Oracle E-Business Suite Cloud Manager Load Balancer with a new FQDN. This command also regenerates the load balancer self-signed certificate for the load balancer listener resource in OCI with the same Common Name (CN) as in the user-provided load balancer FQDN.

For example, enter the following:

```bash
$ sudo su - oracle
$ cd /u01/install/APPS/apps-unlimited-ebs/bin
$ ./ebscmdadmin update-load-balancer-fqdn <argument>
```

2. Import the certificate to your source application tier nodes:
   1. Copy the cacerts file to each application tier node in your source system.
   2. Add the certificate to the keystore following the example commands below, one for each file system:

```
$ keytool -import -trustcacerts -keystore /u01/install/APPS/fs1/EBSapps/comn/util/jdk64/jre/lib/security/cacerts -file democert.crt -alias sample2021webentry
$ keytool -import -trustcacerts -keystore /u01/install/APPS/fs2/EBSapps/comn/util/jdk64/jre/lib/security/cacerts -file democert.crt -alias sample2021webentry
```

3. Stop and start the Oracle E-Business Suite instance.

**Manual Steps For a Self-Signed Certificate (Conditionally Required)**

Perform these steps if you are using a self-signed certificate generated during Cloud Manager configuration and associated with the IP address of the load balancer.

1. Replace the self-signed certificate generated by the Cloud Manager with a new self-signed certificate generated using a common name (CN).

In this case, you are using the IP address of the load balancer as your web entry point, as in the following example:

```bash
$ openssl req -x509 -newkey rsa:4096 -sha256 -days 356 -nodes -keyout democert.key -out democert.crt -subj '/CN=192.0.2.254' -extensions san -config <(echo '[req]'; echo 'distinguished_name=req'; echo '[san]'; echo 'subjectAltName=IP:192.0.2.254')
```

2. Add the newly-created certificate where needed:
   1. Add the certificate to the target OCI; for example, sample2021-ebscm-
2. Paste the SSL Certificate, specify the private key and paste PEM contents.

3. Add democert.crt to the SSL certificate section and democert.key to the private key section.

3. Update the listener. For example, update the listener in sample2021-ebscm-instance-prov-vm-lbaas to select the newly-created certificate.

4. Import the certificate to your source application tier nodes:

1. Copy the cacerts file to each application tier node in your source system.

2. Add the certificate to the keystore following the example commands below, one for each file system:

   $ keytool -import -trustcacerts -keystore /u01/install/APPS/fs1/EBSapps/comn/util/jdk64/jre/lib/security/cacerts -file democert.crt -alias sample2021webentry

   $ keytool -import -trustcacerts -keystore /u01/install/APPS/fs2/EBSapps/comn/util/jdk64/jre/lib/security/cacerts -file democert.crt -alias sample2021webentry

5. Stop and start the Oracle E-Business Suite instance.

**Set Up Networking:**

The network access described below is required at the seclist level. For the source database, the same needs to be opened at the iptables level as well. The target iptables would be updated automatically.

1. From the Target application tier, access the Source application tier: SSH connectivity (port 22)

2. From the Target database tier, access the Source database tier: TNS connectivity (port 1521)

3. From the Source database tier, access the Target database tier: TNS connectivity (port 1521)

4. From the Source application tier, access the Oracle E-Business Suite Cloud Manager URL.

If the source and target belong to the same network (same virtual cloud network), then communication between the source and the target occurs using private IPs; otherwise, communication uses public IPs. The reservation IPs for the target must be secured accordingly.
Reserved Public IP
For information on managing Public IP addresses, see: Public IP Addresses [https://docs.cloud.oracle.com/en-us/iaas/Content/Network/Topics/managingpublicIPs.htm].

1. Create public IP reservations for the application tier and database tier using the OCI console. Use the same compartment as the Oracle E-Business Suite compartment of the network profile.

2. Provide the created IPs in Standby Configuration page in Oracle Applications Manager for the target application and database tier IPs.

Reserved Private IP
Creating a reservation is unnecessary in this scenario.

3. Ensure the IPs entered for the target application and database tiers are within the application tier and database tier subset CIDR respectively, and that these IPs are not already assigned to instances.

Set Up the Source Application Tier:
1. Ensure that you have set up the certificate as described in Set Up Certificates for Oracle E-Business Suite Cloud Manager, page 6-3.


3. Run adpreclone.pl on the source application tier.

Set Up the Source Database Tier:
1. Ensure that the database is in Archive log mode.

2. Create wallet files if the database does not have wallet files already.
   Ensure that the sqlnet.ora file at context directory is updated with the correct wallet location.

3. Run adpreclone on the database Oracle home.
   1. On the application tier, source the environment file and run:
      
      $ $AD_TOP/bin/admkappsutil.pl
      
      This script will create the appsutil.zip file.

   2. Copy this zip file to the /tmp directory on the database tier.

   3. On the database tier, remove the $ORACLE_HOME/appsutil/clone directory.
4. Change to the Oracle directory:
   
   \$ cd $ORACLE_HOME

5. Unzip the file:
   
   \$ unzip -o /tmp/appsutil.zip

6. Run the script
   
   \$ $ORACLE_HOME/perl/bin/perl $ORACLE_HOME/appsutil/scripts/<CONTEXT_NAME>/adpreclone.pl dbTier

---

**Install the Oracle E-Business Suite Cloud Backup Module**

**Install the Oracle E-Business Suite Cloud Backup Module:**


---

**Create a Standby Environment for Oracle Cloud Infrastructure from an On-Premises Environment**

**Important:** Before configuring a standby environment, ensure that the ingress rule from the Oracle E-Business Suite Cloud Manager UI has been updated to give access to the Oracle E-Business Suite IP address. Otherwise, validation will not occur.

Ensure that the proxy is not set in the context file. If the proxy is set, remove the proxy settings in context file, run AutoConfig, and stop and start the application tier services.

Ensure that the Resource Owner option is selected under Allowed Grant Types in the registration of Oracle E-Business Suite Cloud Manager as an application in Oracle Identity Cloud Service (IDCS). This configuration is required to allow REST calls from Oracle E-Business Suite. See Register Oracle E-Business Suite Cloud Manager as a Confidential Application, page 2-36.

Perform these steps to configure a standby environment in Oracle Applications Manager.

**Access the Standby Environment Pages in Oracle Applications Manager:**

1. Log in to Oracle E-Business Suite on-premises environment as a user with access to
Oracle Applications Manager. For example, log on as a user with the out-of-box System Administration responsibility.

2. Select the Oracle Applications Manager responsibility in the Navigator in the home page, then select **Cloud Standby**.

3. The Oracle Cloud Infrastructure page shows details for the OCI account: Tenancy, Account, and EBS Cloud Manager name. Any configurations for existing standby environments are also shown.

**Edit the Oracle Cloud Infrastructure Account:**
You can edit some of the settings for Oracle E-Business Suite Cloud Manager here.

1. Click on **Edit Oracle Cloud Infrastructure Account** to edit the account details.

2. Enter a new Oracle Cloud Username.

3. Enter the Oracle Cloud Password.

4. Choose to define a new Cloud Manager Definition, or use an existing one.
   If you choose a new definition, enter the following:
   - EBS Cloud Manager Name
   - EBS Cloud Manager URL: Select the IP address that you use to connect to the Cloud Manager.
     For example, `https://192.0.2.254`
   If you choose to use an existing definition, select it in the Cloud Manager field.

5. Click **Validate** to validate your settings.

6. The Oracle Cloud Infrastructure Tenancy Details are shown but cannot be edited:
   - Tenancy Name
   - Tenancy OCID
   - Username
   - User OCID

7. Click **Save**.
Enter Standby Environment Information and Introspect the Application Tier:

1. On the main Oracle Cloud Infrastructure page, click **Configure Standby Environment** in the Standby Environments region.

2. Enter a Standby Environment Name.

3. Select a Network Profile.

4. The Region and Compartment are displayed.

5. Optionally select your operating system time zone. This is the operating system time zone for your application and database tier nodes.

   Oracle E-Business Suite Cloud Manager will validate your selection for the server time zone, unless you check the box **Bypass Server Timezone Profile Validation**.

   **Warning:** If you choose to override the time zone defined in the source environment, then the operating system for the new standby environment across all Compute instances and cloud services will be configured to use the selected time zone. After you provision your environment, and prior to starting any database and application tier services, you must set the `TZ` environment variable to match the Server Timezone profile option. Failure to do so could lead to data corruption. See: Time Zone Support [https://docs.oracle.com/cd/E26401_01/doc.122/e22953/T174296T575363.htm] in the Oracle E-Business Suite Setup Guide.

   For more information on time zone support, see: Time Zone Support in Oracle E-Business Suite Cloud Manager, page B-1.

6. Specify a Source IP address.

   This IP address is used to establish communication from the application tier node running in OCI. Ensure that the IP address you enter meets this purpose.

7. Click **Introspect Apps Tier** to submit a concurrent request to introspect the application tier.

8. The new standby environment configuration appears in the Standby Environments list.

Review Your Standby Environment Configuration In Progress in Oracle Applications Manager:

1. Click the name of your new standby environment the Standby Environments list in
Oracle Applications Manager.

2. The details of your standby environment configuration are shown, including the following:
   - Standby Environment Name
   - Network Profile
   - Region
   - Compartment Status
   - Standby Status

3. The Configuration Stages are also shown in a table. A concurrent request is submitted for each stage. Click on the Request ID link to view the log file of the concurrent request.

4. Information on the Application Tier is also shown, including:
   - Oracle E-Business Suite Version
   - Application Top directory
   - OS User
   Information for the local node and the standby node are given in a table.

5. Perform Database Tier Introspection as described below.

**Perform Database Tier Introspection:**

1. If not done already, install the Oracle E-Business Suite Cloud Backup Module on the database tier node. See: Install the Oracle E-Business Suite Cloud Backup Module, page 5-12.

2. Run the `db-introspect.sh` script:

   ```bash
   $ RemoteClone/bin/db-introspect.sh --action introspect --context-file <context file, for example: /u01/install/APPS/12.1.0/appsutil/demosid_demo1221ocompm1db.xml> --standby-name <standby environment name given in the Introspect Application Tier page> --standby-reserved-ip <standby reserved IP previously created in OCI> --standby-reserved-ip-type <Public or Private> --active-db-ip <active database IP reachable from target network> --oci-private-key-file <absolute path to key file> --ebs-username <for example: SYSADMIN> --listener-port <for example, 1521>
   
   Note that for the parameter --oci-private-key-file <absolute path to key file>, this value should be the API signing key of the user that was used to
set the Oracle Cloud Infrastructure credentials. See: Edit Oracle Cloud Infrastructure Account, page 6-8.

**Enter Configuration Information for the Standby Application and Database Tiers:**
In the Standby Environment Configuration on Oracle Cloud Infrastructure page, add the following information:

1. Enter the reserved public or private IP for the application tier.
2. Enter the shape for the standby application and database tiers.
3. Click **Submit**.

**Review Standby Environment Configuration in Oracle Applications Manager:**
If the configuration has failed, click **Retry** in its configuration review page to try configuring the standby environment again.

If the configuration has completed with a Successful or Failed status, you can click **Remove Standby** to remove the standby configuration.

**What’s Next**
You can review your standby environment in Oracle E-Business Cloud Manager. See: Review Standby Environment Details, page 10-12.

From Oracle E-Business Cloud Manager, you can also:

- Promote a Standby Environment, page 11-21
- Delete a Standby Environment, page 11-27
Part 4

Manage Oracle E-Business Suite Instances Using Oracle E-Business Suite Cloud Manager
Access Oracle E-Business Suite Cloud Manager

This chapter covers the following topics:

• Overview of Accessing Oracle E-Business Suite Cloud Manager
• Log In to Oracle E-Business Suite Cloud Manager
• Specify Your User Details (Conditionally Required)
• Check Oracle E-Business Suite Cloud Manager Version
• Navigate within Oracle E-Business Suite Cloud Manager
• Review Environments

Overview of Accessing Oracle E-Business Suite Cloud Manager

This section describes how to access Oracle E-Business Suite Cloud Manager on Oracle Cloud Infrastructure and review basic environment information.

Oracle E-Business Suite Cloud Manager is a tool for managing Oracle E-Business Suite environments on Oracle Cloud Infrastructure through a graphical user interface. You can use Oracle E-Business Suite Cloud Manager for fresh provisioning or provisioning as part of a lift and shift, for environment backups and restores, and for other lifecycle management activities. For a full list of Oracle E-Business Suite Cloud Manager features, see Features, page 1-1.

Prerequisites

You must have the following prerequisites to access Oracle E-Business Suite Cloud Manager and work with Oracle E-Business Suite environments.

• An Oracle E-Business Suite Cloud Manager instance set up as described in Deploy Oracle E-Business Suite Cloud Manager on Oracle Cloud Infrastructure, page 2-1.
• The compartment, resources, and Oracle E-Business Suite administrator user necessary to deploy your Oracle E-Business Suite environments as described in Set Up Your Tenancy to Host Oracle E-Business Suite Environments, page 3-1.

• Your user OCID. Note that you must be an Oracle E-Business Suite administrator to access the Oracle E-Business Suite Cloud Manager UI. See Where to Get the Tenancy’s OCID and User’s OCID [https://docs.cloud.oracle.com/en-us/iaas/Content/API/Concepts/apisigningkey.htm#Other]. Copy and paste the user OCID to a file that you can reference when instructed to enter it later in these steps.

• An Oracle Identity Cloud Service user name and password. See About Cloud Accounts with Identity Cloud Service [https://docs.oracle.com/en/cloud/get-started/subscriptions-cloud/csgsg/oracle-cloud-accounts.html#GUID-7896FC73-7576-42D3-9661-9E08C505F836].

Access Oracle E-Business Suite Cloud Manager

To access Oracle E-Business Suite Cloud Manager, perform the following tasks:

• Log In to Oracle E-Business Suite Cloud Manager, page 7-2

• Specify Your User Details (Conditionally Required), page 7-2

• Check Oracle E-Business Suite Cloud Manager Version, page 7-4

• Navigate within Oracle E-Business Suite Cloud Manager, page 7-4

• Review Environments, page 7-5

Log In to Oracle E-Business Suite Cloud Manager

Navigate to your Oracle E-Business Suite Cloud Manager instance at the URL established during its deployment. Log in with your Oracle Identity Cloud Service credentials. See Deploy Oracle E-Business Suite Cloud Manager on Oracle Cloud Infrastructure, page 2-1.

Specify Your User Details (Conditionally Required)

The following steps are required if you are logging in to Oracle E-Business Suite Cloud Manager for the first time.

Note: The Oracle E-Business Suite Cloud Manager administrator who performed the initial setup does not need to perform these steps.

Before you use Oracle E-Business Suite Cloud Manager for the first time, you must
specify user details in the Oracle Cloud Account Details page, including your user OCID.

1. When you log into Oracle E-Business Suite Cloud Manager for the first time, the Oracle Cloud Account Details page appears by default. You can review the tenancy details for your Oracle Cloud account.

2. In the Account Information region, enter your user OCID.

3. Click **Register User**, and then click **Register** in the confirmation dialog box.

4. Oracle E-Business Suite Cloud Manager generates a new public/private API signing key pair for the user you have registered. When prompted, download the public .pem key file to an accessible location.

   If you need to download the public key again later, click the **Get Public Key** link, and then click **Yes** in the confirmation dialog box.

   Oracle E-Business Suite Cloud Manager also derives the fingerprint for your user account from your key and displays it in the Account Information region.

5. Next, upload your public key to your user settings in the Oracle Cloud Infrastructure console. See “To Upload an API Signing Key” in Using the Console [https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Tasks/managingcredentials.htm#three]

   **Tip:** Navigate to the Oracle Cloud Infrastructure console in another browser window or tab so that you can perform the upload without leaving the Oracle E-Business Suite Cloud Manager page.

6. Return to the Oracle Cloud Account Details page, and click **Validate**. Oracle E-Business Suite Cloud Manager displays a confirmation message and then displays the Environments page.

   **Note:** You cannot change your user OCID after it is validated.

After you have registered and validated your user account, when you access Oracle E-Business Suite Cloud Manager again, the Environments page appears immediately after you log in.

7. To review your account details after your initial login, navigate to the Oracle Cloud Account Details page by clicking your user icon in the Oracle E-Business Suite Cloud Manager header and selecting **Profile**. To return to the Environments page, click **Done**.
Check Oracle E-Business Suite Cloud Manager Version

You should periodically check whether your Oracle E-Business Suite Cloud Manager instance is at the latest version.

1. Click your user icon in the Oracle E-Business Suite Cloud Manager header and select About.

2. The About the EBS Cloud Manager Console window displays the version number that is currently installed. If a later version is available, the window also displays a message indicating the version number that is available for update. We recommend that you update your instance as soon as feasible following the instructions in Update Oracle E-Business Suite Cloud Manager to the Latest Version, page 4-1.

3. The About the EBS Cloud Manager Console window also displays the private and public IP addresses for the Oracle E-Business Suite Cloud Manager VM. You can refer to these IP addresses to assist in troubleshooting any issues with connecting to Oracle E-Business Suite Cloud Manager.

Navigate within Oracle E-Business Suite Cloud Manager

Use the Navigator menu to access the Oracle E-Business Suite Cloud Manager functionality you want to use.

1. To review and manage your Oracle E-Business Suite environments, click the Navigator icon, and then select Environments. See Review Environments, page 7-5.

2. To review the backups of Oracle E-Business Suite environments stored on Oracle Cloud Infrastructure, click the Navigator icon, and then select Backups. See Review Backups, page 11-17.

   The Backups page includes both backups created from on-premises Oracle E-Business Suite environments and backups created from Oracle E-Business Suite environments that you previously provisioned on Oracle Cloud Infrastructure. See Create a Backup of an On-Premises Oracle E-Business Suite Instance on Oracle Cloud Infrastructure, page 5-2 and Create a Backup of a Cloud-Based Oracle E-Business Suite Instance, page 11-11.

   You can also review a list of the backups for a particular environment in the environment details page for that environment. See Review Environment Details, page 10-6.

3. To monitor the status of the activities performed in Oracle E-Business Suite Cloud Manager, click the Navigator icon, and then select Activities. See Monitor Activity Status, page 12-1.
You can also review a list of the activities performed for a particular environment in the environment details page for that environment. See Review Environment Details, page 10-6.

4. To review the network profiles that identify the network resources available for use in provisioning, click the Navigator icon, select Administration, and then select Network Profiles. See Set Up Network Profiles, page 8-1.

   If you are logged in as an Oracle E-Business Suite Cloud Manager administrator, you can use this page to create and delete custom network profiles.

   If you are logged in as a user without administrator privileges, then you can review the details for network profiles assigned to you, but you cannot update them.

5. If you are logged in as an Oracle E-Business Suite Cloud Manager administrator, then to extend Oracle E-Business Cloud Manager activities to meet your own requirements, click the Navigator icon, select Administration, and then select Extensibility. You can define extended activity plans for provisioning, cloning, and promoting standby environments. See Set Up the Extensibility Framework, page 8-8.

6. To set up scheduling policies for backups, click the Navigator icon, select Administration, and then select Scheduling Policies. See Set Up Scheduling Policies, page 8-14.

Review Environments

1. The Environments page lists the Oracle E-Business Suite environments provisioned in your Oracle E-Business Suite Cloud Manager instance, as well as standby environments and incomplete installations from unsuccessful provisioning attempts.

   If you are logged in as an Oracle E-Business Suite Cloud Manager administrator, then the Environments page shows all environments provisioned in your Oracle E-Business Suite Cloud Manager instance. If you are logged in as a user without administrator privileges, then the page shows only environments that were created in compartments to which you have access.

   You can optionally select a compartment to which you have access in the EBS Compartment field to display only environments that reside in that compartment.

   Note: If you used Oracle E-Business Suite Cloud Manager to deploy an environment with Oracle Database Release 11.2.0.4 or Release 12.1.0.2, and you manually upgrade that environment to Oracle Database 19c, then Oracle E-Business Suite Cloud Manager can no longer recognize that environment. For an environment
with the database tier on Compute or Exadata Cloud Service, you can run a script to refresh the metadata for the upgraded environment within Oracle E-Business Suite Cloud Manager. After the environment metadata has been refreshed, you can once again manage the environment through the Oracle E-Business Suite Cloud Manager UI. See Refresh Metadata for an Environment Upgraded to Oracle Database 19c, page 4-23.

2. You can optionally enter a value in the search field to display only environments whose properties contain that value. You can search by the following properties shown in this page:
   - Environment name
   - Network profile that defines the network resources used by the environment
   - Oracle E-Business Suite compartment where the environment resides
   - Database service type
   - Database name
   - Latest activity performed for this environment in Oracle E-Business Suite Cloud Manager
   - Creation date and time

3. To begin provisioning an environment, click **Provision Environment** and select either **One-Click** or **Advanced**. See One-Click Provisioning, page 9-6 or Advanced Provisioning, page 9-8.

4. To review additional details for an environment, including any backups created from that environment and activities performed for that environment, click the environment name link. Note that you can review details only for an existing environment that was successfully provisioned or an existing standby environment that was successfully created. See Review Environment Details, page 10-6.

5. To review details for the latest activity performed for an environment, click the activity status link. See Monitor Activity Status, page 12-1.

6. To clone an environment, click the **Actions** icon next to that environment, and then select **Clone**. Note that you can clone only an existing Compute environment that was successfully provisioned. See Clone an Oracle E-Business Suite Instance, page 11-5.

7. To create a backup of an environment, click the **Actions** icon next to that
environment, and then select **Create Backup**. Note that you can back up only an existing environment that was successfully provisioned. See Create a Backup of a Cloud-Based Oracle E-Business Suite Instance, page 11-11.

8. To promote a standby environment to a production environment, click the **Actions** icon next to that environment, and then select **Promote**. Note that you can promote only an existing standby environment that was successfully set up. See Promote a Standby Environment, page 11-21.

9. To delete an environment, click the **Actions** icon next to that environment, and then select **Delete**. You can delete existing environments or standby environments that you no longer need. You can also delete incomplete installations from unsuccessful provisioning attempts that you do not want to restart. See Delete an Oracle E-Business Suite Environment, page 11-26.
Configure Oracle E-Business Suite Cloud Manager Features

This chapter covers the following topics:

- Set Up Network Profiles
- Set Up the Extensibility Framework
- Set Up Scheduling Policies

Set Up Network Profiles

Before Oracle E-Business Suite Cloud Manager can be used to provision environments, a network and associated network profiles must be created. A network profile maps Oracle Cloud Infrastructure network definitions with the network requirements for Oracle E-Business Suite instances.

First, the network administrator creates a network, as described in Create Network Resources for Deploying Oracle E-Business Suite Environments, page 3-9. Next, the Oracle E-Business Suite Cloud Manager administrator uses Oracle E-Business Suite Cloud Manager to define related network profiles. Oracle E-Business Suite administrators can then select the network profiles when provisioning environments.

The network administrator can optionally use the ProvisionOCINetwork.pl script to create a default network and two default network profiles, one for One-Click Provisioning and one for Advanced Provisioning. The default network profiles are named DEFAULT_PROFILE_ONECLICK and DEFAULT_PROFILE_ADVANCED, respectively. The Oracle E-Business Suite Cloud Manager administrator can then use the UploadOCINetworkProfile.pl script to upload these network profiles. If the default network profiles have been created and uploaded to your Oracle E-Business Suite Cloud Manager instance, then they appear in the list in the Network Profiles page. To preserve consistency in the network, you cannot delete these network profiles. See Use a Default Network with Automated Scripts, page 3-10.

- Review Network Profiles, page 8-2
Review Network Profiles:

1. To review the network profiles that identify the network resources available for use in provisioning, click the Navigator icon, select Administration, and then select Network Profiles.

2. The Network Profiles page displays the network profiles to which you have access. You can optionally enter a full or partial value in the search field to display only network profiles whose properties contain that value. You can search by the following properties shown in this page:
   - Network profile name
   - Oracle E-Business Suite compartment
   - Network compartment
   - Region
   - VCN
   - Availability domain
   - Creation date and time

3. If you are logged in as an Oracle E-Business Suite Cloud Manager administrator, then you can use this page to perform the following actions:
   - To create a new custom network profile, click Create Network Profile. See Create a Network Profile, page 8-4.
   - To resubmit a network profile after correcting invalid property entries, click the Actions icon next to that network profile, and then select Resubmit. See Create a Network Profile, page 8-4.
   - To delete a network profile, click the Actions icon next to that network profile, and then select Delete Network Profile.

Note: To preserve consistency in the network, you cannot delete a network profile that is associated with an existing
environment. Additionally, you cannot delete the two default network profiles DEFAULT_PROFILE_ONECLICK and DEFAULT_PROFILE_ADVANCED.

If you are logged in as a user without administrator privileges, then you can review the details for network profiles assigned to you, but you cannot perform any administrative actions for them.

4. To review additional details for a network profile, click the network profile name link.

5. In the network profile details page, review the following properties:
   - Network profile name
   - Region
   - VCN
   - Network profile description
   - Oracle E-Business Suite compartment
   - Subnet type
   - Network compartment
   - Availability domain

6. In the Subnet Assignments region, review the following properties:
   - Database tier
     - Database tier subnet access, either Public or Private
     - Database tier subnet
   - Application tier internal zone
     - Application tier nodes subnet access, either Public or Private
     - Application tier nodes subnet
     - Load balancer visibility type, either Public or Private
     - Load balancer subnet
• Load balancer subnet for high availability (displayed only for network profiles with the Availability Domain-Specific subnet type and Public load balancer visibility type)

• Application tier external zone (displayed only if external zone support is enabled for this network profile)
  • Application tier nodes subnet access, either Public or Private
  • Application tier nodes subnet
  • Load balancer visibility type, either Public or Private
  • Load balancer subnet
  • Load balancer subnet for high availability (displayed only for network profiles with the Availability Domain-Specific subnet type and Public load balancer visibility type)

7. If you are logged in as an Oracle E-Business Suite Cloud Manager administrator, then you can use this page to perform the following actions:
  • To resubmit the network profile after correcting invalid property entries, click Resubmit. See Create a Network Profile, page 8-4.
  • To delete the network profile, click Delete Network Profile.

    Note: To preserve consistency in the network, you cannot delete a network profile that is associated with an existing environment. Additionally, you cannot delete the two default network profiles DEFAULT_PROFILE_ONECLICK and DEFAULT_PROFILE_ADVANCED.

If you are logged in as a user without administrator privileges, then you can review the details for a network profile assigned to you, but you cannot perform any administrative actions for it.

Create a Network Profile:
Before you create a network profile, ensure that the network administrator has created the network resources for the profile to use, as described in Create Network Resources for Deploying Oracle E-Business Suite Environments, page 3-9.

1. Click the Navigator icon, select Administration, and then select Network Profiles. In the Network Profiles page, click Create Network Profile.
2. In the Provision Network Profiles page, enter the following details:
   - **Network Profile Name**: Enter a name for the network profile, such as ebsprodlondonad1-profile.
   - **Network Profile Description**: Enter a description for the network profile.
   - **EBS Compartment**: Select the Oracle E-Business Suite compartment for this profile, such as ebsprod-compartment.
   - **Network Compartment**: Select the network compartment, such as network-compartment.

   *Note*: The compartments you can select are determined by policies defined in Oracle Cloud Infrastructure Identity and Access Management.

3. In the Network Assignment, region, enter the following details:
   - **Region**: Oracle E-Business Suite Cloud Manager displays the region for the network profile, which is determined by the region of its associated VM, such as uk-london-1.
   - **VCN**: Select a VCN, such as ebscm-vcn.
   - **Subnet Type**: Select the subnet type, either Regional or Availability Domain-Specific.
   - **Availability Domain**: Select the availability domain in which your Compute or VM database resources will be created, such as POKh:UK-LONDON-1-AD-1.

4. In the Subnet Assignments - Database Tier region, enter the following details:
   - **Subnet Access**: Select either Public or Private.
   - **Subnet**: Select the subnet for the database tier, such as db-subnet-ad1.

5. In the Subnet Assignments - Applications Tier region, enter the following details for internal zones:
   - **App Nodes Subnet Access**: Select either Public or Private.
   - **App Nodes Subnet**: Select the subnet for the application tier nodes in internal zones, such as apps-subnet-ad1.
   - **Load Balancer Visibility Type**: Select either Public or Private.
• **Load Balancer Subnet**: Select the subnet for the application tier load balancer in internal zones, such as ebslbaas-subnet-ad1.

• **Load Balancer HA Subnet**: Select the load balancer subnet for high availability, such as ebslbaas-subnet-ad2.

  **Note**: This field appears only if you select the Availability Domain-Specific subnet type and the Public load balancer visibility type. The field is not shown if you choose the Regional subnet type or if you use a single availability domain.

6. In the Subnet Assignments - Applications Tier region, optionally click the Support for External Zones toggle switch to enable external zones for this network profile. If you do so, the External Zones region appears.

7. In the Subnet Assignments - Applications Tier region, enter the following details for external zones:
   
   • **App Nodes Subnet Access**: Select either Public or Private.
   
   • **App Nodes Subnet**: Select the subnet for the application tier nodes in external zones, such as apps-subnet-ad1.
   
   • **Load Balancer Visibility Type**: Select either Public or Private.
   
   • **Load Balancer Subnet**: Select the subnet for the application tier load balancer in external zones, such as ebslbaas-subnet-ad1.
   
   • **Load Balancer HA Subnet**: Select the load balancer subnet for high availability, such as ebslbaas-subnet-ad2.

  **Note**: This field appears only if you select the Availability Domain-Specific subnet type and the Public load balancer visibility type. The field is not shown if you choose the Regional subnet type or if you use a single availability domain.

8. Click **Submit**.

9. You can check the status of the activity to create the backup in the Activities page. Locate the create-network-profile activity that you want to monitor, and click the activity name link to go to the Activity Details page. See Monitor Activity Status, page 12-1.

When you create a network profile, the create-network-profile activity is initially placed in the status Input Validation in Progress while Oracle E-
Business Suite Cloud Manager validates that the network and subnets assigned to the network profile include the required ingress and egress security rules.

The Activity Details page provides links to the log files for each task performed to create the network profile, including pre-validation tasks and main execution tasks. If a network profile creation activity does not succeed, you can review the related log files for the specific task that failed to troubleshoot the issue.

- If the network properties for the profile are specified correctly, but some security rules are missing, then you should first have the network administrator define the required security rules. Then, after the security rules are in place, you can retry the failed `create-network-profile` activity from the Activity Details page. See Monitor Activity Status, page 12-1.

- If you need to correct the network properties specified in the network profile definition, then you should update and resubmit the network profile. You can either navigate to the Network Profiles page, click the Actions icon next to the network profile you need to update, and then select Resubmit, or navigate to the network profile details page for this network profile and click Resubmit. See Review Network Profiles, page 8-2.

The Provision Network Profile page appears to let you re-enter the network and subnet properties. After entering all the required properties, click Resubmit. Then monitor the status of the new `create-network-profile` activity. See Monitor Activity Status, page 12-1.

Note: You can only resubmit a network profile that failed its initial validation. After a network profile is successfully created and validated, you cannot make any further changes in its properties.

Delete a Network Profile:
You can delete a custom network profile either from the Network Profiles page or from the details page for a particular network profile. See Review Network Profiles, page 8-2.

Note: To preserve consistency in the network, you cannot delete a network profile that is associated with an existing environment. Additionally, you cannot delete the two default network profiles `DEFAULT_PROFILE_ONECLICK` and `DEFAULT_PROFILE_ADVANCED`.

Known Limitation:
If you are using the Internet Explorer browser, you may encounter an issue while creating a network profile. As a workaround, switch to another browser to create your network profiles.
Set Up the Extensibility Framework

The Extensibility Framework lets Oracle E-Business Suite Cloud Manager administrators extend the activities performed by Oracle E-Business Suite Cloud Manager by adding tasks to meet your own requirements. You can define extended activity plans for activities including Advanced Provisioning, cloning, and promoting standby environments.

Oracle E-Business Suite Cloud Manager provides several seeded tasks for commonly required processing, which you can add to an extended activity plan as needed. For a list of seeded tasks, see Seeded Tasks in the Extensibility Framework, page A-1.

You can also create your own tasks to use in your extended activity plans. For a custom task, you must develop a script that defines the processing performed in the task and package that script in a zip file together with all its supporting files. You can then upload the zip file when you create the task in the Extensibility Framework UI. For guidelines on developing and packaging a script for a custom task, see Custom Task Scripts in the Extensibility Framework, page A-3.

**Note:** You must be logged in as a user with Oracle E-Business Suite Cloud Manager administrator privileges to manage tasks and extended activity plans in the Extensibility Framework.

- Review and Manage Tasks, page 8-8
- Create a Task, page 8-10
- Review and Manage Extended Activity Plans, page 8-11
- Extend an Activity Plan, page 8-12
- Use an Extended Activity Plan in Oracle E-Business Suite Cloud Manager Processing, page 8-14

**Review and Manage Tasks:**

1. To review and manage the tasks available for use in extended activity plans, click the Navigator icon, select Administration, and then select Extensibility. If the Tasks page is not already displayed, click the Tasks tab.

   **Note:** You must be logged in as a user with Oracle E-Business Suite Cloud Manager administrator privileges to manage tasks in the Extensibility Framework.

2. The Tasks page displays both seeded tasks and custom tasks that you created. You
can optionally enter a full or partial value in the search field to display only tasks whose properties contain that value. You can search by the following properties shown in this page:

- Task name

- Task type, either Seeded or Custom

- The location from which the task is run, either the Oracle E-Business Suite Cloud Manager VM (EBSCloudManager), all nodes for the environment (AllNodes), all database tier nodes for the environment (AllDbNodes), all application tier nodes for the environment (AllAppNodes), or the primary application tier node for the environment (PrimaryAppNode)

  **Note:** Only seeded tasks can be run from the Oracle E-Business Suite Cloud Manager VM (EBSCloudManager).

- The user who created the task

- Creation date and time

3. To review additional details for a task, click the task name link. In the task details window, review the following properties:

- Task name

- Description

- The location from which the task is run

- Whether the task is a lifecycle management activity

- The script that is run to perform the task

- The file name of the zip file that contains the script and any supporting libraries

- Any input parameters for the script, including the following details
  - Internal parameter name
  - Displayed parameter label
  - Whether the parameter is considered sensitive and should have its value masked in display
  - The default value defined for the parameter, if any
For a custom task, you can click the download icon next to the library file name to download a copy of that file.

4. To create a new custom task, click **Create Task**. See Create a Custom Task, page 8-10.

5. To edit a custom task, click the **Actions** icon next to that task, and then select **Edit**. See Create a Custom Task, page 8-10.

   **Note:** You cannot edit seeded tasks.

   Additionally, you cannot edit a custom task that is part of the running activity plan while a provisioning, cloning, or standby promotion activity is in progress.

   provisioning is in progress, if the task is part of the running activity plan.”

6. To delete a custom task, click the **Actions** icon next to that task, and then select **Delete**.

   **Note:** You cannot delete seeded tasks.

   Additionally, you cannot delete a custom task that is part of an extended activity plan. You must first delete all custom plans that reference a task before you can delete that task.

**Create a Task:**

The steps for creating a new custom task and for editing an existing custom task are the same, except that you cannot change the name of an existing task.

1. Click the **Navigator** icon, select **Administration**, and then select **Extensibility**. If the Tasks page is not already displayed, click the **Tasks** tab. Then click **Create Task**.

   If you are editing an existing task, in the Tasks page, click the **Actions** icon next to that task, and then select **Edit**.

2. In the Create Task or Edit Task page, enter the following details:

   • **Task Name**: Enter a name for the task. Note that you cannot change the name of a task after you enter all the required task details and the task details are saved.

   • **Description**: Enter an optional description for the task.

   • **Run From**: Select the location from which the task is run, either All Nodes, All Database Nodes, All Application Tier Nodes, or Primary Application Tier
Configure Oracle E-Business Suite Cloud Manager Features

Node.

- **Script to Run**: Enter the file name of the shell script to run to perform the task. The file name can only contain alphanumeric characters and must end with the file extension `.sh`.
  
  For more information about writing a script for a custom task, see Create a Wrapper Script, page A-4.

- **Source Code Library**: Upload the zip file that contains the main script for the task as well as any supporting libraries required to run the main script. You can either drag and drop the library file onto the **Source Code Library** field, or click in the field and browse to the location of the file to select it.
  
  For more information about packaging the source code for a custom task in a library zip file, see Package the Script in a Zip File, page A-21.
  
  After you upload the library file, Oracle E-Business Suite Cloud Manager displays the uploaded file name.

3. If the script requires input parameters to be entered when the activity is submitted, specify those parameters in the Input Parameters region. Click **Add** to add a new parameter and then enter the following details:
   
   - **Name**: Enter the internal name for the parameter. The internal name can contain only alphanumeric characters and underscores.
   
   - **Label**: Enter the parameter label displayed in the Oracle E-Business Suite Cloud Manager UI.
   
   - **Sensitive**: Use this toggle switch to specify whether the value for this parameter is considered sensitive and should be masked in display.
   
   - **Default Value**: Optionally enter a default value for the parameter.
  
  To remove a parameter that you no longer need, click the remove icon next to that parameter.

4. Click **Create Task**.

**Review and Manage Extended Activity Plans**:

1. To review and manage extended activity plans, click the **Navigator** icon, select **Administration**, and then select **Extensibility**. Then click the **Extended Activity Plans** tab.

   **Note**: You must be logged in as a user with Oracle E-Business Suite
Cloud Manager administrator privileges to manage extended activity plans in the Extensibility Framework.

2. The Extended Activity Plans page displays a list of the extended activity plans defined in your Oracle E-Business Suite Cloud Manager instance. You can optionally enter a full or partial value in the search field to display only plans whose properties contain that value. You can search by the following properties shown in this page:
   - Plan name
   - The base activity plan that this plan extends, either EBS Provisioning, EBS Clone, or EBS Promote Standby.
   - The user who created the plan
   - Creation date and time

3. To review additional details for a plan, click the plan name link. In the plan details window, review the list of phases included in the plan and the tasks included in each phase. The plan details window also displays whether each phase and task is seeded or custom.

4. To create a new extended activity plan, click **Extend Activity Plan**. See Extend an Activity Plan, page 8-12.

5. To edit an extended activity plan, click the **Actions** icon next to that plan, and then select **Edit**. See Extend an Activity Plan, page 8-12.
   
   **Note:** You cannot edit an extended activity plan that is currently in use by an in-progress activity.

6. To delete an extended activity plan, click the **Actions** icon next to that plan, and then select **Delete**.
   
   **Note:** You cannot delete an extended activity plan that is currently in use by an in-progress activity.

**Extend an Activity Plan:**
The steps for creating a new extended activity plan and for editing an existing extended activity plan are the same, except that you cannot change the name or template for an existing plan.
1. Click the **Navigator** icon, select **Administration**, and then select **Extensibility**. Click the **Extended Activity Plans** tab. Then click **Extend Activity Plan**.

   If you are editing an existing plan, then in the Extended Activity Plans page, click the **Actions** icon next to that plan, and then select **Edit**.

2. Enter the following basic plan properties:
   
   - **Name**: Enter a name for the plan. Note that you cannot change the name of an existing plan.
   
   - **Description**: Enter an optional description for the plan.
   
   - **Base Plan**: Select the base plan for the activity you want to extend, either **EBS Provisioning**, **EBS Clone**, or **EBS Promote Standby**. Note that you cannot change the base plan for an existing extended activity plan.

   Then click **Next**.

3. Specify the details for the plan. The Activity Plan Details page initially displays the default phases that are part of the base plan. You can optionally add a phase to the plan with additional tasks to meet your own requirements.

   - Click the **Actions** icon next to the last phase in the base plan, and then select **Insert After** to insert an additional phase at the end of the plan.

   - The Select Tasks window displays the list of available tasks, including seeded tasks provided by Oracle and any custom tasks defined in your Oracle E-Business Suite Cloud Manager instance. You can enter a full or partial value in the **Filter** field to display only tasks whose name matches that value. Select the tasks you want to add to the plan and then click **Add Tasks**.

   - To change the order of the tasks, click the reorder icon next to a task and drag it to the position you want in the list.

   - To add more tasks, click the **Actions** icon next to your additional phase, and then select **Add Tasks**.

   - To delete a task, click the **Actions** icon next to that task, and then select **Delete Task**.

   - To delete the entire additional phase, including all tasks within it, click the **Actions** icon next to that phase, and then select **Delete Phase**.

   When you have finished updating the details for the plan, click **Next**.

4. In the Review Extended Activity Plan page, review the plan’s basic properties and the phase and task details. To save the plan, click **Submit**.
Use an Extended Activity Plan in Oracle E-Business Suite Cloud Manager Processing:

After an Oracle E-Business Suite Cloud Manager administrator has created an extended activity plan for Advanced Provisioning, cloning, or promoting a standby environment, Oracle E-Business Suite administrators can select that plan when submitting that type of activity. The Oracle E-Business Suite administrator must provide any input parameters required by the added tasks. Oracle E-Business Suite Cloud Manager will then perform the activity according to the extended activity plan, including any tasks specified in the additional phase. See Advanced Provisioning, page 9-8, Clone an Oracle E-Business Suite Instance, page 11-5, and Promote a Standby Environment, page 11-21.

Set Up Scheduling Policies

You can create backups for an Oracle E-Business Suite environment automatically on a schedule by defining scheduling policies.

Note: The backup feature is available for environments created using Advanced Provisioning. For more information about prerequisites for backups, see Back Up an Oracle E-Business Suite Instance, page 11-10.

To create a scheduling policy, you first define the policy itself, and then add one or more schedules to the policy. Schedules define the frequency at which backups are created. You can define the following types of schedules:

- **Daily**: Backups are generated daily. You specify the hour of the day for the backup.

- **Weekly**: Backups are generated weekly. You specify the day of the week and the hour of that day for the backup.

- **Monthly**: Backups are generated monthly. You specify the day of the month and the hour of that day for the backup.

- **Yearly**: Backups are generated yearly. You specify the month, the day of that month, and the hour of that day for the backup.

  Note: Scheduled backups are not guaranteed to start at the exact time specified by the schedule. You may see up to several hours of delay between the scheduled start time and the actual start time for the backup in scenarios where the system is overloaded.

- Review Scheduling Policies, page 8-15

- Create a Scheduling Policy, page 8-15
• Assign a Scheduling Policy to an Environment, page 8-17
• Delete a Scheduling Policy, page 8-17

**Review Scheduling Policies:**
1. To review the scheduling policies available for use in scheduling backups, click the Navigator icon, select Administration, and then select Scheduling Policies.

2. The Policies page displays the scheduling policies defined in your Oracle E-Business Suite Cloud Manager instance. You can optionally enter a full or partial value in the search field to display only policies whose properties contain that value. You can search by the following properties shown in this page:
   • Policy name
   • Policy type (create-ossbackup for backup scheduling policies)
   • The user who created the policy
   • Creation date and time

3. To create a new policy, click Create Policy. See Create a Scheduling Policy, page 8-15.

4. To review details or define schedules for a policy, either click the policy name link or click the Actions icon next to that policy and then select Edit. See Manage Policy Details, page 8-16.

5. To delete a policy, click the Actions icon next to that policy, and then select Delete.

**Create a Scheduling Policy:**
To create a scheduling policy, you first define the policy itself, and then add one or more schedules to the policy.

**Create a Policy**
1. Click the Navigator icon, select Administration, and then select Scheduling Policies. In the Policies page, click Create Policy.

2. In the Create Policy window, enter a name for the policy.

3. Select the compartment in which backups created using this policy will be stored.

4. Click Create.
Manage Policy Details
1. Click the Navigator icon, select Administration, and then select Scheduling Policies. In the Policies page, either click the policy name link or click the Actions icon next to that policy and then select Edit.

2. In the policy details page, review the following details:
   - Policy name
   - Compartment
   - The user who created the policy
   - Creation date and time
   - Any schedules defined for the policy, including the schedule type and start time

3. To add a schedule to the policy, click Add Schedule. See Define a Schedule, page 8-16.

4. To edit a schedule, click the Actions icon next to that schedule, and then select Edit. See Define a Schedule, page 8-16.

5. To delete a schedule, click the Actions icon next to that schedule, and then select Delete.

6. After you finish updating schedules for the policy, click Save Policy to commit your changes.

7. To delete the policy, click Delete Policy.

Define a Schedule
1. In the Create Schedule window or Edit Schedule window, select the schedule type: Daily, Weekly, Monthly, or Yearly.

2. Specify the appropriate schedule options depending on the schedule type.
   - Daily: Specify the hour of the day for the backup.
   - Weekly: Specify the day of the week and the hour of that day for the backup.
   - Monthly: Specify the day of the month and the hour of that day for the backup.
   - Yearly: Specify the month, the day of that month, and the hour of that day for the backup.
The schedule settings are based on the UTC time zone.

3. Click Create Schedule for a new schedule, or Edit Schedule for an existing schedule.

4. Click Save Policy in the policy details page to commit your changes.

Assign a Scheduling Policy to an Environment:
After you create a policy, you can use it to create backups for an environment automatically on the specified schedule. To do so, assign the policy to the environment in the environment details page.

If you no longer want to create backups on that schedule, you can remove the policy assignment for the environment in the environment details page.


Delete a Scheduling Policy:
You can delete a scheduling policy either from the Policies page or from the details page for a particular policy. See Review Scheduling Policies, page 8-15 or Review Policy Details, page 8-16.
Provision an Oracle E-Business Suite Instance

This chapter covers the following topics:

- Requirements for Provisioning a New Environment
- One-Click Provisioning
- Advanced Provisioning
- Perform Post-Provisioning and Post-Cloning Tasks

Requirements for Provisioning a New Environment

With the automated provisioning options in Oracle E-Business Suite Cloud Manager, you can create a new environment of Oracle E-Business Suite.

Options for New Environments

The tables in this section show the available options for provisioning a new environment.

The following table describes the options available for provisioning an environment as described in One-Click Provisioning, page 9-6.
Table 9-1 New Environment Options for One-Click Provisioning

<table>
<thead>
<tr>
<th>Available Product Combination for Deployment</th>
<th>Cloud Service For Application, Database, and Oracle Enterprise Command Center Framework Tiers [1]</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Oracle E-Business Suite Release 12.2.10</td>
<td>• Oracle Cloud Infrastructure Compute virtual machine (VM)</td>
</tr>
<tr>
<td>• Oracle Database Release 19c (19.8) - Vision demo</td>
<td>• Oracle Cloud Infrastructure Compute supports only single instance databases; it does not support Oracle RAC databases.</td>
</tr>
<tr>
<td>• Oracle Enterprise Command Center Framework V5 [2]</td>
<td></td>
</tr>
</tbody>
</table>

Footnotes on Table 9-1:

1. If you use One-Click Provisioning, page 9-6, then the application, database, and Oracle Enterprise Command Center Framework tiers will be installed on a single Compute VM as part of the streamlined preset topology. This Compute VM will be created with Oracle Linux 7.9.

2. The Oracle Assets Command Center dashboard is pre-configured in your environment, and you can configure other dashboards as needed.

   **Note:** Oracle E-Business Suite Release 12.2.10 (with Oracle Database 19c (19.8) and Oracle Enterprise Command Center Framework V5) is available only if you have upgraded to Oracle E-Business Suite Cloud Manager version 20.2.1.0.2. If you are on Oracle E-Business Suite Cloud Manager version 20.2.1.0.1 or earlier, then the product combination available for One-Click Provisioning is Oracle E-Business Suite Release 12.2.9 with Oracle Database 19c (19.6) - Vision demo, and the combined application tier and database tier VM will be created with Oracle Linux 7.8.

The following table describes the options available for provisioning an environment as described in Advanced Provisioning, page 9-8.
### Table 9-2 New Environment Options for Advanced Provisioning

<table>
<thead>
<tr>
<th>Products Available for Deployment</th>
<th>Cloud Service For Application Tier</th>
<th>Cloud Service For Database Tier [1]</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Oracle E-Business Suite Release 12.2.10 with the following Oracle Database release:</td>
<td>Oracle Cloud Infrastructure Compute virtual machine (VM) [2]</td>
<td>• Oracle Cloud Infrastructure Compute VM [2]</td>
</tr>
<tr>
<td>• 19c (19.7) - Vision demo and fresh installation</td>
<td></td>
<td>Oracle Cloud Infrastructure Compute virtual machine (VM) [2]</td>
</tr>
<tr>
<td>• Oracle E-Business Suite Release 12.2.9 with the following Oracle Database releases:</td>
<td></td>
<td>• 1-Node VM DB System (Single Instance) [3]</td>
</tr>
<tr>
<td>• 19c (19.6) - Vision demo and fresh installation</td>
<td></td>
<td>• Database edition options:</td>
</tr>
<tr>
<td>• 12.1.0.2 - Vision demo and fresh installation</td>
<td></td>
<td>• Enterprise Edition</td>
</tr>
<tr>
<td>• Oracle E-Business Suite Release 12.2.8 with the following Oracle Database release:</td>
<td></td>
<td>• Enterprise Edition High Performance</td>
</tr>
<tr>
<td>• 11.2.0.4 - Vision demo</td>
<td></td>
<td>• Enterprise Edition Extreme Performance</td>
</tr>
<tr>
<td>• Oracle E-Business Suite Release 12.1.3 with the following Oracle Database release:</td>
<td></td>
<td>2-Node VM DB System (Oracle RAC) [3]</td>
</tr>
<tr>
<td>• 12.1.0.2 - Vision demo and fresh installation</td>
<td></td>
<td>• Database edition option</td>
</tr>
<tr>
<td>• 11.2.0.4 - Vision</td>
<td></td>
<td>• Enterprise Edition Extreme Performance</td>
</tr>
</tbody>
</table>


This database tier service provides Oracle RAC support.
Footnotes on Table 9-2:

1. If you use Advanced Provisioning, page 9-8, then you can choose any of the cloud services listed here for your database tier.

2. The application tier and database tier VMs will be created with Oracle Linux 7.6.

3. When placing your Release 19c or 12.1.0.2 database tier on either 1-Node VM DB System or 2-Node VM DB System using Advanced Provisioning in Oracle E-Business Suite Cloud Manager, you will choose from the available certified database bundle patches shown.

4. When placing your Release 19c or 12.1.0.2 database tier on Exadata Cloud Service using Advanced Provisioning in Oracle E-Business Suite Cloud Manager, you will choose from the available certified database bundle patches shown.

Cloud Services Minimum Resource Recommendations

To provision a new environment, we recommend that you have cloud service resources that match or exceed those specified in the following table:

Table 9-3 Cloud Services Minimum Resource Recommendations

<table>
<thead>
<tr>
<th>Description</th>
<th>Machine Type</th>
<th>Number of Machines</th>
<th>OCPUs</th>
<th>Memory</th>
<th>Storage</th>
<th>External IPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle E-Business Suite Cloud Manager VM</td>
<td>1</td>
<td>1</td>
<td>7 GB</td>
<td>55 GB (block)</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Machine Type</td>
<td>Number of Machines</td>
<td>OCPUs</td>
<td>Memory</td>
<td>Storage</td>
<td>External IPs</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------</td>
<td>--------------</td>
<td>--------------------</td>
<td>-------------</td>
<td>--------</td>
<td>---------</td>
<td>--------------</td>
</tr>
<tr>
<td>A load balancer (You can use your own load balancer or Load Balancer as a Service [LBaaS])</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>1</td>
</tr>
<tr>
<td>Application tier</td>
<td>VM</td>
<td>n (where 'n' is the number of application tier nodes in the target environment)</td>
<td>n*m (where 'm' is the number of OCPUs in the shape selected for the application tier; the minimum for 'm' is 1)</td>
<td>Release 12.2 = 14 GB per VM</td>
<td>Release 12.1 = 7 GB per VM</td>
<td>Shared application tier: 170 GB + 40 GB for each additional application tier (block) Non-shared application tier: 170 GB x n (block) Per language: 16 GB (block)</td>
</tr>
<tr>
<td>Database tier on Oracle Cloud Infrastructure Compute</td>
<td>VM</td>
<td>1</td>
<td>2</td>
<td>14 GB</td>
<td>Vision demo: 300 GB Fresh install: 200 GB</td>
<td>1</td>
</tr>
<tr>
<td>Description</td>
<td>Machine Type</td>
<td>Number of Machines</td>
<td>OCPUs</td>
<td>Memory</td>
<td>Storage</td>
<td>External IPs</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>--------------</td>
<td>--------------------</td>
<td>-------</td>
<td>--------</td>
<td>------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Database tier on 1-Node VM DB System (Single Instance)</td>
<td>VM</td>
<td>1</td>
<td>2</td>
<td>14 GB</td>
<td>Vision demo: 256 GB</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Fresh install: 256 GB</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Total storage: 712 GB [1]</td>
<td></td>
</tr>
<tr>
<td>Database tier on 2-Node VM DB System</td>
<td>VM</td>
<td>2</td>
<td>2 per VM</td>
<td>30 GB per VM</td>
<td>Vision demo: 256 GB</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Fresh install: 256 GB</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Total storage: 912 GB [1]</td>
<td></td>
</tr>
<tr>
<td>Database tier on Exadata Cloud Service Oracle RAC [2]</td>
<td>Bare Metal</td>
<td>2</td>
<td>11 x 2</td>
<td>720 GB x 2</td>
<td>84 TB</td>
<td>2</td>
</tr>
</tbody>
</table>

Footnotes on Table 9-3:

1. The Available Storage Size and Total Storage Size are different. For more information, see Bare Metal and Virtual Machine DB Systems [https://docs.cloud.oracle.com/en-us/iaas/Content/Database/Concepts/overview.htm#virtualmachine].

2. These are the minimum specifications provided by an Exadata Cloud Service Quarter Rack.

**One-Click Provisioning**

One-Click Provisioning streamlines the process of provisioning a new environment by using preset topology options. This option is available if your network administrator
created the necessary network resources for your Oracle E-Business Suite Virtual Cloud Network (VCN), using the `ProvisionOCINetwork.pl` script. These resources are grouped into a default network profile called `DEFAULT_PROFILE_ONECLICK`. Your Oracle E-Business Suite Cloud Manager administrator must also upload this network profile using the `UploadOCINetworkProfile.pl` script. One-Click Provisioning uses the subnets and security lists defined in the `DEFAULT_PROFILE_ONECLICK` network profile. See Create Network Resources For Deploying Oracle E-Business Suite Instances, page 3-9.

Your new environment will be created with a single application tier and database tier on the same Compute instance, using default configuration options. The environment is created in Availability Domain 1 in a Compute instance with the VM Standard 2.1 shape. For more information on the shape, refer to Standard Shapes [https://docs.cloud.oracle.com/en-us/iaas/Content/Compute/References/computeshapes.htm#vmshapes__vm-standard].

The environment is configured with Transport Layer Security (TLS) enabled for inbound HTTP traffic.

Your new environment will have Enterprise Command Centers pre-configured, using the same virtual machine (VM) as the application tier and database tier. The Oracle Assets Command Center dashboard is pre-configured in your environment. You can configure other dashboards as needed.

If you would like to configure your environment instead of using the preset One-Click Provisioning topology, follow the steps in the section Advanced Provisioning, page 9-8.

When provisioning, you can choose a predefined tag or specify a new (free-form) tag to identify all resources associated with an environment or group of environments. Refer to Managing Tags and Tag Namespaces [https://docs.cloud.oracle.com/en-us/iaas/Content/Tagging/Tasks/managingtagsandtagnamespaces.htm] for more information.

Note that One-Click Provisioning was formerly referred to as Simplified Provisioning in an earlier release.

**Prerequisites**

- You must have cloud resources that match or exceed the minimum recommendations specified in the section Requirements for Provisioning a New Environment, page 9-1.

- You must have network resources including the subnets needed to support the topology created by One-Click Provisioning. See the section Create Network Resources For Deploying Oracle E-Business Suite Environments, page 3-9.

- If you choose to use tags, you can create defined tags first. Any tag namespace selected must be defined for the compartment in which you are provisioning, as
specified in the network profile. Refer to Managing Tags and Tag Namespaces [https://docs.cloud.oracle.com/en-us/iaas/Content/Tagging/Tasks/managingtagsandtagnamespaces.htm] for more information.

**Provision an Environment using One-Click Provisioning:**

1. On the Oracle E-Business Suite Cloud Manager Environments page, click **Provision Environment** and select **One-Click**.

2. Enter the values for your new environment:
   - **Environment Name**: Accept the system-generated name or enter a new name for your environment. For example: `usdev1`
   - **Purpose**: Vision Demo Install
   - **EBS Version**: Select the Oracle E-Business Suite version for your environment.
   - **DB Version**: Select the database version for your environment.

   The available database versions depend on the Oracle E-Business Suite version you selected. See Requirements for Provisioning a New Environment, page 9-1.

3. Optionally enter tagging information in the Tags region.
   - **Tag Namespace**: Select a predefined tag namespace or select **None (add a free-form tag)**.
   - **Tag Key**: Enter the name you use to refer to the tag.
   - **Value**: Enter the value for the tag key.

4. Click **Submit**.

5. You can check the status of the activity to provision the environment in the Activities page.

   After the environment is successfully provisioned, perform any necessary post-provisioning steps and access your environment following the instructions provided in Perform Post-Provisioning and Post-Cloning Tasks, page 9-24.

**Advanced Provisioning**

With Advanced Provisioning, you can choose how to configure your own topology for a new environment, instead of using the basic preset topology options in One-Click Provisioning, page 9-6. You can also use Advanced Provisioning to provision an environment based on a backup of another environment.
Note these additional key attributes:

- Advanced Provisioning provides the option to deploy and configure a Load Balancer as a Service (LBaaS). You may instead choose not to use a load balancer, or to use an on-premises load balancer. Perform Post-Provisioning and Post-Cloning Tasks, page 9-24 provides instructions appropriate to each use case.

- The administrator of your Oracle E-Business Suite Cloud Manager instance defines network profiles, which specify the network resources that you can use to provision Oracle E-Business Suite environments. During Advanced Provisioning, you select the network profile to use for the environment you are creating. For information on how to create default network resources and an associated default network profile DEFAULT_PROFILE_ADVANCED designed for use in Advanced Provisioning, refer to the following sections:
  - Create Network Resources For Deploying Oracle E-Business Suite Environments, page 3-9
  - Create Network Profiles, page 3-34

You can also create additional network profiles. Refer to Create a Network Profile, page 8-4

- Note that a network profile can be defined to use a private subnet for the database, application tier, or Load Balancer as a Service (LBaaS). If you select a network profile that uses a private subnet for any VM, then the corresponding VM will not have a public IP address and no inbound connections to this VM from outside the current VCN will be allowed.

- Our automation configures the application tier services to utilize port pools 0 and 1. These cannot be changed. Create Security Rules, page 3-21 lists the ports that must be open between subnets in order for your system to function properly.

- If you choose Virtual Machine DB System or Exadata System for the Cloud Database Service, then Transparent Data Encryption (TDE) is automatically enabled, both for new environments and for environments created from a backup. Additionally, if you provision an environment from a backup of a TDE-enabled source environment and you choose Compute as the Cloud Database Service, TDE is also automatically enabled.

- If you use Advanced Provisioning to provision a new environment on Compute or an environment on Compute that is created from a backup of a non-TDE source environment, then you can optionally choose to enable TDE.

- When you provision an environment, the Installation Details page allows you to choose a pre-defined tag, or specify a new (free-form) tag. You can use this tag to identify all resources associated with an environment or group of environments. Refer to Managing Tags and Tag Namespaces [https://docs.cloud.oracle.com/e-
• When an environment is provisioned, the deployed database tier node or nodes and application tier node or nodes will be associated with a fault domain. The fault domains can be chosen for you, or you can specify them yourself. Refer to Fault Domains [https://docs.cloud.oracle.com/iaas/Content/General/Concepts/regions.htm#fault ] for more information.

In addition, you can configure multiple zones in your environment. Each zone has its own web entry point and application tier nodes. Each zone can have its own load balancer to manage traffic, or multiple zones of the same type can share a load balancer. One zone is created by default when you provision an environment. For more information on using zones, see: My Oracle Support Knowledge Document 1375670.1, Oracle E-Business Suite Release 12.2 Configuration in a DMZ [https://support.oracle.com/rs?type=doc&id=1375670.1].

Example Virtual Cloud Network with an Internal Zone and External Zone

Prerequisites

❑ You must have cloud resources that match or exceed the minimum recommendations specified in Requirements for Provisioning a New Environment, page 9-1.

❑ You must have a network profile that includes network resources to support the topology you plan to use, including the security lists and subnets. The administrator of your Oracle E-Business Suite Cloud Manager instance defines network profiles and assigns you the profiles that you can use to provision Oracle E-Business Suite environments.

Refer to the following sections:

• Create Network Resources For Deploying Oracle E-Business Suite
• Create Network Profiles, page 3-34

❑ If you choose to use tags, you can create defined tags first. Any tag namespace selected must be defined for the compartment in which you are provisioning, as specified in the network profile. Refer to Managing Tags and Tag Namespaces [https://docs.cloud.oracle.com/en-us/iaas/Content/Tagging/Tasks/managingtagsandtagnamespaces.htm] for more information.

❑ You can optionally choose to use an on-premises load balancer. If you choose to use a load balancer that you deploy on-premises, the network profile must have the application tier security list configured so that it can communicate with the on-premises load balancer.

Additional Requirements for Exadata Cloud Service:
Beginning with Release 20.2.1.1.1 of the Oracle E-Business Suite Manager, Advanced Provisioning can provision environments only on Exadata Cloud Service instances that follow the new Exadata Resource Model.


If you plan to use Oracle E-Business Suite Cloud Manager Advanced Provisioning to provision your database to a pre-existing Exadata Cloud Service instance, you must first ensure that the SSH keys associated with the Oracle E-Business Suite Cloud Manager Virtual Machine (VM) are added to the associated Exadata VM cluster. Follow the instructions below to obtain the Oracle E-Business Suite Cloud Manager VM SSH key and copy it to the Exadata Cloud Service VM Cluster. For more information about Oracle E-Business Suite Cloud Manager deployment prerequisites, refer to Deploy Oracle E-Business Suite Cloud Manager on Oracle Cloud Infrastructure, page 2-1.

1. Log in to the Oracle E-Business Suite Cloud Manager VM using the oracle user ID, as shown below:
   $ cd ~/.ssh
   $ cat id_rsa.pub

2. Copy the contents to the clipboard.

3. Use the Oracle Cloud Infrastructure Direct Sign-in to log in to the Oracle Cloud
Infrastructure console.

4. Using the menu, navigate to Oracle Database, then Bare Metal, VM, and Exadata.

5. Choose the compartment where your infrastructure is located.

6. Under Exadata at Oracle Cloud, select Exadata Infrastructure, and click on your Exadata Infrastructure resource to go to the Exadata Infrastructure Details page.

7. Click on the name of the Exadata VM Cluster.

8. Select Add SSH Keys.

9. Select Paste SSH Keys, and paste the content previously copied into the SSH KEYS field.

10. Click Save Changes.

Access the Advanced Provisioning Feature:
Advanced Provisioning can be used to create a new environment or create an environment from a backup. Navigate to Advanced Provisioning using one of the following options. Then continue either to Enter Installation Details for a New Implementation, page 9-13 or Enter Installation Details for an Environment from a Backup, page 9-14 depending on the option you chose.

- If you are creating a new environment: On the main Oracle E-Business Suite Cloud Manager Environments page, click Provision Environment and select Advanced. Make sure the Installation Type option is defaulted to New Installation. Now continue to Enter Installation Details for a New Implementation , page 9-13 for the next steps.

- If you are creating an environment from a backup of either an on-premises environment or a Cloud environment: On the main Oracle E-Business Suite Cloud Manager Environments page, click Provision Environment and select Advanced. Select Provision from Object Storage Backup as the installation type. Now continue to Enter Installation Details for an Environment from a Backup, page 9-14 for the next steps.

- If you are creating an environment from a backup of either an on-premises environment or a Cloud environment: Click the Navigator icon and select Backups. Click Action for a backup and select Provision Environment. Make sure the Installation Type option is defaulted to Provision from Object Storage Backup. Now continue to Enter Installation Details for an Environment from a Backup, page 9-14 for the next steps.

- If you are creating an environment from a backup of a Cloud environment: On the
Environment Details page for the source environment, choose the **Backups** tab, click **Action** for a backup and select **Provision Environment**. Make sure the Installation Type option is defaulted to **Provision from Object Storage Backup**. Now continue to Enter Installation Details for an Environment from a Backup, page 9-14 for the next steps.

**Enter Installation Details for a New Implementation:**

1. Enter details for your new environment:
   - **EBS Compartment**: Select your Oracle E-Business Suite compartment. Only compartments that you have access to are shown.
   - **Network Profile**: Select the network profile that contains the network resources you want to use to provision your environment. For example: `DEFAULT_PROFILE_ADVANCED`. Click the information icon to view the Network Profile Details.
   - **Environment Name**: Enter a name for your environment. For example: usdev1

2. Ensure that the **New Installation** option is selected. Then enter values for the following:
   - **Database**: Select the type of environment you want to create, either **Vision Demo Install** or **Fresh Install**.
   - **EBS Version**: Select the Oracle E-Business Suite version for your environment.
   - **DB Version**: Select the database version for your environment. The available database versions depend on the Oracle E-Business Suite version you selected.

3. Optionally select your operating system time zone. This is the operating system time zone for your application and database tier nodes. For more information on time zone support, see: Time Zone Support in Oracle E-Business Suite Cloud Manager, page B-1.
   - The default value for a Fresh Install implementation is 'UTC'. For a Fresh Install instance, leave the **Bypass Server Timezone Profile Validation** box unchecked.
   - The default value for a new implementation for Vision Demo Install is 'America/Chicago', the time zone for the Vision Demo instance. For a Vision Demo Install instance, Oracle E-Business Suite Cloud Manager will validate your selection for the server time zone, unless you check the box **Bypass Server Timezone Profile Validation**.
Note: If you are provisioning on an Exadata Cloud Service instance, when the Bypass Server Timezone Profile Validation box is unchecked, the system will set the time zone variable (TZ) in the database environment file and the SRVCTL utility will use this time zone value.

4. Optionally enter tagging information in the Tags region.

   - **Tag Namespace**: Select a predefined tag namespace or select None (add a free-form tag).

   - **Tag Key**: Enter the name you use to refer to the tag.

   - **Value**: Enter the value for the tag key.

5. Click Next. Now continue to the section Enter Database Information, page 9-15 for the next steps.

### Enter Installation Details for an Environment from a Backup:

1. Enter details for your new environment:

   - **Environment Name**: Enter a name for your environment. For example: usdev1

   - **Network Profile**: Select the network profile that contains the network resources you want to use to provision your environment. For example: DEFAULT_PROFILE_ADVANCED

2. In the Installation Type region, ensure that the **Provision from Object Storage Backup** option is selected. Then enter values for the following:

   - **Backup Bucket**: Select the backup from which you want to provision the environment. If you navigated to Advanced Provisioning from the Backups page or from the Backups region in an environment details page, then the backup you chose there is selected by default.

   - **Backup Encryption Password**: Enter the encryption password that was specified for the backup when the backup was created.

   - **Backup Apps Password**: Enter the password for the Oracle E-Business Suite APPS schema for the source environment.

   - **New WebLogic Server Password**: (Conditionally Required) Enter the password that you want to set for the Oracle WebLogic Server administration user on the target environment. This field appears only if you selected a backup created from a source environment on Oracle E-Business Suite Release 12.2. Note that
this password should comply with the Weblogic Server Policy that was present on the source instance at the time the backup was taken. If the default policy was set for the source instance, then provide a password complying with the default policy. If a custom policy was set for the source instance, then provide a password complying with the custom policy.

- **Source Wallet Password**: (Conditionally Required) If you selected a backup created from a TDE-enabled source environment, enter the source wallet password.

3. Optionally select your operating system time zone. This is the operating system time zone for your application and database tier nodes. For more information on time zone support, see: Time Zone Support in Oracle E-Business Suite Cloud Manager, page B-1.

Oracle E-Business Suite Cloud Manager will validate your selection for the server time zone, unless you check the box **Bypass Server Timezone Profile Validation**.

**Warning**: If you choose to override the time zone defined in the backup environment, then the operating system for the new environment will be configured to use the selected time zone. After you provision your environment, and prior to starting any database and application tier services, you must set the $TZ$ environment variable to match the Server Timezone profile option. Failure to do so could lead to data corruption. See: Time Zone Support [https://docs.oracle.com/cd/E26401_01/doc.122/e22953/T174296T575363.htm] in the Oracle E-Business Suite Setup Guide.

4. Optionally enter tagging information in the Tags region.
   - **Tag Namespace**: Select a predefined tag namespace or select **None (add a free-form tag)**.
   - **Tag Key**: Enter the name you use to refer to the tag.
   - **Value**: Enter the value for the tag key.

5. Click **Next**. Oracle E-Business Suite Cloud Manager will validate all passwords. The WebLogic Server password will be validated based on the default/custom policy set on the source instance of the backup.

If there are any validation issues, errors will be displayed. Correct the passwords and click **Next** to proceed.

**Enter Database Information**:
1.
Select the Cloud Database Service option for your environment, either Compute, Virtual Machine DB System, or Exadata DB System.

2. If you chose Compute for the Cloud Database Service, enter the following:
   
   - **DB SID**: Enter the database SID. For example: `demodb`
   - **Logical Hostname**: Provide the logical hostname that will be used as part of the Oracle E-Business Suite configuration. Note that this is not the physical hostname.
   - **Logical Domain**: Provide the logical domain that will be used as part of the Oracle E-Business Suite configuration. Note that this is not the physical domain.
   - **PDB Name**: If the database version is 19c, enter the pluggable database (PDB) name.
   - **VM Shape**: Select a shape that is available in the OCI region. Ensure that you have checked the quota for the shape in advance. For example: `VM Standard2.1 (1 OCPU, 15GB RAM)`
   - **Enable TDE**: Select this option if you want to enable Transparent Database Encryption (TDE) for a new environment on Compute, or for an environment on Compute that is created from a backup of a non-TDE source environment. If you provision an environment on Compute from a backup of a TDE-enabled source environment, then TDE is automatically enabled. Note that to run a TDE-enabled database on Compute, you must have or acquire the Advanced Security Option (ASO).
   - **Admin Password**: Enter the admin password for the database. This password is used for the SYS user as well, and must not contain the username 'SYS'. If TDE is enabled for the environment, then this password is also used as the TDE wallet password. The password must be 9 to 30 characters and contain at least two uppercase, two lowercase, two special, and two numeric characters. The special characters must be underscores (_), number signs (#), or hyphens (-). Re-enter the password in the next field to confirm it.
   - **Fault Domain Selection**: Select **Automatic** or **Manual**. If you choose Manual, you are prompted to select fault domains. Refer to Fault Domains [https://docs.cloud.oracle.com/en-us/iaas/Content/General/Concepts/regions.htm#fault] for more information.
   - **(Advanced Options) RMAN_CHANNEL_COUNT**: Specify the number of Recovery Manager (RMAN) staging channels to allocate for restoring from the backup. The default value used by RMAN is 100% of the number of OCPUs. The minimum value is one channel. The maximum value is 255 irrespective of shape.
3. If you chose Virtual Machine DB System for the Cloud Database Service, enter the following:

- **DB Name**: Enter the database name. For example: `vmdb1`

- **DB Patch Level**: Select a certified database patch level from the options provided, identified by the database version and the release year, month, and day.

- **Shape**: Select the shape. Note that for an Oracle RAC environment, you must select a shape that supports it. For example: **VM Standard2.2 (2 OCPU, 30GB RAM)**

- **Node Count**: Select 1 for a 1-Node VM DB System (Single Instance), or select 2 for a 2-Node VM DB System (Oracle RAC).

- **DB Software Edition**: Select the database software edition. If the Node Count is 2, then the only choice is **Enterprise Edition Extreme Performance**. If the Node Count is 1, then you can choose either **Enterprise Edition**, **Enterprise Edition High Performance**, or **Enterprise Edition Extreme Performance**.

- **Cluster Name**: If the Node Count is 2, then this field appears and you can optionally enter a cluster name. For example: `demo-1`

- **License Type**: Select **License Included** if you want to obtain a new license or **Bring Your Own License (BYOL)** if you want to use a license you already own.

- **PDB Name**: If the database version is either 12.1.0.2 or 19c, enter the pluggable database (PDB) name. For example: `vmdbpdb`

- **Admin Password**: Enter the admin password for the database. This password is used for the SYS user as well, and must not contain the username 'SYS'. This password is also used as the TDE wallet password. The password must be 9 to 30 characters and contain at least two uppercase, two lowercase, two special, and two numeric characters. The special characters must be underscores (_), number signs (#), or hyphens (-). Re-enter the password in the next field to confirm it.

- **Fault Domain Selection**: Select **Automatic** or **Manual**. If you choose Manual, you are prompted to select fault domains. Refer to Fault Domains [https://docs.cloud.oracle.com/en-us/iaas/Content/General/Concepts/regions.htm#fault] for more information.

- **(Advanced Options) RMAN_CHANNEL_COUNT**: Specify the number of Recovery Manager (RMAN) staging channels to allocate for restoring from the backup. The default value used by RMAN is 100% of the number of OCPUs. The minimum value is one channel. The maximum value is 255 irrespective of
4. If you selected Exadata DB System for the Cloud Database Service, enter the following:

- **Infrastructure Name**: Select the Exadata infrastructure name. The infrastructure resource is used to manage the hardware configuration and maintenance schedule at the infrastructure level. For information on using the infrastructure resource, see: The New Exadata Cloud Service Resource Model [https://docs.oracle.com/en-us/iaas/Content/Database/Concepts/exaflexsystem.htm#exaflexsystem_topic-resource_model].

- **Cluster Name**: Select the name of the VM Cluster resource. The VM cluster is a child resource of the infrastructure resource, providing a link between your Exadata cloud infrastructure resource and Oracle Database. For information on using the cluster resource, see: The New Exadata Cloud Service Resource Model [https://docs.oracle.com/en-us/iaas/Content/Database/Concepts/exaflexsystem.htm#exaflexsystem_topic-resource_model].

- **DB System Name**: Select the database system name. For example: demoexaxxadb1.

  **Note**: This field displays only Exadata Cloud Service instances with a status of **ACTIVE**. If an action is currently being performed on an Exadata Cloud Service instance that causes the system to have a status of **UPDATING**, then that system will temporarily be omitted from the list of values in this field. For example, if a user is adding SSH keys, then the system will have a status of **UPDATING** for a few minutes. Consequently, if you do not see the system you want to use, wait for the action being performed on the system to complete and then return to this page to select the system.

- **DB Name**: Enter the database name. For example: exadb

- **PDB Name**: If the database version is either 12.1.0.2 or 19c, enter the pluggable database (PDB) name. For example: exapdb

- **DB Patch Level**: Select the database patch level, identified by the database version and the release year, month, and day.

- **Admin Password**: Enter the admin password for the database. This password is used for the SYS user as well, and must not contain the username 'SYS'. This password is also used as the TDE wallet password. The password must be 9 to
30 characters and contain at least two uppercase, two lowercase, two special, and two numeric characters. The special characters must be underscores (_), number signs (#), or hyphens (-). Re-enter the password in the next field to confirm it.

- **(Advanced Options) RMAN_CHANNEL_COUNT**: Specify the number of Recovery Manager (RMAN) staging channels to allocate for restoring from the backup. The default value used by RMAN is 16. The minimum value is one channel. The maximum value is 255 irrespective of shape.

5. Click Next.

**Enter Application Tier Information:**


   Note that you can have multiple zones across subnets. You can configure your environment such that your functional redirection per zone is in accordance with functional affinity.

   Also, you can have a load balancer shared between multiple zones of the same type. This configuration allows for two separate URLs to resolve to the same IP address and the shared load balancer will target one backend set or another.

   Note too that you have flexibility in your configuration. One zone, Zone A, can have one load balancer assigned to it, while another two zones, Zone B and Zone C, can have a second load balancer assigned to them.

   Define your internal zone first.

   Enter values for the following properties:

   - **Name**
   - **Type**

2. In the Web Entry Point region, enter values for the following properties:

   - **Web Entry Type**: Choose one of the following: **New Load Balancer (LBaaS)**, **Manually Configured Load Balancer** to select a manually deployed existing load balancer, or **Application Tier Node** to choose the primary application tier as the entry point.

   - **Load Balancer Shape**: If you are using LBaaS, select the load balancer shape. For example: **100Mbps**

   - **Protocol**: Select the protocol for access to the environment, either **http** or **https**.
• **Hostname**: Enter the hostname for your web entry point. For example: myhost

• **Domain**: Enter the domain for your web entry point. For example: example.com

• **Port**: Select the port for your web entry point. If there is no load balancer, then the port is automatically populated depending on the protocol: 8000 for http and 4443 for https. Otherwise, select the appropriate port for use with your load balancer, such as 80 for http or 443 for https. Note that to allow access to the Oracle E-Business Suite login URL, your network administrator must define an ingress rule in the load balancer security list. See Create Network Resources For Deploying Oracle E-Business Suite Instances, page 3-9.

3. For Storage, choose the **File System Type**: Non-Shared or Shared.

   If you choose Shared, then the storage is shared across all nodes in your network. You must enter a value for the Block Volume Storage field for the first node under Application Tier Nodes. This storage is then shared across all nodes, so you do not enter in storage values for your subsequent nodes. In addition, after you save your first zone with Shared storage, any subsequent zones will also be defined with Shared storage automatically.

   **Important**: You must ensure you specify enough storage for your nodes. Refer to Oracle E-Business Suite Installation Guide: Using Rapid Install [https://docs.oracle.com/cd/E26401_01/doc.122/e22950/toc.htm] for guidelines on space usage.

   If you choose Non-Shared, you must specify a value for the Block Volume Storage field for every node in the Application Tier Nodes field.

4. In the Logical Host region, enter values for the following properties:

   • **Logical Host Option**: Choose Automatic or Manual.

   • **Logical Hostname Prefix**: If you chose Automatic, enter your desired hostname prefix.

     You do not need to enter this if you chose Manual for your logical host option, but you will be prompted for the Logical Hostname for your nodes in the Application Tier Nodes region.

   • **Logical Domain**: Enter the logical domain.

5. In the **Application Tier Nodes** region, enter properties for each node.

   Note that you can define a specific shape for each application tier node.

   • **Logical Hostname**
• **Logical FQDN**

• **Shape**: Select the shape. For example: **VM.Standard2.1** - (1 OCPU, 15 GB RAM)

• **Block Volume Storage**

• **Fault Domain**: Select the fault domain. Refer to [Fault Domains](https://docs.cloud.oracle.com/en-us/iaas/Content/General/Concepts/regions.htm#fault) for more information.

6. Click **Save Zone** to save your zone definition.

7. Define additional zones using the **Add Zone** button.

8. When you have completed adding your zones, click **Next**.

**Specify Your Extensibility Options:**
You can optionally extend the provisioning activity to meet your own requirements. By default, Oracle E-Business Suite Cloud Manager follows a standard activity plan for provisioning. However, Oracle E-Business Suite Cloud Manager administrators can also create extended activity plans that include additional tasks as part of the provisioning activity. In this case you can select the appropriate extended activity plan for Oracle E-Business Suite Cloud Manager to follow when provisioning your environment. If you select an extended activity plan, you may need to enter values for input parameters required by the additional tasks in that plan.

**Additional Information**: For more information on using the Extensibility Framework to extend activity plans, see [Set Up the Extensibility Framework](#), page 8-8.

Additionally, whether you are using the standard provisioning activity plan or an extended activity plan, you can choose to have Oracle E-Business Suite Cloud Manager pause at specified points during the provisioning activity. For example, if you want to perform your own validations after a particular phase before allowing Oracle E-Business Suite Cloud Manager to proceed to the next phase, you can add a pause at that point. You can then resume the provisioning activity when you are ready to proceed. See Monitor Activity Status, page 12-1.

**Define Your Activity Plan**

1. Optionally select an extended activity plan for provisioning your environment in the **Activity Plan** field.

2. In the Task Parameters tab, specify any parameter values required for the additional tasks in the plan. Some parameters may include default values, which
Define Your Activity Plan Details
3. Click the Activity Plan Details tab. This tab displays a list of the phases in the activity plan and the tasks within each phase.

4. To specify that Oracle E-Business Suite Cloud Manager should pause its processing before a particular phase, click the Actions icon next to that phase, and then select Add Pause.

   Note: Pauses occur before the phase at which they are defined.

5. Click Next.

Enter SSH Keys:
Optionally upload SSH keys for users.

   Note: You cannot add keys after the provisioning process is completed.

   Note: If you selected Exadata DB System as your Cloud Database Service, then you can add keys to the application tier only.

1. Click Add Key.

2. Specify the tiers for the SSH key. Choose All Tiers, Application Tier, or Database Tier.

3. Specify the pertinent OS User type. Choose All Users, Operating System Administrator, or Application Administrator.

4. Upload the SSH key file. The file name will default in.

5. The system will validate the SSH key. Click Next to continue.

Review Your Advanced Provisioning Details:
1. Review the installation details, including:
   - Installation details, including environment name, installation type, network profile, and operating system time zone.
   - Database details, including database service type, database name, and pluggable database name. For Exadata Cloud Services, the cluster name is
Provision an Oracle E-Business Suite Instance

- Application tier details, including web entry details and information on zones.
- Activity plan details.
- SSH Key information.

2. To provision your environment, click Submit.

3. You can check the status of the activity to provision the environment in the Activities page.

Known Issues for Advanced Provisioning:

Workaround for Oracle Database 19c Restore Failure

When using the Oracle E-Business Suite Cloud Manager Advanced Provisioning to provision from a backup containing Oracle Database 19c, whether that backup is part of a lift and shift from on-premises or the result of a Create Backup operation in OCI, you may encounter the error "ORA-65174: invalid or conflicting name in service <service name> found in the pluggable database."

You can fix this issue by first deleting the conflicting service from the source environment. Here is the complete list of steps to work around the issue:

1. On the database tier of the source environment, list the services registered with the database.

   ```
   $ source <cdb env file>
   $ lsnrctl status <LISTENER_NAME>
   $ sqlplus "/as sysdba"
   $ select NAME,NETWORK_NAME,CON_NAME,CREATION_DATE from v$active_services
   ```

2. Next, connect to the CDB:

   ```
   $ cd <19c home>$ source <cdb_sid>_<hostname>.env
   ```
   and run the query shown to list all services in the database:

   ```
   $ select name,enabled,creation_date,pdb from cdb_services;
   ```

3. Ensure the conflicting service name is not in the list of lsnrctl output and v$active_services. Perform this step to ensure that you are not deleting active services on the source. If the service does appear in the list, then do not proceed with the next steps; instead, contact your Oracle Support representative.

4. Connect to the container and delete the service causing the conflict.
$ cd <19chome>
$ source <cdb_sid>_<hostname>.env
$ sqlplus "/ as sysdba"
$ alter session set container="<PDB NAME>";
$ exec DBMS_SERVICE.DELETE_SERVICE('<CONFLICTING SERVICE NAME>');

5. Repeat the backup and restore operation that originally failed:
   1. Recreate the backup by running the Oracle E-Business Suite Cloud Backup Module or running the Oracle E-Business Suite Cloud Manager Create Backup feature.
   2. Use Oracle E-Business Suite Cloud Manager Advanced Provisioning to provision your new environment.

Additional Patches for the Internal Concurrent Manager
You might see issues regarding Internal Concurrent Manager (ICM) startup failure after provisioning in 12.1.3 environments. You should apply the following patches and restart Concurrent Manager Services:

- Patch 31081204:R12.TXK.B [https://updates.oracle.com/download/31081204.html]
- Patch 27091621:R12.FND.B [https://updates.oracle.com/download/27091621.html]

What's Next
After the environment is successfully provisioned, perform any necessary post-provisioning steps and access your environment following the instructions provided in Perform Post-Provisioning and Post-Cloning Tasks, page 9-24.

Perform Post-Provisioning and Post-Cloning Tasks
After you provision or clone an environment, you must perform some tasks to configure access and secure the environment. You may also need to perform other tasks depending on your Oracle E-Business Suite release, Oracle Database release, and the cloud service on which the database tier resides. These tasks apply for new environments created through either One-Click Provisioning or Advanced Provisioning, for environments created from a backup through Advanced Provisioning, and for environments created through cloning in Oracle E-Business Suite Cloud Manager.

**Note:** You can optionally use the Extensibility Framework to automate some of these tasks by adding them to custom provisioning and processing plans. See Set Up the Extensibility Framework, page 8-8.

- Implement Workaround for Oracle Databases on Exadata Cloud Services
• Implement Workaround for Oracle Databases on VM DB Systems (Conditionally Required), page 9-26

• Update Profile Options (Conditionally Required), page 9-27

• Update Web Entry Host and Domain Name (Conditionally Required), page 9-27

• Upload TLS Certificate (Conditionally Required), page 9-29

• Manually Enable TLS When Using Load Balancer as a Service (LBaaS) as an Alternate Termination Point (Conditionally Required), page 9-32

• Enable TLS for Manually Configured Load Balancer (Conditionally Required), page 9-35

• Manually Enable TLS When Using Oracle HTTP Server on the Application Tier Node as the Web Entry Point (Conditionally Required), page 9-36

• Manually Configure Firewall When Using Oracle HTTP Server or an On-Premises Load Balancer as the Web Entry Point (Conditionally Required), page 9-37

• Implement Workaround for Oracle Databases on 2-Node VM DB System (Conditionally Required), page 9-38

• Configure Security and Firewall Rules for Secure Access to the Fusion Middleware Control and WebLogic Server Administration Console (Conditionally Required), page 9-39

• Enable and Set Oracle E-Business Account Passwords (Conditionally Required), page 9-40

• Apply Oracle E-Business Suite and Database Patches (Conditionally Required), page 9-42

• Configure Enterprise Command Centers after One-Click Provisioning (Conditionally Required), page 9-43

Implement Workaround for Oracle Databases on Exadata Cloud Services (Conditionally Required):
This workaround resolves a known issue that impacts SQL*Net configuration files on secondary nodes. The steps in this section are required only for a provisioned environment with the database on an Exadata Cloud Service instance with Oracle Database Release 12.1.0.2.

1. Identify the private IP address of each secondary Exadata Cloud Service node from
the Exadata Cloud Service console.

2. Perform steps 3-8 for all secondary Exadata Cloud Service nodes.

3. While logged in to the Oracle E-Business Suite Cloud Manager VM as the oracle user, use ssh to connect to the secondary Exadata Cloud Service node.

4. Obtain the ORACLE_HOME details from the oratab file:
   $ cat /etc/oratab

5. Source the environment file:
   $ cd <ORACLE_HOME>
   $ source <SID>_<HOSTNAME>.env

6. Navigate to the $ORACLE_HOME/network/admin directory:
   $ cd $ORACLE_HOME/network/admin

7. Using a text editor such as vi, edit the sqlnet.ora file. First, delete all existing lines from the sqlnet.ora file. Then add the following line:
   IFILE=<ORACLE_HOME>/network/admin/<SID>_<HOSTNAME>/sqlnet.ora

8. Create a listener.ora file with a text editor such as vi, and add the following line:
   IFILE=<ORACLE_HOME>/network/admin/<SID>_<HOSTNAME>/listener.ora

Implement Workaround for Oracle Databases on VM DB Systems (Conditionally Required):
This workaround is required only for a provisioned environment with the database on a VM DB System.

1. On the VMDB node, run the following in order to obtain the database unique_name value:
   $ source <cdb>.env
   $ sqlplus "/as sysdba"
   SQL> show parameter unique;
   SQL> exit;
   The output displayed after entering the show parameter unique command is the unique_name value you should record for use in the next step.

2. Using the unique_name from the previous step, update the <pdb>_ebs_patch service in the spfile as shown:
   $ source <cdb>.env
   $ sqlplus "/as sysdba"
   SQL> alter system set service_names='<unique_name>', '<PDB_SID>_ebs_patch' scope=both;
   SQL> exit;
Update Profile Options (Conditionally Required):

If you provision an environment as part of a lift and shift process, then profile options, which impact the way your application looks and behaves, are carried over from the on-premises Oracle E-Business Suite environment to Oracle Cloud Infrastructure.

Profile options are handled in various ways by the automated lift and shift process through the Oracle E-Business Suite Cloud Backup Module and Oracle E-Business Suite Cloud Manager.

- Oracle E-Business Suite Cloud Manager resets the site level and server level values of some instance-specific profile options containing a web entry point to match the Oracle Cloud Infrastructure deployment. For example, the APPS_FRAMEWORK_AGENT profile option value is set to the web entry point that you chose in the Oracle E-Business Suite Cloud Manager Advanced Provisioning UI.

- Other profile option settings, including those at the user level and responsibility level, are preserved at their original on-premises values. The Oracle E-Business Suite Cloud Backup Module generates a report of the existing user level values for some commonly used profile options containing URLs that you must manually reset. This report is located in the /u01/install/APPS/apps/appsinfo/appsinfo.txt file on the target system. The report includes the following profile options: APPS_WEB_AGENT, APPS_SERVLET_AGENT, APPS_JSP_AGENT, APPS_FRAMEWORK_AGENT, ICX_Forms_Launcher, ICX_Discoverer_Launcher, HELP_WEB_AGENT, and ICX_Discoverer_Viewer_Launcher.

Review all the profile options in your newly provisioned environment and modify them as required to reflect your Oracle Cloud Infrastructure configuration.

For more information about the use of profile options in Oracle E-Business Suite, see User Profiles and Profile Options in Oracle Application Object Library [https://docs.oracle.com/cd/E26401_01/doc.122/e22953/T174296T202994.htm], Oracle E-Business Suite Setup Guide.

Update Web Entry Host and Domain Name (Conditionally Required):

When you provision an Oracle E-Business Suite environment with One-Click Provisioning, the environment is automatically configured to use the application tier node as the web entry point, with Transport Layer Security (TLS) enabled for inbound HTTP traffic. The login URL is automatically generated in the format <instance name>.example.com, and the listener for the Oracle HTTP Server for the application tier is associated by default with a self-signed TLS certificate generated by Oracle E-Business Suite Cloud Manager.

With the simplified preset topology used in One-Click Provisioning, you cannot specify a different host and domain for the web entry point during provisioning. However, you can use the steps in this section to update the host and domain for the web entry point
after provisioning is complete.

Note that if you plan to replace the self-signed certificate generated by Oracle E-Business Suite Cloud Manager with a certificate issued by a certificate authority (CA), then you must follow the steps in this section to change the domain name before you request the certificate, because you cannot obtain a certificate from a CA for the demonstration example.com domain.

If you provisioned an environment with Advanced Provisioning, you can also optionally use the steps in this section to update the host and domain for the web entry point if you need to change these values from those you initially specified during provisioning.

To update the host and domain, perform the following steps.

1. Using a text editor such as vi, update the following variables in the context file on all application tier nodes.
   - s_webentryhost - Set the value for this variable to the new web entry host you want to use.
   - s_webentrydomain - Set the value for this variable to the new web entry domain you want to use.
   - s_external_url - Update the value for this variable to use the new web entry host and domain that you specified in the s_webentryhost and s_webentrydomain variables. Do not change any other parts of the URL value. The full new value should be in the following form:
     
     ![https://docs.oracle.com/cd/E26401_01/doc.122/e22953/T174296T589913.htm#6237534](https://docs.oracle.com/cd/E26401_01/doc.122/e22953/T174296T589913.htm#6237534), Oracle E-Business Suite Setup Guide.
   - s_login_page - Update the value for this variable to use the new web entry host and domain that you specified in the s_webentryhost and s_webentrydomain variables. Do not change any other parts of the URL value. The full new value should be in the following form:

2. If you are finished updating the context file, then you should now run AutoConfig on all application tier nodes. See Using AutoConfig Tools for System Configuration [https://docs.oracle.com/cd/E26401_01/doc.122/e22953/T174296T589913.htm#6237534], Oracle E-Business Suite Setup Guide.

   **Note:** If you plan to make additional changes in the context file in order to configure TLS, according to the instructions in later sections in this chapter, then you can defer running AutoConfig until you are instructed to do so in those sections. In this case, you can skip this step and the following step. Instead, proceed to the
3. After running AutoConfig, on all application tier nodes, stop and restart all services by running the adstpall.sh script and the adstrtal.sh script.

Upload TLS Certificate (Conditionally Required):
Perform the steps in this section to upload a certificate if you enabled or plan to enable Transport Layer Security (TLS) for your environment.

TLS is enabled during provisioning if you used One-Click Provisioning, which automatically configures the application tier node as the web entry point with the https protocol, or if you used Advanced Provisioning and you chose either New Load Balancer (LBaaS) or Application Tier Node as the web entry type and you chose the https protocol. In this case Oracle E-Business Suite Cloud Manager configures your environment to encrypt inbound HTTP traffic with TLS. The initial configuration uses a self-signed certificate generated by Oracle E-Business Suite Cloud Manager. It is mandatory that you replace this certificate with a TLS certificate issued by a certificate authority (CA) or your own self-signed certificate generated using the web entry host for your Oracle E-Business Suite instance.

If you did not enable TLS during provisioning, you can enable it manually as a post-provisioning step. TLS is not enabled during provisioning if you used Advanced Provisioning and you chose either New Load Balancer (LBaaS) or Application Tier Node as the web entry type and you chose the http protocol. As a prerequisite for enabling TLS, you must obtain and upload a TLS certificate issued by a certificate authority (CA) or generate and upload your own self-signed certificate using the web entry host for your Oracle E-Business Suite instance.

Additionally, if you are using an on-premises load balancer and you chose Manually Configured Load Balancer as the web entry type, you can enable TLS manually as a post-provisioning step. To do so, you must upload a TLS certificate as required for your load balancer.

New Load Balancer (LBaaS)
If you configured TLS using LBaaS during provisioning or will manually perform this configuration, perform the following steps to upload your certificate.

1. Obtain a TLS certificate valid for the name of the web entry host for your Oracle E-Business Suite instance, or generate a self-signed certificate. The web entry host name is formed by combining the values of the application tier context variables s_webentryhost and s_webentrydomain.

Oracle Cloud Infrastructure provides a public IP address but does not provide a public host name, so you should ensure that appropriate DNS entries are present to resolve the web entry host name to the public IP address.

If you changed the web entry host and domain for your environment in the next task, Upload TLS Certificate, page 9-29.
previous section, ensure that you use the new host, domain, and URL when you request or generate a certificate.

2. If you are using a self-signed certificate that you generated yourself, ensure that you import the certificate to the JDK trust stores.
   • For Release 12.2, see Section 5.3: Configure Loopback and Outbound Connections, Step 3, in My Oracle Support Knowledge Document 1367293.1, Enabling TLS in Oracle E-Business Suite Release 12.2 [https://support.oracle.com/rs?type=doc&id=1367293.1].
   • For Release 12.1, see Section 5.3: Configure Loopback and Outbound Connections, Step 3, in My Oracle Support Knowledge Document 376700.1, Enabling TLS in Oracle E-Business Suite Release 12.1 [https://support.oracle.com/rs?type=doc&id=376700.1].

3. Log in to the Oracle Cloud Infrastructure console. From the navigation menu, select Networking > Load Balancers, and then select the load balancer you want to configure.

4. Add your certificate bundle to the load balancer. See To upload an SSL certificate bundle to your load balancing system [https://docs.cloud.oracle.com/iaas/Content/Balance/Tasks/managingcertificates.htm#add] in the Oracle Cloud Infrastructure Services documentation. If you have multiple certificates that form a single certification chain, such as one or more intermediate certificates together with a root certificate, then you must include all relevant certificates in one file before you upload them to the system. See "Uploading Certificate Chains" in the section Working with SSL Certificates [https://docs.cloud.oracle.com/iaas/Content/Balance/Tasks/managingcertificates.htm#working] in the Oracle Cloud Infrastructure Services documentation.

5. If you chose the https protocol for LBaaS during Advanced Provisioning, and the load balancer listener is using the self-signed certificate generated by Oracle E-Business Suite Cloud Manager, then you should now update the certificate. To do so, on the Load Balancer page, click the Listeners link in the Resources menu. Click the Actions icon (three dots) for your listener, and select Edit from the context menu. In the Edit Listener pop-up, select the certificate bundle that you added in step 4 in the Certificate Name field. Then click Save Changes, and wait for the listener to be updated. See To edit a listener [https://docs.cloud.oracle.com/iaas/Content/Balance/Tasks/managinglisteners.htm#edit] in the Oracle Cloud Infrastructure Services documentation.

Manually Configured Load Balancer
If you are using an on-premises load balancer, follow the instructions from your vendor to create and upload a certificate.
**Application Tier Node**

If you configured TLS at the application tier layer during provisioning, perform the following steps to upload your certificate. TLS is configured at the application tier layer in the following cases:

- You used One-Click Provisioning to deploy your environment, which automatically configures the application tier node as the web entry point with the **https** protocol.

- You used Advanced Provisioning to deploy your environment and you chose **Application Tier Node** as the web entry type with the **https** protocol.

**Note:** If you plan to configure TLS at the application tier layer manually, you will perform the certificate steps as part of that configuration instead in the task Manually Enable TLS When Using Oracle HTTP Server on the Application Tier Node as the Web Entry Point, page 9-36.

1. Obtain a TLS certificate valid for the name of the web entry host for your Oracle E-Business Suite instance, or generate a self-signed certificate. The web entry host name is formed by combining the values of the application tier context variables `s_webentryhost` and `s_webentrydomain`.

Oracle Cloud Infrastructure provides a public IP address but does not provide a public host name, so you should ensure that appropriate DNS entries are present to resolve the web entry host name to the public IP address.

If you changed the web entry host and domain for your environment in the previous section, ensure that you use the new host, domain, and URL when you request or generate a certificate. Note that if you deployed your environment with One-Click Provisioning and you plan to request a certificate from a CA, you must ensure that you have changed the domain name from the default `example.com` domain before you request the certificate, because you cannot obtain a certificate from a CA for the demonstration `example.com` domain.

2. If you are using a self-signed certificate that you generated yourself, ensure that you import the certificate to the JDK trust stores.


3. Upload your certificate to replace the initial certificate generated by Oracle E-Business Suite Cloud Manager.

   • For Release 12.2, see Section 8: Renewing Expired Certificates in My Oracle Support Knowledge Document 1367293.1, Enabling TLS in Oracle E-Business Suite Release 12.2 [https://support.oracle.com/rs?type=doc&id=1367293.1].

   • For Release 12.1, see Section 8: Renew Revoked or Expired Certificates in My Oracle Support Knowledge Document 376700.1, Enabling TLS in Oracle E-Business Suite Release 12.1 [https://support.oracle.com/rs?type=doc&id=376700.1].

**Manually Enable TLS When Using Load Balancer as a Service (LBaaS) as an Alternate Termination Point (Conditionally Required):**

We highly recommend that you configure your environment to encrypt inbound HTTP traffic with Transport Layer Security (TLS). The steps in this section are applicable in either of the following cases:

   • You used Advanced Provisioning to deploy an environment using Load Balancer as a Service (LBaaS) as the web entry point and you did not enable Transport Layer Security (TLS) during provisioning. That is, you chose **New Load Balancer (LBaaS)** as the web entry type and you chose the **http** protocol for the web entry point.

   • You manually configured LBaaS but did not yet configure TLS.

We highly recommend that you perform the steps in this section to offload the encryption to the LBaaS and configure Oracle E-Business Suite to use HTTPS (HTTP over TLS).

Note that the configuration described here terminates TLS at the load balancer; that is, TLS is used only for communication between the client and the load balancer. Communication between the load balancer and the Oracle E-Business Suite instance does not use TLS. See "Terminating SSL at the Load Balancer" in the section Configuring SSL Handling [https://docs.cloud.oracle.com/en-us/iaas/Content/Balance/Tasks/managingcertificates.htm#configuringSSLhandling] in the Oracle Cloud Infrastructure Services documentation.

If you used Advanced Provisioning and chose to deploy LBaaS with the **https** protocol, you can also optionally perform the relevant steps in this section to update the port for the load balancer listener if you need to change this value from the port you initially specified during provisioning.

To manually enable TLS in an environment that uses LBaaS as an alternate termination point, perform the following steps:

1. Ensure that you have obtained and uploaded a certificate according to the steps in Upload TLS Certificate, page 9-29.
2. Log in to the Oracle Cloud Infrastructure console. From the navigation menu, select **Networking > Load Balancers**, and then select the load balancer you want to configure.

3. On the Load Balancer page, click the **Listeners** link in the **Resources** menu. Click the Actions icon (three dots) for your listener, and select **Edit** from the context menu.

4. Edit the load balancer listener to enable TLS. Enter the port to use for secure communication, such as 443. Then check the **Use SSL** option and specify the certificate name. See To edit a listener [https://docs.cloud.oracle.com/iaas/Content/Balance/Tasks/managinglisteners.htm#edit] in the Oracle Cloud Infrastructure Services documentation.

5. Using a text editor such as vi, verify or update the following variables in the context file on all application tier nodes for your environment.

   - **s_webentryurlprotocol** - Set the value for this variable to https.
   - **s_url_protocol** - Set the value for this variable to http.
   - **s_enable_sslterminator** - Remove any value set for this variable; that is, the value should be left blank.
   - **s_active_webport** - Set the value for this variable to the port you specified for the load balancer listener, such as 443.
   - **s_external_url** - Update the value for this variable to use the https protocol and the port you specified for the load balancer listener. The full new value should be in the following form:

     ```
     https ://<web_entry_host>.<web_entry_domain>: <new_load_balancer_listener_port>
     ```

     If you are using the default HTTPS port 443, then you should omit the colon separator and the port from this URL. That is, if you are using port 443, then the value should be in the following form:

     ```
     https ://<web_entry_host>.<web_entry_domain>
     ```

   - **s_login_page** - Update the value for this variable to use the https protocol and the port you specified for the load balancer listener. The full new value should be in the following form:

     ```
     https ://<web_entry_host>.<web_entry_domain>: <new_load_balancer_listener_port>/OA_HTML/AppsLogin
     ```

     If you are using the default HTTPS port 443, then you should omit the colon separator and the port from this URL. That is, if you are using port 443, then the value should be in the following form:

Additionally, ensure you have set other context file variables as needed for using the load balancer as the TLS termination point.

- For Release 12.2, see the "Changes When Using a TLS Termination Point Other than OHS" table in Section 9: Alternate TLS Termination Point from My Oracle Support Knowledge Document 1367293.1, Enabling TLS in Oracle E-Business Suite Release 12.2 [https://support.oracle.com/rs?type=doc&id=1367293.1].

- For Release 12.1, see the "Changes When Using a TLS Termination Point Other than OHS" table in Section 9: Alternate TLS Termination Point from My Oracle Support Knowledge Document 376700.1, Enabling TLS in Oracle E-Business Suite Release 12.1 [https://support.oracle.com/rs?type=doc&id=376700.1].

If you are running Oracle HTTP Server on a privileged port - that is, a port number below 1024 - then you must perform additional configuration steps. See Running Oracle HTTP Server on a Privileged Port in Managing Configuration of Oracle HTTP Server and Web Application Services in Oracle E-Business Suite Release 12.2 [https://support.oracle.com/rs?type=doc&id=1905593.1], My Oracle Support Knowledge Document 1905593.1. For more information, see Enabling Oracle HTTP Server to Run as Root for Ports Set to Less Than 1024 (UNIX Only) [https://docs.oracle.com/cd/E28280_01/core.1111/e10105/ports.htm#BABHCHGA], Oracle Fusion Middleware Administrator’s Guide and Starting Oracle HTTP Server on a Privileged Port [https://docs.oracle.com/cd/E28280_01/web.1111/e10144/getstart.htm#BEHDHFGE], Oracle Fusion Middleware Administrator’s Guide for Oracle HTTP Server.


7. On all application tier nodes, stop and restart all services by running the adstpall.sh script and the adstrtal.sh script.

8. If necessary, update the security lists for the load balancer subnets by adding a security rule that allows inbound communication on the port you specified for the load balancer listener, from the clients from which you will access the Oracle E-Business Suite URL. See Working with Security Lists [https://docs.cloud.oracle.com/iaas/Content/Network/Concepts/securitylists.htm#working]. This step is required only if you updated the port for the load balancer listener; that is, if you...
chose the http protocol for LBaaS during Advanced Provisioning, or if you chose the https protocol for LBaaS during Advanced Provisioning but used the preceding steps to change the port from the port specified during provisioning.

In the Oracle Cloud Infrastructure console, open the security list for the load balancer and add a new entry under Allow rules for ingress with the following properties:

- **Source CIDR** - The CIDR block for your on-premises network that includes the relevant clients
- **Protocol** - TCP
- **Destination Port Range** - The port you specified for the load balancer secure communication, such as 443

Repeat these steps for each load balancer subnet.

**Enable TLS for Manually Configured Load Balancer (Conditionally Required):**

The steps in this section are applicable if you used Advanced Provisioning to deploy an environment and chose Manually Configured Load Balancer as the web entry type. These steps apply whether you chose http or https as the protocol for the web entry point.

We highly recommend that you perform the steps in this section to perform the necessary encryption. First, encrypt the traffic between the client and the load balancer. Next, encrypt the traffic between the load balancer and the Oracle HTTP Server. After the encryption setup is complete, configure the Oracle E-Business Suite web entry point.

1. Encrypt the traffic from the client to the load balancer by performing the configuration for an alternate TLS termination point for your Oracle E-Business Suite release.
   - For Oracle E-Business Suite Release 12.2, see My Oracle Support Knowledge Document 1367293.1, Enabling TLS in Oracle E-Business Suite Release 12.2 [https://support.oracle.com/rs?type=doc&id=1367293.1], Section 9: Alternate TLS Termination Point > Alternate TLS Termination Point other than OHS.
   - For Oracle E-Business Suite Release 12.1, see My Oracle Support Knowledge Document 376700.1, Enabling TLS in Oracle E-Business Suite Release 12.1 [https://support.oracle.com/rs?type=doc&id=376700.1], Section 9: Alternate TLS Termination Point > Alternate TLS Termination Point other than OHS.

2. Encrypt the traffic between the load balancer and the Oracle HTTP Server.
   - If you have VPN set up between your on-premises network and Oracle Cloud, then you can optionally set up TLS end-to-end, or you can skip this setup and
go to the next step 3.

- If you do not have VPN set up between your on-premises network and Oracle Cloud, then we highly recommend that you set up TLS end-to-end.

To set up TLS end-to-end, perform the appropriate configuration for your Oracle E-Business Suite release.


3. You can now configure access to the Oracle E-Business Suite web entry point. To do so, perform the steps in Manually Configure Firewall When Using Oracle HTTP Server or an On-Premises Load Balancer as the Web Entry Point, page 9-37.

**Manually Enable TLS When Using Oracle HTTP Server on the Application Tier Node as the Web Entry Point (Conditionally Required):**

The steps in this section are applicable if you used Advanced Provisioning to deploy an environment using Oracle HTTP Server as the web entry point, without using a load balancer, and you did not enable Transport Layer Security (TLS) during provisioning. That is, you chose Application Tier Node as the web entry type and you chose the http protocol for the web entry point. In this case we highly recommend that you perform the following steps to encrypt the traffic between the client and the Oracle HTTP Server. After the encryption setup is complete, you must configure the Oracle E-Business Suite web entry point.

1. Prepare the environment by applying the prerequisites for your Oracle E-Business Suite release.


2. Encrypt the traffic from the client to the Oracle HTTP Server by performing the configuration for inbound connections for your Oracle E-Business Suite release.

3. You can now configure access to the Oracle E-Business Suite web entry point. To do so, perform the steps in Manually Configure Firewall When Using Oracle HTTP Server or an On-Premises Load Balancer as the Web Entry Point, page 9-37.

Manually Configure Firewall When Using Oracle HTTP Server or an On-Premises Load Balancer as the Web Entry Point (Conditionally Required):
Perform the steps in this section to configure the required firewall rules if you are using Oracle HTTP Server or an on-premises load balancer as the web entry point. These steps apply if you used one of the following deployment options:
   • You used One-Click Provisioning to deploy your environment, which automatically configures the application tier node as the web entry type.
   • You used Advanced Provisioning to deploy your environment and chose either Application Tier Node or Manually Configured Load Balancer as the web entry type.

We recommend limiting access to a specific CIDR range.

1. First, on all application tier nodes, create firewall rules that allow inbound communication to the web entry port from the clients from which you will access the Oracle E-Business Suite URL. To do so, log on to the Oracle Cloud Infrastructure instance that hosts your Oracle E-Business Suite environment, using SSH. See Connecting to an Instance [https://docs.cloud.oracle.com/iaas/Content/Compute/Tasks/accessinginstance.htm].

Then switch to the root user:

   $ sudo su -

Run the following commands to create the required firewall rules:

```
# firewall-cmd --zone=public --add-rich-rule='rule family=ipv4 source address=<source_CIDR_range> port port=<web_entry_port> protocol=tcp accept' --permanent
# firewall-cmd --zone=public --add-rich-rule='rule family=ipv4 source address=<source_CIDR_range> port port=<web_entry_port> protocol=tcp accept'
```
In these commands, replace `<source_CIDR_range>` with the set of IP addresses from which you will access the Oracle E-Business Suite URL. Replace `<web_entry_port>` with the appropriate port, for example 4443.

Run the following command to restart the firewall to activate the changes:

```
# sudo systemctl restart firewalld
```

Run the following command to verify the current firewall settings:

```
# firewall-cmd --list-all
```

2. Next, update the security list for the subnet that contains the application tier nodes by adding a security rule that allows inbound communication on the web entry port from the clients from which you will access the Oracle E-Business Suite URL. See Working with Security Lists [https://docs.cloud.oracle.com/iaas/Content/Network/Concepts/securitylists.htm#working](https://docs.cloud.oracle.com/iaas/Content/Network/Concepts/securitylists.htm#working).

In the Oracle Cloud Infrastructure console, open the security list for the application tier subnet and add a new entry under **Allow rules for ingress** with the following properties:

- **Source CIDR** - The CIDR block for your on-premises network that includes the relevant clients, as specified in your firewall rules

- **Protocol** - TCP

- **Destination Port Range** - The web entry port, for example 443

**Implement Workaround for Oracle Databases on 2-Node VM DB System (Conditionally Required):**

This workaround resolves a known issue on 2-Node VM DB System. The steps in this section are required only for an environment created using an Oracle E-Business Cloud Manager version prior to 19.3.1.1, with the database on a 2-Node VM DB System with Oracle Database Release 11.2.0.4.

Perform the following steps on the primary node of the VM DB System, except where noted.

1. Get the database unique name using the following command. Run this command as root.

   ```
   $ dbcli list-databases --json|grep databaseUniqueName
   ```

   Copy the output from this command. This value will be referred to in subsequent steps as `<DB_UNIQUE_NAME>`.

2. Remove the database from `srvctl` using the following command. Run this command as the oracle user.

   ```
   $ srvctl stop database -d <dbname>
   $ srvctl remove database -d <dbname>
   ```
3. On both VM DB System nodes, change the db_unique_name value in the database using the following commands.

   $ sqlplus "/ as sysdba"
   $ startup nomount
   $ alter system set db_unique_name='<DB_UNIQUE_NAME>' sid='*' scope=spfile;

4. On both VM DB System nodes, shut down the database using the following command.

   $ shutdown immediate

5. Add the new database unique name to CRS using the following commands.

   $ srvctl add database -d <DB_UNIQUE_NAME> -o /u01/app/oracle/product/11.2.0.4/dbhome_1
   $ srvctl add database -d <DB_UNIQUE_NAME> -i <SID of instance1> -n <Node 1 HOST_NAME>
   $ srvctl add database -d <DB_UNIQUE_NAME> -i <SID of instance2> -n <Node 2 HOST_NAME>

6. On both VM DB System nodes, modify /etc/oratab as follows.

   <DB_UNIQUE_NAME>:/u01/app/oracle/product/11.2.0.4/dbhome_1:N
   # line added by Agent

7. Start the database using the following command.

   $ srvctl start database -d <DB_UNIQUE_NAME>

Configure Security and Firewall Rules for Secure Access to the Fusion Middleware Control and WebLogic Server Administration Console (Conditionally Required):

The steps in this section are required only for Oracle E-Business Suite Release 12.2.

Administration of the Oracle Fusion Middleware 11g components delivered with Oracle E-Business Suite Release 12.2, including Oracle HTTP Server and Oracle WebLogic Server, requires secure access to the WebLogic Server administration ports running on the Oracle E-Business Suite primary application tier node. Ports 7001 and 7002 are the default WebLogic Server administration ports for the dual file system with Oracle E-Business Suite Release 12.2. The examples in this section use these default ports. If you have configured different port numbers, change the port numbers in the instructions to match the port numbers for your environment.

When you create an Oracle E-Business Suite Release 12.2 environment on Oracle Cloud Infrastructure, you should create a security rule and firewall rules that allow inbound communication on the WebLogic Server administration ports on the primary application tier node from the Oracle E-Business Suite Cloud Manager VM. These rules are required as a prerequisite so that a system administrator can securely access the administration ports and the Fusion Middleware Control and WebLogic Server Administration Console. See Access the Fusion Middleware Control and WebLogic Server Administration Console with SSH Port Forwarding for Oracle E-Business Suite on Oracle Cloud Infrastructure, page 10-4.
Perform the following steps to configure the required security rule and firewall rules:

1. Update the security list for the primary application tier node by adding a security rule that allows inbound communication on ports 7001 and 7002 from the Oracle E-Business Suite Cloud Manager VM. See Working with Security Lists [https://docs.cloud.oracle.com/iaas/Content/Network/Concepts/securitylists.htm#working].

In the Oracle Cloud Infrastructure console, open the security list for the Oracle E-Business Suite application tier subnet and add a new entry under Allow rules for ingress with the following properties:

- **Source CIDR** - The CIDR for the Oracle E-Business Suite Cloud Manager VM
- **Protocol** - TCP
- **Destination Port Range** - 7001–7002

2. Create firewall rules on the primary application tier node that allow inbound communication on ports 7001 and 7002 from the subnet that contains the Oracle E-Business Suite Cloud Manager VM. First, log on to the Oracle Cloud Infrastructure instance that hosts your Oracle E-Business Suite environment, using SSH. See Connecting to an Instance [https://docs.cloud.oracle.com/iaas/Content/Compute/Tasks/accessinginstance.htm].

Then switch to the root user:

```
$ sudo su -
```

Run the following commands to create the required firewall rules:

```bash
# firewall-cmd --zone=public --add-rich-rule 'rule family=ipv4
source address=<EBS_Cloud_Admin_Tool_VM_CIDR> port port=7001
protocol=tcp accept' --permanent ;
# firewall-cmd --zone=public --add-rich-rule 'rule family=ipv4
source address=<EBS_Cloud_Admin_Tool_VM_CIDR> port port=7002
protocol=tcp accept' --permanent ;
# firewall-cmd --zone=public --add-rich-rule 'rule family=ipv4
source address=<EBS_Cloud_Admin_Tool_VM_CIDR> port port=7001
protocol=tcp accept';
```

```bash
# firewall-cmd --zone=public --add-rich-rule 'rule family=ipv4
source address=<EBS_Cloud_Admin_Tool_VM_CIDR> port port=7002
protocol=tcp accept';
```

Run the following command to restart the firewall to activate the changes:

```
# sudo systemctld restart firewalld
```

Run the following command to verify the current firewall settings:

```
# firewall-cmd --list-all
```

**Enable and Set Oracle E-Business Account Passwords (Conditionally Required):**

The steps in this section are required only for a new environment or for a cloned environment if the steps were not previously performed on the source environment. To ensure your environment is adequately protected, you must change your Oracle E-
Business Suite account passwords.

If you created your environment from a backup, you can skip this section.

1. Log on to the Oracle Cloud Infrastructure instance that hosts your Oracle E-Business Suite environment.

2. Switch user from the opc user to the oracle user using the following command:
   
   $ sudo su - oracle

3. Set the environment using the appropriate command for your Oracle E-Business Suite release:
   
   - Release 12.2
     
     $ . /u01/install/APPS/EBSapps.env run
   
   - Release 12.1.3
     
     $ . /u01/install/APPS/apps_st/appl/APPS_<CONTEXT_NAME>.env run

4. Download Patch 24831241 to obtain scripts to enable the SYSADMIN user and to enable demo users in a VISION demo environment.

   Download Patch 24831241 [https://updates.oracle.com/download/24831241.html] to the $PATCH_TOP directory and unzip the patch using the following commands:

   $ cd $PATCH_TOP
   $ unzip p24831241_R12_GENERIC.zip -d /u01/install/APPS/scripts/

5. To log in through the web interface, you must initially set a password of your choice for the SYSADMIN user. After the SYSADMIN user is active with the new password, you can create new users or activate existing locked users. To enable the SYSADMIN user, run the following commands:

   $ mkdir -p ~/logs
   $ cd ~/logs
   $ sh /u01/install/APPS/scripts/enableSYSADMIN.sh

   When prompted, enter a new password for the SYSADMIN user.

   The SYSADMIN user can now connect to Oracle E-Business Suite through the web interface and create new users or activate existing locked users.

6. For a VISION demo environment, you can run another script to unlock a set of 36 application users that are typically used when demonstrating Oracle E-Business using the VISION database. Run this script with the same environment as when running the enableSYSADMIN.sh script. To enable the demo users, run the following commands:

   $ cd ~/logs
   $ sh /u01/install/APPS/scripts/enableDEMOusers.sh

   When prompted, enter a new password.

   Do not run this script on a fresh or production environment.
For details about the default passwords set during installation, see:


**Apply Oracle E-Business Suite and Database Patches (Conditionally Required):**

If you provisioned your environment from a backup of an existing on-premises environment, then you must now apply any additional patches required for your release level and database tier. For a cloned environment or an environment provisioned from a backup of a Cloud environment, these steps are required only if you did not already apply these patches on the source environment.

1. Apply the Oracle E-Business Suite patches required for your release.
   - Release 12.2.9, 12.2.8, 12.2.7, or 12.2.6 - Patch 24300571:12.2.0 [https://updates.oracle.com/download/24300571.html]
   - Release 12.2.5 - Patch 24300571:12.2.0 [https://updates.oracle.com/download/24300571.html] and Patch 23560508:R12.MSC.C [https://updates.oracle.com/download/23560508.html]
   - Release 12.2.4 - Patch 24300571:12.2.0 [https://updates.oracle.com/download/24300571.html] and Patch 23588491:R12.MSC.C [https://updates.oracle.com/download/23588491.html]
   - Release 12.2.3 - Patch 24300571:12.2.0 [https://updates.oracle.com/download/24300571.html] and Patch 23588492:R12.MSC.C [https://updates.oracle.com/download/23588492.html]
   - Release 12.1.3 - For Oracle E-Business Suite Release 12.1.3 on Oracle Database Release 12.1.0.2 only, you must apply interoperability Patch 25859639:12.1.0 [https://updates.oracle.com/download/25859639.html] on the application tier.

2. This step is required only if your new database tier is on 1-Node VM DB System, 2-Node VM DB System, or Exadata Cloud Service. Apply one-off database patches per the following:
   - For Oracle E-Business Suite Release 12.2, ETCC recommended database patches have been applied as part of the automated provisioning process. If you applied any additional one-off database patches beyond those recommended by ETCC
to the source on-premises database, then you must now reapply those additional one-off patches to your new 1-Node VM DB System, 2-Node VM DB System, or Exadata Cloud Service database.

- For Oracle E-Business Suite Release 12.1, if you applied any one-off database patches to the source on-premises database, then you must now reapply those one-off patches to your new 1-Node VM DB System, 2-Node VM DB System, or Exadata Cloud Service database.

If your database tier is on an Oracle Cloud Infrastructure Compute VM, then you do not need to reapply any one-off database patches.

Configure Enterprise Command Centers after One-Click Provisioning (Conditionally Required):
If you create an environment with One-Click Provisioning and you want to use Enterprise Command Centers in that environment, perform the following configuration steps.

1. Update the source system URL.
   - Log into your Oracle E-Business Suite environment as the sysadmin user, and select the ECC Developer responsibility.
   - Select Source System in the navigation pane of the Oracle Enterprise Command Center Framework administration UI.
   - In the Source System Definition page, enter your Oracle E-Business Suite login URL in the Source System URL field. For more information on the login URL, see User Access, page 10-2.

2. Initially, the Oracle Enterprise Command Center Framework installation includes data only for the Oracle Assets Command Center (FA). Before you can access an Enterprise Command Center dashboard for any other products, you must perform a full load of the product-specific data into the Oracle Enterprise Command Center Framework installation.
   - Ensure that the Oracle E-Business Suite Cloud Manager VM can access the Oracle E-Business Suite login URL by either configuring a DNS entry for the Oracle E-Business Suite host name or updating the local hosts file on the VM. See User Access, page 10-2.
   - Run the data load concurrent program for your product as listed in Loading Product Data to Enterprise Command Centers, Installing Oracle Enterprise Command Center Framework, Release 12.2 [https://support.oracle.com/rs?type=doc&id=2495053.1], My Oracle Support Knowledge Document 2495053.1. For more details about each data load program, see your product-specific
Enterprise Command Center documentation.
This chapter covers the following topics:

- Oracle E-Business Suite System Administration
- Access Your Oracle E-Business Suite Environment
- Access the Fusion Middleware Control and WebLogic Server Administration Console with SSH Port Forwarding for Oracle E-Business Suite on Oracle Cloud Infrastructure
- Review Environment Details (Standard)
- Review Standby Environment Details

Oracle E-Business Suite System Administration


Access Your Oracle E-Business Suite Environment

After you deploy an Oracle E-Business Suite environment through Oracle E-Business Suite Cloud Manager, users can access the login page for the environment, and administrators can access the application tier and database tier nodes that make up the environment.
User Access:
Before you can log in to Oracle E-Business Suite from a client computer, your network administrator must configure a DNS entry for the Oracle E-Business Suite host name. This entry lets the DNS server resolve the host name for the web entry point to the IP address.

The administrator should use the host name of the web entry point for the environment, including the domain name, to configure the DNS entry. For example, if the host for the web entry point is myhost and the domain is example.com, then the host name in the DNS entry should be myhost.example.com.

The IP address for the web entry point is available in the Oracle E-Business Suite Cloud Manager environment details page for the environment.

In situations such as demos where a DNS server is not readily available, you can modify the local hosts file on your client computer to enable host name resolution. To accomplish this, perform the following steps:

1. Update the /etc/hosts file on your client computer by adding a DNS entry in the following format:
   <external_IP_address> <host_name>

2. You can now navigate to the Oracle E-Business Suite login page at the following URL:
   [http|https]://<host_name>:<port>/OA_HTML/AppsLogin

   For example:
   http://myhost.example.com:8000/OA_HTML/AppsLogin

   **Note:** For environments created with One-Click Provisioning, the protocol is https and the port is 443. For environments created with Advanced Provisioning, the protocol and the port depend on the options selected in the Topology page.

Administrator Access:
After you create an Oracle E-Business Suite environment, as a database administrator (DBA) for the environment you will need to perform tasks such as starting and stopping services, applying patches, modifying files, and so on. One method to access the nodes that make up the environment is to connect through the Oracle E-Business Suite Cloud Manager Compute instance, as follows:

1. First, connect to your Oracle E-Business Suite Cloud Manager Compute instance that was created according to the instructions in Create Oracle E-Business Suite Cloud Manager Compute Instance, page 2-28. To connect, follow the instructions in Connecting to an Instance [https://docs.cloud.oracle.com/en-us/iaas/Content/Compute/Tasks/accessinginstance.htm].
2. After you have logged on to the Cloud Manager Compute instance, change to the oracle user.

   $ sudo su - oracle

3. You can now connect directly from the Cloud Manager Compute instance to the node you want in your Oracle E-Business Suite environment using the node's private IP address. Check the Oracle E-Business Suite Cloud Manager environment details page for your environment to find the private IP address for each application tier node and database tier node in the environment.

   $ ssh<private_IP>

If you deployed a separate bastion server and you plan to manage access to the Oracle E-Business Suite environments from that bastion server, then you can copy the private key in /u01/install/APPS/.ssh/id_rsa from the Oracle E-Business Suite Cloud Manager VM to the appropriate home directories on the bastion server. Alternatively, you can create accounts for each individual user on the bastion host and a corresponding user on the Oracle E-Business Suite VMs that the user needs to manage. On each VM host, grant the user "sudo to oracle" access.

   Note: If you uploaded SSH keys for the environment during provisioning, then you can use those keys to access the environment's nodes.

Database Administration Access:

When you provision an environment through Advanced Provisioning, you must specify a database admin password as part of the database tier details. You can use this password to log in to the database as the SYS user and perform database administration tasks.

Additionally, if Transparent Data Encryption (TDE) is enabled for an environment created through Advanced Provisioning, then you can also use the same database admin password to access the TDE wallet for the new environment. TDE is enabled for the following types of environments provisioned using Advanced Provisioning:

- All environments with a database tier on 1-Node VM DB System, 2-Node VM DB System, or Exadata Cloud Service, including both new environments and environments created from a backup. Note that even if the source environment for a backup was not TDE-enabled, TDE is still enabled for environments that are created from that backup on 1-Node VM DB System, 2-Node VM DB System, or Exadata Cloud Service.

- All environments with a database tier on Compute that are created from a backup of a TDE-enabled source environment.

- Environments with a database tier on Compute that are created from a backup of a non-TDE source environment, if you select the Enable TDE option during
provisioning.

- New environments created with Advanced Provisioning with a database tier on Compute, if you select the Enable TDE option during provisioning.

**Note:** TDE is not enabled for environments created with One-Click Provisioning. Also, TDE is not enabled if you do not select the Enable TDE option when it appears during Advanced Provisioning for environments on Compute.

### Access the Fusion Middleware Control and WebLogic Server Administration Console with SSH Port Forwarding for Oracle E-Business Suite on Oracle Cloud Infrastructure

System administrators can securely access the Fusion Middleware Control and WebLogic Server Administration Console in order to perform administration of an Oracle E-Business Suite Release 12.2 environment that was provisioned or cloned using Oracle E-Business Suite Cloud Manager on Oracle Cloud Infrastructure.

Administration of the Oracle Fusion Middleware 11g components delivered with Oracle E-Business Suite Release 12.2, including Oracle HTTP Server and Oracle WebLogic Server, requires secure access to the WebLogic Server administration ports running on the Oracle E-Business Suite primary application tier node. This section describes the steps a system administrator must follow each time they need to access the Fusion Middleware Control or WebLogic Server Administration Console in order to create a secure connection using SSH port forwarding.

You must have the following prerequisites to perform these steps:

- An environment provisioned in Oracle E-Business Suite Cloud Manager on Oracle Cloud Infrastructure.

- A security rule and firewall rules that allow inbound communication on the WebLogic Server administration ports on the primary application tier node from the Oracle E-Business Suite Cloud Manager VM. See Perform Post-Provisioning and Post-Cloning Tasks, page 9-24.

### Access the Fusion Middleware Control and WebLogic Server Administration Console with SSH Port Forwarding:

If you are a system administrator who needs access to the Fusion Middleware Control and WebLogic Server Administration Console to perform administrative tasks, follow these steps to create a secure connection from either a Windows or Linux client to the WebLogic Server administration port currently running on the Oracle E-Business Suite primary application tier node. You use SSH port forwarding to enable the connection.
Note: The SSH port forwarding steps must be performed and running in the background each time you connect to the URLs for the Fusion Middleware Control and WebLogic Server Administration Console from your browser.

These steps are required only for Oracle E-Business Suite Release 12.2. The required security rule and firewall rules must already be set up for the primary application tier node to allow inbound communication on the WebLogic Server administration ports.

1. Determine which WebLogic Server administration port is currently running on the primary application tier node. First set the environment to the run file system using the following command:

   $ . <EBS_ROOT>/EBSapps.env run

   Then obtain the current WebLogic Server administration port on the run file system, using the following command:

   $ grep s_wls_adminport $CONTEXT_FILE

   Make a note of the port for use in the next steps.

2. If you are using a UNIX client, perform this step to set up SSH port forwarding. If you are using a Windows client, skip this step and continue with step 3.

   From a UNIX client, set up SSH port forwarding using the following command:

   $ ssh -Llocalhost:<WLS_admin_port>:<primary_application_tier_node_private_IP_address>:<primary_application_tier_node_private_IP_address>:<WLS_admin_port> opc@<EBS_Cloud_Admin_Tool_VM_IP_address>

3. If you are using a Windows client, perform this step to set up SSH port forwarding. If you are using a UNIX client, skip this step and continue with step 4.

   From a Windows client, use PuTTY to set up SSH port forwarding. First, use the PuTTYgen tool to convert the private key for the Oracle E-Business Suite Cloud Manager VM into the appropriate format for PuTTY. In PuTTYgen, load the private key for the Oracle E-Business Suite Cloud Manager VM and click Save private key to save the key in the PuTTY format. Note that you should only load and save the existing key. Do not click the Generate button to generate a private key and public key again.

   Then start a PuTTY session and enter the following settings to configure the session:

   - In the Category pane of the PuTTY Configuration window, choose Connection >SSH >Auth to display the Options controlling SSH authentication panel. In the Private key file for authentication field, select Browse and select the private key file for connecting to the Oracle E-Business Suite Cloud Manager VM.

   - In the Category pane of the PuTTY Configuration window, choose Connection >SSH >Tunnels to display the Options controlling SSH port forwarding
In the Source port field, enter the WebLogic Server administration port. In the Destination field, enter the private IP address of the application tier node followed by a colon and the WebLogic Server administration port (<primary_application_tier_node_private_IP_address>:<WLS_admin_port>). Then choose Add.

- In the Category pane of the PuTTY Configuration window, choose Connection > Data to display the Data to Send to the Server panel. In the Auto-login username field, enter the following user name: oracle

- In the Category pane of the PuTTY Configuration window, choose Session to display the Basic options for your PuTTY session panel. In the Host Name field, enter the public IP address of the Oracle E-Business Suite Cloud Manager VM. Then enter a name for this session in the Saved Sessions field and click Save to save the session with this connection configuration.

Then use the saved session to open a connection to the Oracle E-Business Suite Cloud Manager VM.

4. After you set up SSH port forwarding from your UNIX or Windows client, you can securely access the Fusion Middleware Control and WebLogic Server Administration Console. Launch a browser from your client and connect to the following administrative URLs as required.

- Fusion Middleware Control - http://localhost:<WLS_admin_port>/em

- WebLogic Server Administration Console - http://localhost:<WLS_admin_port>/console

### Review Environment Details (Standard)

You can review details of an Oracle E-Business Suite environment using Oracle E-Business Suite Cloud. Oracle E-Business Suite Cloud Manager provides many details on an environment, including:

- General information, such as the Oracle E-Business Suite version, the Oracle E-Business Suite compartment and the network profile.

- Its assigned backup policy, if any. You can also assign a backup policy to the environment using this page.

- Topology information for the application tier and database tier.

- Any backups created for the environment.

- Activities related to the environment.
If you used Oracle E-Business Suite Cloud Manager to deploy an environment with Oracle Database Release 11.2.0.4 or Release 12.1.0.2, and you manually upgrade that environment to Oracle Database 19c, then Oracle E-Business Suite Cloud Manager can no longer recognize that environment. For an environment with the database tier on Compute or Exadata Cloud Service, you can run a script to refresh the metadata for the upgraded environment within Oracle E-Business Suite Cloud Manager. After the environment metadata has been refreshed, you can once again manage the environment through the Oracle E-Business Suite Cloud Manager UI. See Refresh Metadata for an Environment Upgraded to Oracle Database 19c, page 4-23.

**Note:** Some metadata for some attributes related to an environment are not shown, including

- After the successful creation of an environment using One-Click Provisioning, the Environment Details page does not display the related metadata for some attributes such as DB System Name, DB Edition, DB Patch Level, and Disk Redundancy.

- After the successful creation of an environment using Advanced Provisioning for Virtual Machine DB System, the Environment Details page does not display the related database metadata for some attributes such as DB System Name, DB Patch Level, and Disk Redundancy.

- After the successful creation of an environment using Advanced Provisioning for Exadata Cloud Service, the Environment Details page does not display the related database metadata for some attributes such as Disk Redundancy.

- After the successful creation of an environment using Oracle Database 11.2.0.4, the Details page will not display information for PDB Name as this feature does not apply to Oracle Database 11gR2.

For reviewing standby environments, refer to the section Review Standby Environment, page 10-12.

**Prerequisites**

- To perform the steps in this section, you must have an Oracle E-Business Suite environment on Oracle Cloud Infrastructure created in Oracle E-Business Suite Cloud Manager using a procedure described in One-Click Provisioning, page 9-6, Advanced Provisioning, page 9-8, or Clone an Oracle E-Business Suite Instance, page 11-5.
Access Environment Details Page:
1. For an environment that has been successfully provisioned, click the environment name in the Environments page to review more details for the environment.
2. Note that you can use buttons provided in the Environment details page to clone, back up, or delete an environment.

Review General Information:
1. The General Information region on the Overview page displays the following details:
   - Oracle E-Business Suite version
   - Version of the Oracle E-Business Suite Cloud automation tools with which the environment was provisioned
   - Oracle E-Business Suite Compartment, with the associated network profile name.
   - Number of application tier nodes
   - Number or database tier nodes
   - Latest activity, with a Status link for details
     For more information, see: Monitor Activity Status, page 12-1
   - Creation date and time
2. You can click the network profile name information link to review the details about the network resources defined in the network profile. See Set Up Network Profiles, page 8-1 for more information.
   The network profile window displays the following details:
   - Network Profile Description
   - Oracle E-Business Suite compartment
   - Network compartment
   - Region
   - VCN
   - Subnet type
- Availability domain
- Subnet access, either Private or Public
- Database subnet

3. Any Backup Policy defined for the environment is shown. If you want to specify a backup policy for this environment, click Assign under Backup Policy. For more information, see Schedule Backups, page 11-14.

   See Set Up Scheduling Policies, page 8-14 for more information on scheduling policies for backups.

4. For the application tier nodes, the following are provided:
   - Application tier nodes subnet access, either Private or Public
   - Application tier nodes subnet name

   The following load balancer information is shown:
   - Load balancer visibility type, either Private or Public
   - Load balancer subnet name
   - High availability subnet, if applicable. This field appears only if the subnet type is Availability Domain-Specific. The default subnet type is Regional.

Review Topology Information:
The Topology tab includes information for the Application Tier, Database Tier, and their nodes.

Review Application Tier Information
1. The Application Tier region includes the following:
   - EBS Base
   - File system type

2. For each zone defined for the application tier, the following details are shown:
   - Zone type
   - Web entry IP
   - Web entry type
• A link to the Oracle E-Business Suite login page
• LBaaS name, if any

3. For each node in each zone, the following details are provided:
   • Node ID
   • Fault domain
   • Shape
   • OCI Compute Instance OCID
   • Public IP
   • Private IP
   • Storage
   • Logical FQDN
   • DNS FQDN

   Note that the primary node is designated with a "P" on its icon.

4. If the environment utilizes load balancing, you can add a node using the Add Node button. For more information on adding and deleting nodes, see: Add and Delete Nodes, page 11-1.

**Review Database Tier Information**
1. The Database Tier region displays the following:
   • Cloud service type
   • Database name
   • VM Cluster Name (for Exadata Cloud Service only)
   • Database patch level
   • Update date for the database patch level
   • Database version
   • Pluggable database (PDB) name
   • Database edition
• SQL*Net port
• Creation date and time
• Shape
• Cluster name
• Oracle home

2. For each database tier node, the following is included:
   • Node ID
   • Fault domain
   • Public IP
   • Private IP
   • Logical FQDN
   • DNS FQDN

Review Backups:
If any backups have been created for the environment, you can select the Backups tab to view the list of backups.

Use the Search box to search for a specific backup.

1. To begin provisioning an environment from a backup, click Action for that backup and select Provision Environment.
   See Advanced Provisioning, page 9-8 for more information.

2. You can also select Delete from the Action menu for a backup to delete it.
   See Delete a Backup, page 11-18 for more information.

Review Activities:
The Activities tab lists activities associated with the environment.

1. You can use the Search box to search for a specific activity.

2. For each activity, the following fields are shown:
   • Environment
• Created By
• Action
• Status
• Start Time
• End Time

3. Click on an activity name to navigate to the Activity Details page.

See: Monitor Activity Status, page 12-1 for more information.

Review Standby Environment Details

You can review details of a standby environment you created in Oracle Applications Manager. Details on standby environments include:

• General information, such as the Oracle E-Business Suite version, the Oracle E-Business Suite compartment and the network profile.

• Its standby status.

• Topology information for the application tier and database tier.

• Activities related to the environment.

• Synchronization details.

For information on creating a standby environment, see: Create a Standby Environment for Oracle Cloud Infrastructure from an On-Premises Environment, page 6-7.

Access Environment Details Page:

1. For a standby environment that has been successfully provisioned, click the environment name in the Environments page to review more details for the environment.

Review General Information:

1. The overview section displays the following details:

• Oracle E-Business Suite version

• Release with which the environment was provisioned
• Oracle E-Business Suite Compartment, with the associated network profile name.

• Standby status

• Environment role

• Number of application tier nodes and database tier nodes

• Latest activity, with a Status link for details
  For more information, see: Monitor Activity Status, page 12-1

• Creation date and time

2. You can click the network profile name information link to review the details about the network resources defined in the network profile. See Set Up Network Profiles, page 8-1 for more information.

The network profile window displays the following details:

• Network Profile Description

• Oracle E-Business Suite compartment

• Network compartment

• Region

• VCN

• Subnet type

• Availability domain

• Subnet access, either Private or Public

• Database subnet

**Review Topology Information:**

The Topology tab includes information for the Application Tier, Database Tier, and their nodes.

For more information on adding and deleting nodes, see: Add and Delete Nodes, page 11-1.

1. The Application Tier region lists the Oracle E-Business Suite base directory and for each zone, the following is shown for each node:
• Node ID
• Fault Domain
• Shape
• Public IP
• Private IP
• Logical FQDN
• DNS FQDN
• OCI Compute Instance OCID: You can click the Show link to see the entire OCID or Copy to copy it.

Note that the primary node is designated with a "P" on its icon.

2. The Database Tier region list the following:
   For the Database Tier region, the following information is shown:
   • Cloud Service Type
   • Database Name
   • Database System Name
   • Database Patch Level
   • Database Patch Level Updated Date
   • Database Version
   • Pluggable Database Name
   • Database Edition
   • SQL*Net Port
   • Creation date and time
   • Shape
   • Cluster Name
   • Oracle Home
For each database node, the following information is listed:

- Node ID
- Fault Domain
- Public IP
- Private IP
- Logical FQDN
- DNS FQDN

**Review Activities:**
The Activities tab lists activities associated with the standby environment.
If an activity has been restarted from a parent activity a link is provided for details for the parent.

1. You can use the **Search** box to search for a specific activity.

2. For each activity, the following fields are shown:
   - Environment
   - Created By
   - Action
   - Status
   - Start Time
   - End Time

3. Click on an activity name to navigate to the Activity Details page.
   See: Monitor Activity Status, page 12-1 for more information.

**Review Synchronization Details:**
Details for a synchronization process are shown on the Synchronization Details tab. Use the **Refresh** button to refresh the data.

1. For the Application Tier, the following fields are shown:
   - Rsync Status
• Last Rsync Timestamp
• Total Number of Files
• Synchronized Number of Created Files
• Number of Deleted Files

2. For the Database Tier, the following fields are shown:
• Database Role
• Database Open Mode
• Database Unique Name
• Data Guard Status
• Last Sequence in Primary
• Last Sequence in Standby
• Last Redo Log Applied Timestamp
• Last Transport Lag
• Last Apply Lag
• Standby Apply Status
• Protection Mode
This chapter covers the following topics:

- Add and Delete Nodes
- Clone an Oracle E-Business Suite Instance
- Back Up an Oracle E-Business Suite Instance
- Promote a Standby Environment
- Delete an Oracle E-Business Suite Environment

Add and Delete Nodes

Use these procedures to add or delete nodes from a provisioned environment that has load balancing configured.

Note that adding and deleting nodes can both be done while the system is online. The system does restart the administration server during these procedures but the running Oracle E-Business Suite instance should not be affected.

Prerequisites

- You must have an Oracle E-Business Suite environment on Oracle Cloud Infrastructure created using the procedure Advanced Provisioning, page 9-8 or Clone an Oracle E-Business Suite Instance, page 11-5.

- The environment must have either New Load Balancer (LBaaS) or Manually Configured Load Balancer as the Web Entry Point for the primary zone. If an environment has the Web Entry Point defined as Application Tier Node, then only one application tier node is possible for that zone, so you cannot add more nodes.
Add a Node:
The Oracle E-Business Suite Cloud Manager performs the following actions when adding a node to your application tier:

- Runs generic validations
  - Validates that the AD Online Patching (adop) cycle is complete
  - Validates that the Administration Server is up
  - Validates that the Oracle HTTP Server (OHS) has custom directives
  - Validates application connectivity

- Creates the infrastructure: Creates the VM required for the additional node

- Performs pre-configuration tasks
  - Creates the Add Node pairs file
  - Performs pre-cloning steps

- Configures the newly-added application tier node
  For a non-shared environment on Compute, if the primary node has additional block volume attached to extend Logical Volume Management (LVM) to increase the space under `/u01`, then the Add Node feature will pick up the size of the LVM (`/dev/mapper/ebs_vg-ebs_lv`) on `app01` and create a single block volume of the same size.

- Performs post-provisioning steps

- Brings up the newly-added application tier node

In addition, the Cloud Manager modifies the load balancer back-end set to accommodate the new application tier node.

Note that if Manual Configured Load Balancer was chosen for the Web Entry Point, you can add nodes, but LBaaS is not deployed.

1. For an environment that has been successfully provisioned, click the environment name in the Environments page to navigate to the Environment Details page.

2. In the Topology tab, for a chosen Zone, click the Add Node button.

3. In the Add Node window, enter the following:
   - Shape
• File System Type - This value is derived for you and cannot be changed.

• Fault Domain

• Logical Hostname

• APPS Password

• WLS Password - For Oracle E-Business Suite Release 12.2 only.

4. Click **Submit**.

**Manual Steps after Adding a Node**

You must perform the following manual steps after adding a node. Run these steps on all existing nodes.

**Update the TNS Listener Service**

1. Source the run file system.

2. Run AutoConfig. This step is required to register the new node with the TNS listener and to update the APPL_TOP IDs correctly.

3. Stop and start the TNS listener service as follows:

   $ cd ADMIN_SCRIPTS_HOME
   $ adalnctl.sh stop
   $ adalnctl.sh start

**Stop and Start the OHS Service**

4. Source the run file system.

5. Run the following commands to stop and start the OHS service:

   $ cd ADMIN_SCRIPTS_HOME
   $ sh adapcctl.sh stop
   $ sh adapcctl.sh start

**Delete a Node:**

In deleting a node, the system will:

• Run generic validations

• Validate that the administration server is up

• Validate application connectivity

• Remove the secondary application tier node
• Remove the secondary application tier configuration
• Detach the custom volumes of the node
• Remove all other OCI infrastructure associated with this application tier node
• Delete any LBaaS infrastructure (delete whatever is applicable)

• Perform post-cleanup tasks

In deleting an application tier node, the system also modifies the back-end set to account for the loss of the node.

1. For an environment that has been successfully provisioned, click the environment name in the Environments page to navigate to the Environment Details page.

2. In the Topology tab, navigate to the node you want to delete and click the Delete button.

3. Enter the APPS Password. For Oracle E-Business Suite Release 12.2, also enter the WLS Password.

4. If the selected node is the only node in its zone, specify whether to remove LBaaS. The load balancer is removed only if it is not in use by other resources.

   Note that any custom block volume associated with the node is detached from the node when it is deleted.

5. Click Yes to confirm the deletion.

**Manual Steps after Deleting a Node**

You must perform the following manual steps after deleting a node. Run these steps on all remaining nodes.

**Update the TNS Listener Service**

1. Source the run file system.

2. Run AutoConfig.

3. Stop and start the TNS listener service as follows:

   $ cd ADMIN_SCRIPTS_HOME
   $ adainctl.sh stop
   $ adainctl.sh start

**Stop and Start the OHS Service**

4. Source the run file system.
5. Run the following commands to stop and start the OHS service:

$ cd ADMIN_SCRIPTS_HOME
$ sh adapcctl.sh stop
$ sh adapcctl.sh start

Clone an Oracle E-Business Suite Instance

The cloning procedure leverages the native Block Volume Cloning capability in Oracle Cloud Infrastructure, and is available only for environments where the Oracle E-Business Suite database and application tiers both reside on a Compute VM.

Note these additional key attributes:

- This procedure can be run either when the Oracle E-Business Suite services (application tier and database tier) are running, or when they are shut down.

- The clone uses the same network profile as the source environment.

- The load balancer can be deployed as a public or private Load Balancer as a Service (LBaaS) for the clone, depending on the load balancer type defined in the network profile.

- The clone resides in the same availability domain as the source environment.

- The shape of database tier of the clone is same as the shape of the source environment. However, the shape of the application tier of the clone can be changed.

- The application tier of the clone mirrors that of the source environment. For example, if the source environment has one application tier node, then the clone will have one application tier node. If the source environment has two application tier nodes, then the clone will have two application tier nodes. Additionally, if the source environment has an application tier node and database on a single Compute VM, then the clone will also have its application tier node and database on a single Compute VM.

- The Cloud Manager automation configures the application tier services to utilize port pools 0 and 1. These cannot be changed. The section Create Security Rules, page 3-21 lists the ports that must be open between subnets in order for your system to function properly.

- You can choose to start the Oracle E-Business Suite services automatically on the clone.

- When you clone an environment, you can use tagging by choosing a pre-defined tag or specifying a new (free-form) tag. You can use this tag to identify all resources associated with an environment or group of environments. Refer to Managing Tags...
Prerequisites

☑️ You must have a source Oracle E-Business Suite environment on Oracle Cloud Infrastructure created using One-Click Provisioning, page 9-6 or Advanced Provisioning, page 9-8.

☑️ You must have access to the network profile used by the source environment. The network profile specifies the network resources for the environment, including the security lists and subnets. The administrator of your Oracle E-Business Suite Cloud Manager instance defines network profiles and assigns you the profiles that you can use to provision Oracle E-Business Suite environments.

Refer to the following documentation for more information:

- Create Network Resources For Deploying Oracle E-Business Suite Environments, page 3-9
- Create Network Profiles, page 3-34

☑️ If you choose to use tags, you can create defined tags first. Any tag namespace selected must be defined for the compartment in which you are provisioning, as specified in the network profile. Refer to Managing Tags and Tag Namespaces [https://docs.cloud.oracle.com/en-us/iaas/Content/Tagging/Tasks/managingtagsandtagnamespaces.htm] for more information.

Access the Clone Environment Page:

1. Click the Navigator icon and select Environments.

2. For a successfully created environment, click the Action icon and select Clone.

3. Alternatively, in the environment details page for a single environment, click the Action icon and select Clone.

Enter Environment Details:

1. Enter values for the clone details:

   - Environment Name: Enter a name for your environment. For example: usdev3
• **EBS Compartment:** The compartment for the source environment. This cannot be updated.

• **Network Profile Name:** The cloned environment will use the same network profile as the source environment.

• **Source Apps Password:** Enter the password for the Oracle E-Business Suite APPS schema for the source environment.

• **Source WebLogic Server password:** For an Oracle E-Business Suite Release 12.2 environment only, enter the Oracle WebLogic Server administration password.

2. Optionally enter tagging information in the Tags region.
   - **Tag Namespace:** Select a predefined tag namespace or select None (add a free-form tag).
   - **Tag Key:** Enter the name you use to refer to the tag.
   - **Value:** Enter the value for the tag key.

3. Click Next.

**Enter Application Tier Information:**

Zone information from the source environment will appear by default.

You can change the shape for an application tier node

1. Toggle **Start Application Tier Services** to indicate whether application tier services should start when the clone is complete.

2. You must edit the zones. Click **Edit** for each zone.

3. Enter the **Zone** name. Note that you cannot change the type of the zone.

4. In the **Web Entry Point** region, choose one of the following web entry types: **New Load Balancer (LBaaS)**, **Manually Configured Load Balancer** to select a manually deployed existing load balancer, or **Application Tier Node** to choose the primary application tier as the entry point.

   **Note:** You must choose the web entry type that is the same as the source web entry type.

5. If you choose to use LBaaS, then you must also select a shape in the **Load Balancer Shape** field. The default shape is **100Mbps**.
6. Enter values for the following web entry properties.
   - **Protocol**: Select the protocol for access to the environment, either http or https.
   - **Hostname**: Enter a hostname. For example: myhost
   - **Domain**: Enter a domain name. For example: example.com
   - **Port**: Select the port. If there is no load balancer, then the port is automatically populated depending on the protocol: 8000 for http and 4443 for https. Otherwise, select the appropriate port for use with your load balancer, such as 80 for http or 443 for https. Note that to allow access to the Oracle E-Business Suite login URL, your network administrator must define an ingress rule in the load balancer security list configuring the load balancer port to be open for public access. See Create Network Resources For Deploying Oracle E-Business Suite Environments, page 3-9.

7. Under Storage, the **File System Type** is the same as that for the source environment.

8. Review the properties for each node in the Application Tier Nodes information.
   - **Logical FQDN**
   - **Shape**: You can change the shape for the node. You are prompted to confirm your choice. For example: **VM.Standard2.1 - (1 OCPU, 15 GB RAM)**
   - **Storage**
   - **Fault Domain**

9. Click **Save Zone**.

10. When you are finished editing your zones, click **Next**.

**Specify Your Extensibility Options:**
You can optionally extend the cloning activity to meet your own requirements. By default, Oracle E-Business Suite Cloud Manager follows a standard activity plan for cloning. However, Oracle E-Business Suite Cloud Manager administrators can also create extended activity plans that include additional tasks as part of the cloning activity. In this case you can select the appropriate extended activity plan for Oracle E-Business Suite Cloud Manager to follow when cloning your environment. If you select an extended activity plan, you may need to enter values for input parameters required by the additional tasks in that plan.

**Additional Information**: For more information on using the Extensibility
Framework to extend activity plans, see Set Up the Extensibility Framework, page 8-8.

Additionally, whether you are using the standard cloning activity plan or an extended activity plan, you can choose to have Oracle E-Business Suite Cloud Manager pause at specified points during the cloning activity. For example, if you want to perform your own validations after a particular phase before allowing Oracle E-Business Suite Cloud Manager to proceed to the next phase, you can add a pause at that point. You can then resume the cloning activity when you are ready to proceed. See Monitor Activity Status, page 12-1.

Define Your Activity Plan
1. Optionally select an extended activity plan for cloning your environment in the Activity Plan field.

2. In the Task Parameters tab, specify any parameter values required for the additional tasks in the plan. Some parameters may include default values, which you can override as needed.

Define Your Activity Plan Details
3. Click the Activity Plan Details tab. This tab displays a list of the phases in the activity plan and the tasks within each phase.

4. To specify that Oracle E-Business Suite Cloud Manager should pause its processing before a particular phase, click the Actions icon next to that phase, and then select Add Pause.

   Note: Pauses occur before the phase at which they are defined.

5. Click Next.

Enter SSH Keys:
Optionally upload SSH keys for users.

   Note: You cannot add keys after the provisioning process is completed.

1. Click Add Key.

2. Specify the tiers for the SSH key. Choose All Tiers, Application Tier, or Database Tier.

3. Specify the pertinent OS User type. Choose All Users, Operating System Administrator, or Application Administrator.
4. Upload the SSH key file. The file name will default in.

5. The system will validate the SSH key. Click **Next** to continue.

**Review Your Clone Environment Flow Details:**
1. Review the installation details; database details; application tier details, including zones; execution plan details, and SSH key information.

2. To provision your environment, click **Submit**.

3. You can check the status of the activity to provision the environment in the Activities page.

**Perform Post-Cloning Tasks:**
After the environment is successfully cloned, perform any necessary post-cloning steps and access your environment following the instructions provided in Perform Post-Provisioning and Post-Cloning Tasks, page 9-24.

**Back Up an Oracle E-Business Suite Instance**
You can use Oracle E-Business Suite Cloud Manager to create a backup of an existing Oracle E-Business Suite environment on Oracle Cloud Infrastructure. This feature is available for environments created using Advanced Provisioning. You can either create an individual backup or schedule backups to be created automatically. Oracle E-Business Suite Cloud Manager creates backups on the Oracle Cloud Infrastructure Object Storage service.

You must have the following prerequisites to create a backup.

**Prerequisites**
- An Oracle E-Business Suite environment provisioned on Oracle Cloud Infrastructure. This environment must meet all prerequisites for Oracle E-Business Suite Cloud Manager provisioning, including required patches based on the target database location. See Source Environment Requirements, page 5-4.

- Cloud resources that match or exceed the minimum recommendations specified in Cloud Services Minimum Resource Recommendations, page 5-7.

- An Oracle Cloud Infrastructure Object Storage compartment in which to create the backup. See Backing Up to Oracle Cloud Infrastructure Object Storage [https://docs.cloud.oracle.com/en-us/iaas/Content/Database/Tasks/backingupOS.htm].
Manage Backups:
You can use Oracle E-Business Suite Cloud Manager to manage both backups created from environments on Oracle Cloud Infrastructure and backups created from on-premises Oracle E-Business Suite environments. You can provision another environment based on a backup, or delete a backup when you no longer need it.

- Create a Backup of an On-Premises Oracle E-Business Suite Instance on Oracle Cloud Infrastructure, page 5-2
- Create a Backup of a Cloud-Based Oracle E-Business Suite Instance, page 11-11
- Schedule Backups, page 11-14
- Review Backups, page 11-17
- Delete a Backup, page 11-18

Create a Backup of a Cloud-Based Oracle E-Business Suite Instance:
Perform the following steps when creating a backup:

1. Create a backup, page 11-11.


Create a Backup

1. Click the Navigator icon, and then select Environments. In the Environments page, click the Actions icon next to the environment you want, and then select Create Backup.

   Alternatively, click an environment name link in the Environments page to navigate to the environment details page for a single environment, and click Create Backup.

   Note that the Create Backup option is not available for environments generated using One-Click Provisioning, and is therefore grayed out for those environments.

2. In the Create Backup window, accept the system-generated backup name or enter a new name to uniquely identify your backup. The name must be a maximum of 31 characters long and must include only alphanumeric characters and underscores. It cannot include any special characters other than underscores. Additionally, the first character of the name must be an alphabetic letter. The name cannot begin with a numeral or an underscore.

   Oracle E-Business Suite Cloud Manager adds the backup name as a prefix when creating the containers to store objects in a compartment within an Oracle Cloud Infrastructure Object Storage namespace, known as buckets. The generic bucket for the application tier and database tier Oracle home backup is named
<Backup_Name>Generic. The database bucket for the database RMAN backup is named <Backup_Name>DB.

3. Select the Oracle Cloud Infrastructure Object Storage compartment where you want to create the backup.

4. In the Encryption Password field, specify a password to encrypt the application tier file system and database tier file system. If Transparent Data Encryption (TDE) is not enabled in the source database, then this password is also used to encrypt the database RMAN backup.

Re-enter the encryption password in the next field to confirm it.

5. Enter the password for the Oracle E-Business Suite APPS schema for the source environment.

6. For an Oracle E-Business Suite Release 12.2 environment only, enter the Oracle WebLogic Server administration password for the source environment.

7. If Transparent Data Encryption (TDE) is enabled in the source database, enter the password for the TDE wallet.

8. You can optionally specify advanced Recovery Manager (RMAN) parameters. To do so, click Show Advanced Options. If you do not need to change the RMAN parameters, skip to step 14.

9. As part of RMAN backup, in the copy phase database blocks will be validated implicitly, and any corruption or missing object will be reported at that time. If you want to enforce the database validation before the RMAN backup, then click the RMAN_VALIDATE_DATABASE toggle switch to turn this option on.

10. Select the binary compression algorithm to use for RMAN backup, either Basic, Low, Medium, or High. The default value is Basic. Note that the Low, Medium, and High compression algorithms fall under Advanced Compression. You must have or acquire a license for the Advanced Compression option to use these compression algorithms. The Advanced Compression option is included in all Exadata cloud service subscriptions, and in VM DB Systems subscriptions with Enterprise Edition High Performance and Extreme Performance options.

11. Specify the number of RMAN staging channels to allocate for creating the backup. The default value is 75% of the number of OCPUs. For example, for a VM with the shape Standard 2.4, the default value for the RMAN Channel Count parameter is 6. The minimum value is one channel. The maximum value is 255 channels.

12. Specify the section size for multisection backups. The default value is 64G. Valid values are 2G, 4G, 8G, 16G, 32G, 64G, 128G, or 256G.

13. The following parameters are set automatically to default values by RMAN unless
you enter specific values for them here. You should only set values for these parameters if you fully understand their effects, as inappropriate settings can reduce backup performance.

- Specify the maximum number of data files to place in each backup set. The default value is 64. To determine the number of data files in each backup set, RMAN uses either the value you specify in this parameter or the number of files read by each channel, whichever is lower. If you allocate only one channel, then you can use this parameter to make RMAN create multiple backup sets.

- Specify the maximum number of input files that a backup or copy can have open at a given time. The default value used by RMAN is 8.

- Specify the rate of bytes per second that RMAN can read on this channel. Use this parameter to set an upper limit for bytes to read so that RMAN does not consume excessive disk bandwidth and degrade online performance. Specify the rate as an integer, and select the unit of measurement in which you are expressing the rate, either K, M, or G.

- It is not recommended to use the RMAN_DATAFILE_ID_ALLOWED_MAXCORRUPT parameter for normal processing. However, if necessary, you can set this parameter to specify the maximum number of corruptions permitted in a data file during the backup job. Specify the parameter value as a list showing each data file ID and the maximum number of corruptions for that data file, in the following format: `<DATA_FILE_ID_1>:<MAX_CORRUPTIONS_1>, <DATA_FILE_ID_2>:<MAX_CORRUPTIONS_2>, ...`

14. Click **Create Backup**.

   **Note:** Oracle E-Business Suite Cloud Manager automatically records the operating system time zone for the source database node as part of the backup metadata. This time zone value is used to help determine the default time zone for environments provisioned from this backup if the Server Timezone profile option is not set within the source environment. For more information, see Advanced Provisioning, page 9-8.

15. You can check the status of the activity to create the backup in the Activities page. Locate the create-ossbackup activity that you want to troubleshoot, and click the activity name link to go to the Activity Details page. See Monitor Activity Status, page 12-1.

   The Activity Details page provides links to the log files for each task performed to create the backup, including pre-validation tasks and main execution tasks. If a backup creation activity does not succeed, you can review the related log files for
the specific task that failed to troubleshoot the issue.

16. After a backup is successfully created, you can review the backup details in the Backups page or in the Administration tab of the environment details page for the source environment. From these pages, to begin provisioning another environment on Oracle Cloud Infrastructure based on the backup, click the action icon and select **Provision Environment**. See Advanced Provisioning, page 9-8.

17. If you no longer need a backup, to begin deleting it, navigate to that backup in the Backups page or the Administration tab of the environment details page for the source environment, then click the action icon, and select **Delete**. You can also use a command-line API to delete a failed backup. See Delete a Backup, page 11-18.

**Review Oracle WebLogic Server Validation Warnings (Conditionally Required)**
Oracle E-Business Suite Cloud Manager performs certain validations on the Oracle WebLogic Server domain and stops the backup creation activity with a warning if the default threshold values are exceeded. If the activity logs show one of these warning messages, then you should review the source environment to decide whether you can make changes to resolve the issue and proceed with the backup.

- **WLS domain size is higher than EBS default threshold: 5120 MB** - Check what factors are causing the Oracle WebLogic Server domain size to be greater than 5120 MB (5 GB). If the domain size is due to large log files or temporary files, then you should first clean up those files to reduce the domain size, and then retry the backup creation activity.

- **ERROR : Backup config.xml file count is higher than EBS default threshold : 500. Please clean up some of the backup config.xml files available in `<EBS_DOMAIN_HOME>/config` directory.** - Check the `<EBS_DOMAIN_HOME>/config` directory to determine whether you can delete any older Oracle WebLogic Server backup configuration files (`backup_config*.xml`) before retrying the backup creation activity.

For more information about retrying a backup creation activity, see Monitor Activity Status, page 12-1.

**Schedule Backups:**
You can schedule backups to be created for an environment automatically by creating a scheduling policy and then assigning it to the environment in the environment details page. See Set Up Scheduling Policies, page 8-14 and Review Environment Details, page 10-6.

If you no longer want to create backups on the specified schedule, you can remove the policy assignment for the environment.

**Note:** A scheduled backup can be run only when no other activity is
being performed for that environment.

- If two backups are scheduled at the same time for the same environment, then Oracle E-Business Suite Cloud Manager only runs one backup activity at that time. The status for the other scheduled backup activity is marked as **Missed**.

- If a backup is scheduled to be created at a certain time but another activity is already running for the environment at that time, such as adding or deleting a node, cloning, or another backup, then the scheduled backup is not created and the status of the scheduled backup activity is set to **Missed**.

You cannot retry a missed activity directly. However, you can schedule another backup or manually create another backup for the environment if necessary.

1. Click the **Navigator** icon, and then select **Environments**. Click the environment name link for the environment you want to back up.

2. In the environment details page, locate the Backup Policy property. If no policy is currently assigned, click the **Assign** link.

3. In the Assign Backup Policy window, select the Oracle Cloud Infrastructure Object Storage compartment where you want to create the backups.

4. Select the policy that specifies the schedule on which you want to create backups.

5. Enter a backup name prefix to uniquely identify your backups. The name prefix must be a maximum of 18 characters long and must include only alphanumeric characters and underscores. It cannot include any special characters other than underscores. Additionally, the first character of the name must be an alphabetic letter. The name cannot begin with a numeral or an underscore.

Oracle E-Business Suite Cloud Manager adds the backup name prefix when creating the containers to store objects in a compartment within an Oracle Cloud Infrastructure Object Storage namespace, known as buckets. The generic bucket for the application tier and database tier Oracle home backup is named `<Backup_Name>Generic`. The database bucket for the database RMAN backup is named `<Backup_Name>DB`.

6. In the Encryption Password field, specify a password to encrypt the application tier file system and database tier file system. If Transparent Data Encryption (TDE) is not enabled in the source database, then this password is also used to encrypt the database RMAN backup.

Re-enter the encryption password in the next field to confirm it.
7. Enter the password for the Oracle E-Business Suite **APPS** schema for the source environment.

8. For an Oracle E-Business Suite Release 12.2 environment only, enter the Oracle WebLogic Server administration password for the source environment.

9. If Transparent Data Encryption (TDE) is enabled in the source database, enter the password for the TDE wallet.

10. You can optionally specify advanced Recovery Manager (RMAN) parameters. To do so, click **Show Advanced Options**. If you do not need to change the RMAN parameters, skip to step 14.

11. As part of RMAN backup, in the copy phase database blocks will be validated implicitly, and any corruption or missing object will be reported at that time. If you want to enforce the database validation before the RMAN backup, then click the **RMAN_VALIDATE_DATABASE** toggle switch to turn this option on.

12. Select the binary compression algorithm to use for RMAN backup, either **Basic**, **Low**, **Medium**, or **High**. The default value is **Basic**. Note that the Low, Medium, and High compression algorithms fall under Advanced Compression. You must have or acquire a license for the Advanced Compression option to use these compression algorithms. The Advanced Compression option is included in all Exadata cloud service subscriptions, and in VM DB Systems subscriptions with Enterprise Edition High Performance and Extreme Performance options.

13. Specify the number of RMAN staging channels to allocate for creating the backup. The default value is 75% of the number of OCPUs. For example, for a VM with the shape **Standard 2.4**, the default value for the RMAN Channel Count parameter is 6. The minimum value is one channel. The maximum value is 255 channels.

14. Specify the section size for multisection backups. The default value is **64G**. Valid values are **2G**, **4G**, **8G**, **16G**, **32G**, **64G**, **128G**, or **256G**.

15. The following parameters are set automatically to default values by RMAN unless you enter specific values for them here. You should only set values for these parameters if you fully understand their effects, as inappropriate settings can reduce backup performance.

   - Specify the maximum number of data files to place in each backup set. The default value is 64. To determine the number of data files in each backup set, RMAN uses either the value you specify in this parameter or the number of files read by each channel, whichever is lower. If you allocate only one channel, then you can use this parameter to make RMAN create multiple backup sets.

   - Specify the maximum number of input files that a backup or copy can have open at a given time. The default value used by RMAN is 8.
• Specify the rate of bytes per second that RMAN can read on this channel. Use this parameter to set an upper limit for bytes to read so that RMAN does not consume excessive disk bandwidth and degrade online performance. Specify the rate as an integer, and select the unit of measurement in which you are expressing the rate, either K, M, or G.

• It is not recommended to use the RMAN_DATAFILE_ID_ALLOWED_MAXCORRUPT parameter for normal processing. However, if necessary, you can set this parameter to specify the maximum number of corruptions permitted in a data file during the backup job. Specify the parameter value as a list showing each data file ID and the maximum number of corruptions for that data file, in the following format:
  
  <DATA_FILE_ID_1>:<MAX_CORRUPTIONS_1>, <DATA_FILE_ID_2>:<MAX_CORRUPTIONS_2>, ...

16. Click Assign.

17. For an environment that currently has a backup policy, if you no longer want to create backups on the schedule specified by that policy, click Unassign to remove the policy assignment.

Review Backups:

1. To review the backups stored on the Oracle Cloud Infrastructure Object Storage service for your deployment, click the Navigator icon, and then select Backups.

   Note: You can also review a list of the backups for a particular environment in the environment details page for that environment. See Review Environment Details, page 10-6.

2. The Backups page displays the available backups, including both backups of on-premises environments and backups of environments on Oracle Cloud Infrastructure. You can optionally enter a full or partial value in the search field to display only backups whose properties contain that value. You can search by the following properties shown in this page:

   • Backup name
   • Oracle E-Business Suite version
   • Database version
   • Compartment name
   • Database name
• Whether TDE is enabled for the environment
• The size of the database after it is restored
• Creation date and time

3. To provision an environment from a backup, click the Actions icon next to that backup, and then select Provision Environment. See Advanced Provisioning, page 9-8.

4. To delete a backup, click the Actions icon next to that network profile, and then select Delete. See Delete a Backup, page 11-18.

Delete a Backup:
The Delete Backup operation is available for backups created using the Oracle E-Business Suite Cloud Backup Module or using Oracle E-Business Suite Cloud Manager. See: Create a Backup of an On-Premises Oracle E-Business Suite Instance on Oracle Cloud Infrastructure, page 5-2 or Create a Backup of a Cloud-Based Oracle E-Business Suite Instance, page 11-11.

Delete a Successful Backup
This section covers instructions on how to delete a successful backup in Oracle E-Business Suite Cloud Manager.

   Note: This action is irreversible. Use caution with this feature.

1. Click the Navigator icon and select Backups. Alternatively navigate to the Environment Details page for the Cloud environment and select the Backups tab.

2. Select a backup from the list of available backups on the page. You can search for the backup if you know its name or part of its name.

3. Click Action icon for the backup and select Delete.

4. In the confirmation window, select Yes.

5. You can check the status of the activity to delete the backup in the Activities page. See: Monitor Activity Status, page 12-1.

Delete a Failed Backup
This section covers instructions on how to delete a failed backup. Use these instructions if your backup process fails and you need to reuse the same bucket name in creating a new backup. The "Backup Identifier Tag" is used to create the bucket name.

1. For the failed backup, note the path to the session ID. This ID is displayed on the
console while the backup is being created when you run the Oracle E-Business Suite Cloud Backup Module. If you create a backup using Oracle E-Business Suite Cloud Manager, you can find the session ID in the activity logs for the failed activity. See the section Monitor Activity Status, page 12-1 for more information. The session ID should be in the format $<STAGE_DIRECTORY>/session/<SESSION_ID>$. An example is /u01/db1/session/xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.

2. Connect to the primary node of the application tier and the database tier, and identify if any remote clone processes related to the failed backup are running. For example, run the following command:

```bash
$ ps -ef|grep remoteclone|grep xxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

and terminate those processes in both the application tier and the database tier. Note that there could be other backup processes running on the source application tier or database tier. Ensure that you terminate only the processes related to the failed backup.

3. Ensure that the OCI configuration file and PEM key file are present on the Oracle E-Business Suite Cloud Manager orchestration VM. For information on the OCI configuration file, see Create a Profile in the Oracle Cloud Infrastructure CLI Configuration File [https://docs.cloud.oracle.com/en-us/iaas/Content/Functions/Tasks/functionsconfigureocicli.htm].

4. Go to the RemoteClone directory in the current backup session, and run the command for deleting the Database and Generic buckets.

1. Run the following command on the Oracle E-Business Suite Cloud Manager orchestration VM:

```bash
$ cd /u01/install/APPS/apps-unlimited-ebs/RemoteClone
```

2. Run the following command with the required details to delete the bucket.

   ```bash
   ```

Description of parameters:

- `<bucketName>` is the Bucket name.
- `<proxyPort>` is the Proxy Port.
• `<proxyProtocol>` is the Proxy Protocol.
• `<bmcsTenantName>` is the BMCS Tenant name.
• `<compartmentID>` is the BMCS Compartment ID.
• `<proxyUsername>` is the Proxy Username.
• `<bmcsConfigFilePath>` is the complete path to the BMCS configuration file.
• `<proxyHost>` is the Proxy Host.
• `-h` can be used for help with the command.

Example commands:

• For deleting a Generic bucket with Backup Identifier Tag 'PRODBACKUP':

```$ 3pt/jre/bin/java -cp lib/cln_utils.jar:3pt/ext-jars/* oracle.apps.liftNshift.commandline.client.bmcs.EBSLiftBMCSDeleteBucketClient -bucketName PRODBACKUPGeneric -compartmentID ocid1.compartment.oc1..xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx -bmcsTenantName BMCSTENANT -bmcsConfigFilePath /u01/install/APPS/userpem/user```

• For deleting a Database bucket with Backup Identifier Tag 'PRODBACKUP':

```$ 3pt/jre/bin/java -cp lib/cln_utils.jar:3pt/ext-jars/* oracle.apps.liftNshift.commandline.client.bmcs.EBSLiftBMCSDeleteBucketClient -bucketName PRODBACKUPDB -compartmentID ocid1.compartment.oc1..xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx -bmcsTenantName BMCSTENANT -bmcsConfigFilePath /u01/install/APPS/userpem/user```

**Note:** If you want to rerun the Oracle E-Business Suite Cloud Backup Module using the same bucket name, then you must first provide a new stage directory path for both the application and database tier.

**Related Topics**

Back up a Database to Object Storage Using RMAN [https://docs.cloud.oracle.com/en-us/iaas/Content/Database/Topics/backupstorage.htm]

Promote a Standby Environment

You may promote only standby environments that have been successfully configured.

Select the Standby Environment:
1. Navigate to the Environments page in Oracle E-Business Suite Cloud Manager.
2. Select Promote from the Action menu for the standby environment you wish to promote.
3. Alternatively, select the standby environment and click on Promote from its Environment Details page.

Enter Standby Environment Details:
The Environment Name, EBS Compartment, and Network Profile Name are shown and cannot be changed.
1. Enter the APPS Password.
2. Enter the WebLogic Server Password.
3. Optionally enter tagging information in the Tags region.
   - Tag Namespace: Select a predefined tag namespace or select None (add a free-form tag).
   - Tag Key: Enter the name you use to refer to the tag.
   - Value: Enter the value for the tag key.
4. Click Next.

Enter Database Information:
Review and enter database details and related options.
1. Enter the following:
   - DB SID: This field is read-only. The database SID. For example: demodb
• **Database Service Type**: This field is read-only.

• **Logical Hostname**: Provide the logical hostname that will be used as part of the Oracle E-Business Suite configuration. Note that this is not the physical hostname.

• **Logical Domain**: Provide the logical domain that will be used as part of the Oracle E-Business Suite configuration. Note that this is not the physical domain.

• **VM Shape**: This field is read-only. The shape shown is the shape selected during standby creation.

• **Enable TDE**: This field is read-only and enabled by default.

• **Admin Password**: This field is read-only. The admin password for the database is used for the SYS user as well. If TDE is enabled for the environment, then this password is also used as the TDE wallet password.

2. Enter the Active Database credentials:
  - **Admin Password**
  - **Wallet Password**

3. Click Next.

**Enter Application Tier Information:**

1. Define your zones in the Zone region.


   Note that you can have multiple zones across subnets. You can configure your environment such that you functional redirection per zone is in accordance with functional affinity.

   Also, you can have a load balancer shared between multiple zones of the same type. This configuration allows for two separate URLs to resolve to the same IP address and the shared load balancer will target one backend set or another.

   Note too that you have flexibility in your configuration. One zone, Zone A, can have one load balancer assigned to it, while another two zones, Zone B and Zone C, can have a second load balancer assigned to them.

   Define your internal zone first.

   Enter values for the following properties:
2. In the Web Entry Point region, enter values for the following properties:

- **Web Entry Type**: Choose one of the following: New Load Balancer (LBaaS), Manually Configured Load Balancer to select a manually deployed existing load balancer, or Application Tier Node to choose the primary application tier as the entry point.

- **Load Balancer Shape**: If you are using LBaaS, select the load balancer shape. For example: 100Mbps

- **Protocol**: Select the protocol for access to the environment, either http or https.

- **Hostname**: Enter the hostname for your web entry point. For example: myhost

- **Domain**: Enter the domain for your web entry point. For example: example.com

- **Port**: Select the port for your web entry point. If there is no load balancer, then the port is automatically populated depending on the protocol: 8000 for http and 4443 for https. Otherwise, select the appropriate port for use with your load balancer, such as 80 for http or 443 for https. Note that to allow access to the Oracle E-Business Suite login URL, your network administrator must define an ingress rule in the load balancer security list. See Create Network Resources For Deploying Oracle E-Business Suite Instances, page 3-9.

3. For Storage, choose the **File System Type**: Non-Shared or Shared.

   If you choose Shared, then the storage is shared across all nodes in your network. You must enter a value for the Block Volume Storage field for the first node under Application Tier Nodes. This storage is then shared across all nodes, so you do not enter in storage values for your subsequent nodes. In addition, after you save your first zone with Shared storage, any subsequent zones will also be defined with Shared storage automatically.

   **Important**: You must ensure you specify enough storage for your nodes. Refer to Oracle E-Business Suite Installation Guide: Using Rapid Install [https://docs.oracle.com/cd/E26401_01/doc.122/e22950/toc.htm] for guidelines on space usage.

   If you choose Non-Shared, you must specify a value for the Block Volume Storage field for every node in the Application Tier Nodes field.

4. In the Logical Host region, enter values for the following properties:
• **Logical Host Option**: Choose *Automatic* or *Manual*.

• **Logical Hostname Prefix**: If you chose Automatic, enter your desired hostname prefix.
  
  You do not need to enter this if you chose Manual for your logical host option, but you will be prompted for the Logical Hostname for your nodes in the Application Tier Nodes region.

• **Logical Domain**: Enter the logical domain.

5. In the **Application Tier Nodes** region, enter properties for each node.

   Note that you can define a specific shape for each application tier node.

   • **Logical Hostname**
   
   • **Logical FQDN**
   
   • **Shape**: Select the shape. For example: *VM.Standard2.1* - (1 OCPU, 15 GB RAM)
   
   • **Block Volume Storage**
   
   • **Fault Domain**: Select the fault domain. Refer to Fault Domains [https://docs.cloud.oracle.com/en-us/iaas/Content/General/Concepts/regions.htm#fault] for more information.

6. Click **Save Zone** to save your zone definition.

7. Define additional zones using the **Add Zone** button.

8. When you have completed adding your zones, click **Next**.

**Specify Your Extensibility Options:**

You can optionally extend the provisioning activity to meet your own requirements. By default, Oracle E-Business Suite Cloud Manager follows a standard activity plan for provisioning. However, Oracle E-Business Suite Cloud Manager administrators can also create extended activity plans that include additional tasks as part of the provisioning activity. In this case you can select the appropriate extended activity plan for Oracle E-Business Suite Cloud Manager to follow when provisioning your environment. If you select an extended activity plan, you may need to enter values for input parameters required by the additional tasks in that plan.

**Additional Information**: For more information on using the Extensibility Framework to extend activity plans, see Set Up the Extensibility
Additionally, whether you are using the standard provisioning activity plan or an extended activity plan, you can choose to have Oracle E-Business Suite Cloud Manager pause at specified points during the provisioning activity. For example, if you want to perform your own validations after a particular phase before allowing Oracle E-Business Suite Cloud Manager to proceed to the next phase, you can add a pause at that point. You can then resume the provisioning activity when you are ready to proceed. See Monitor Activity Status, page 12-1.

Define Your Activity Plan
1. Optionally select an extended activity plan for provisioning your environment in the Activity Plan field.
2. In the Task Parameters tab, specify any parameter values required for the additional tasks in the plan. Some parameters may include default values, which you can override as needed.

Define Your Activity Plan Details
3. Click the Activity Plan Details tab. This tab displays a list of the phases in the activity plan and the tasks within each phase.
4. To specify that Oracle E-Business Suite Cloud Manager should pause its processing before a particular phase, click the Actions icon next to that phase, and then select Add Pause.

    Note: Pauses occur before the phase at which they are defined.

5. Click Next.

Enter SSH Keys:
Optionally upload SSH keys for users.

    Note: You cannot add keys after the promotion process is completed.

1. Click Add Key.
2. Specify the tiers for the SSH key. Choose All Tiers, Application Tier, or Database Tier.
3. Specify the pertinent OS User type. Choose All Users, Operating System Administrator, or Application Administrator.
4. Upload the SSH key file. The file name will default in.

5. The system will validate the SSH key. Click **Next** to continue.

**Review Your Promotion Details:**
1. Review the installation details; database details; application tier details, including zones; activity plan details, and SSH key information.

2. To promote your environment, click **Submit**.

3. You can check the status of the activity to promote the environment in the Activities page.

**Post-Promotion Steps:**
1. After the standby environment has been promoted, run the following cleanup script on the source database server to clean up the local configuration.

```
$ RemoteClone/bin/db-standby-cleanup.sh --context-file <absolute path to DB context file> --standby-name <standby name> --oci-private-key-file <absolute path to key file> --ebs-username <ebs username>
```

**Delete an Oracle E-Business Suite Environment**

You can delete environments that you no longer need in order to make those resources available for other uses. The Delete option is available for environments with the statuses Successful, Aborted, and Failed. It is not available for an environment for which the Last Activity status is "In Progress" on the Environments page. In addition, the Delete option is not available while a backup of the environment is being taken.

The Delete option is available for environments on all Cloud Database Service options: Compute, Virtual Machine DB System, and Exadata Cloud Service.

**Prerequisites**

- To perform the steps in this section, you must have an Oracle E-Business Suite environment on Oracle Cloud Infrastructure created in Oracle E-Business Suite Cloud Manager using One-Click Provisioning, page 9-6, Advanced Provisioning, page 9-8, or Clone an Oracle E-Business Suite Instance, page 11-5.

**Delete a Standard Environment:**

Follow these instructions to delete a standard environment.

**Important:** Environment deletion is irreversible. Use caution with this
feature.

Backups created from an environment that is subsequently deleted remain, and can still be utilized.

For environments that were not provisioned successfully, this procedure cleans up the resources of incomplete installations.

1. From the Oracle E-Business Suite Cloud Manager Environments page, click the Action icon for an environment with its Last Activity status shown as Successful, Aborted, or Failed, then select Delete. Alternatively, from the environment details page for a specific environment, click Action and select Delete.

2. In the confirmation window, select Yes.

3. You can check the status of the activity to delete the environment in the Activities page. See: Monitor Activity Status, page 12-1.

Deletion of an environment will delete the associated load balancer only if the service has only one backend set which was created by the Oracle E-Business Suite Cloud Manager.

**Delete a Standby Environment:**

You can delete a standby environment from within Oracle Applications Manager, but not within Oracle E-Business Suite Cloud Manager. You cannot delete a standby environment that has an "In Progress" status.

1. Navigate to the Oracle Cloud Infrastructure page within Oracle Applications Manager.

2. Click on the name of the standby environment you wish to delete.

3. Click Remove Standby in the Standby Environment Configuration on Oracle Cloud Infrastructure page.

4. After the standby environment has been deleted, run the following cleanup script on the source database server to clean up the local configuration.

```bash
$ RemoteClone/bin/db-standby-cleanup.sh --context-file <absolute path to DB context file> --standby-name <standby name> --oci-private-key-file <absolute path to key file> --ebs-username <ebs username>
```
Monitor Activity Status

This chapter covers the following topics:

- Monitor Activity Status

Monitor Activity Status

You can monitor the status of an activity performed within Oracle E-Business Suite Cloud Manager to check its progress, resume a paused activity, and retry a failed activity if necessary. Each activity comprises multiple phases, including prevalidation phases and main execution phases. A phase can include one or more tasks. For each phase and task, you can view the overall status as well as a detailed log.

You can monitor the following types of activities:

- **create-ebs** - Provisioning an Oracle E-Business Suite environment.
- **cleanup** - Deleting a previously provisioned Oracle E-Business Suite environment or cleaning up resources of an incomplete installation from an unsuccessful provisioning attempt.
- **add-apptier-nodes** - Adding application tier nodes to an Oracle E-Business Suite environment.
- **delete-apptier-nodes** - Deleting application tier nodes from an Oracle E-Business Suite environment.
- **attach-backup-policy** - Attaching a backup policy to an Oracle E-Business Suite environment.
- **create-ossbackup** - Creating a backup of a previously provisioned Oracle E-Business Suite environment.
• cleanup-backup - Deleting a backup of an Oracle E-Business Suite instance that was stored on Oracle Cloud Infrastructure.

• create-ebs-vms - Creating the VMs for an Oracle E-Business Suite standby environment.

• validate-standby-network - Validating the network defined for an Oracle E-Business Suite standby environment.

• setup-standby - Creating an Oracle E-Business Suite standby environment.

• promote-standby - Promoting an Oracle E-Business Suite standby environment to a production environment.

• delete-standby - Deleting an Oracle E-Business Suite standby environment.

• create-network-profile - Creating a network profile. Activities of this type are displayed only if you are logged in as an Oracle E-Business Suite Cloud Manager administrator.

If you added pauses in the activity plan for an activity such as provisioning, cloning, or promoting a standby environment, then Oracle E-Business Suite Cloud Manager stops its processing at the specified point. For example, you can pause an activity if you want to perform your own manual validations after a particular phase before allowing Oracle E-Business Suite Cloud Manager to proceed to the next phase. You can then resume the activity when you are ready to proceed.

If an activity fails, you can review the log for the specific task that failed to help you resolve the problem before you retry the activity. When you retry an activity, depending on the task that failed, Oracle E-Business Suite Cloud Manager may either continue the activity from the point of failure or clean up the previous attempt and restart the activity from the beginning.

• Review Activity Status, page 12-2

• Resume a Paused Activity, page 12-5

• Retry a Failed Activity, page 12-6

Review Activity Status:
1. To review activity status, click the Navigator icon, and then select Activities.

   Note: Alternatively, you can review a list of the activities performed for a particular environment in the environment details page for that environment. See Review Environment Details, page 10-6.
You can also review the history of all activities related to an environment by navigating to the subdirectory for that environment within the out directory (/u01/install/APPS/apps-unlimited-ebs/out/ <environment_name>/). Within the environment directory, look for the subdirectory that begins with the activity type you are interested in reviewing and the timestamp when the activity was performed.

2. The Activities page lists the most recent activity of each type for each Oracle E-Business Suite environment you have provisioned or attempted to provision, and for each backup. Activities are listed in order by start time. If you are logged in as an Oracle E-Business Suite Cloud Manager administrator, then the page also lists the most recent activity for each network profile.

You can optionally enter a full or partial value in the search field to display only activities whose properties contain that value. You can search by the following properties shown in this page:

- Activity name
- Environment name or network profile name
- User who initiated the activity
- Action being performed
- Status, either Input Validation in Progress, Scheduled, In Progress, Paused, Successful, Failed, Aborted, or Missed
- Start time, if applicable
- End time, if applicable

3. When you first submit an activity, its status is set to Input Validation in Progress. After the validation is completed, if the processing engine is available to start performing the activity, the activity status changes to In Progress. If the processing engine is not immediately available, the activity status is first set to Scheduled and then changes to In Progress later when the processing engine starts performing the activity.

If you added a pause before a particular phase of a provisioning or cloning activity, then when the activity reaches that point, the activity status changes to Paused. After you have performed any necessary manual action, you can resume the activity. The activity then returns to the In Progress status. See Resume a Paused Activity, page 12-5.
When an activity is in progress, continue monitoring it until the activity is completed and its status is set to either **Successful** or **Failed**.

**Note:** If a mailer is configured for your Oracle E-Business Suite Cloud Manager, then the mailer sends you an email message to notify you when a `create-ebs`, `clone-snapshot`, or `cleanup` activity that you submitted is completed successfully. Email messages are not sent for other types of activities.

Alternatively, you can intentionally abort in-progress activities by stopping the Oracle E-Business Suite Cloud Manager VM services with the `stopall force` options. When you restart the services, activities that were previously in progress are changed to the status **Aborted**. See Abort Running Jobs, page 4-14.

**Note:** A scheduled backup activity can be run only when no other activity is being performed for that environment.

- If two backups are scheduled at the same time for the same environment, then Oracle E-Business Suite Cloud Manager only runs one backup activity at that time. The status for the other scheduled backup activity is marked as **Missed**.

- If a backup is scheduled to be created at a certain time but another activity is already running for the environment at that time, such as adding or deleting a node, cloning, or another backup, then the scheduled backup is not created and the status of the scheduled backup activity is set to **Missed**.

You cannot retry a missed activity directly. However, you can schedule another backup or manually create another backup for the environment if necessary. See Schedule Backups, page 11-14 and Create a Backup of a Cloud-Based Oracle E-Business Suite Instance, page 11-11.

4. For activities with a status of **In Progress**, **Paused**, **Successful**, **Failed**, **Aborted**, or **Missed**, click the activity name link to navigate to the Activity Details page.

Alternatively, you can navigate to the Activity Details page for an environment-related activity by clicking the activity status link in the Environments page or the activity name link in the environment details page.

5. In the Activity Details page, you can review the following activity properties:

   - Activity name

   - Environment name or network profile name
• User who initiated the activity
• Prevalidation status
• Execution status

Note: For a status of Failed, click the task link included in the status to review the specific task at which the failure occurred.

• Execution start time, if applicable
• Execution end time, if applicable
• Activity plan that defines the phases and tasks in the activity

6. The Activity Details page also displays a list of the phases and tasks that make up the activity, including prevalidation and main execution.

After Oracle E-Business Suite Cloud Manager starts performing a phase or task, the task list displays an icon indicating its status of the phase or task and a log icon that you can click to view the log details.

7. To refresh the information in the Activity Details page automatically, click the Auto Refresh toggle switch. When Auto Refresh is on, the page refreshes every four minutes and displays the date and time of the last refresh.

8. If an activity fails, click Download Logs to download the complete activity logs. You can review the log details to help you resolve the problem before you retry the activity. See Retry a Failed Activity, page 12-6.

Resume a Paused Activity:

1. If you added a pause before a particular phase of an activity such as provisioning, cloning, or promoting a standby environment, then when the activity reaches that phase, the activity status changes to Paused. At this point, you can perform any manual action that you choose, such as validating the results of the previous phase.

2. When you are ready to proceed to the next phase in the activity plan, navigate to the Activity Details page for the activity and click Resume.

Note: You cannot resume activities with any status other than Paused.
Retry a Failed Activity:

1. To retry a failed activity, navigate to the Activity Details page for the activity and click Retry.

   Note: You cannot retry activities with any status other than Failed.

2. When you retry an activity, Oracle E-Business Suite Cloud Manager marks the original failed activity as the parent of the newly initiated child activity. For a child activity, the Activities page and the Activity Details page both display a Parent Activity link along with the other activity properties. Click the Parent Activity link to navigate to the Activity Details page for the parent activity.

3. Similarly, for a parent activity the Activity Details page displays a Child Activity link which you can click to navigate to the Activity Details page for the child activity.

   Note that you can only retry a particular failed activity once, so after you have retried the activity, the Retry action is disabled for that activity. Instead, monitor the status of the child activity to track its progress. If the child activity also fails, you can choose Retry for the child to try again.

4. Alternatively, if an attempt to create an environment or a backup was unsuccessful and you no longer want to continue, you can also choose to delete the incomplete installation or the incomplete backup to clean up any resources from it instead of retrying the activity. See Delete an Oracle E-Business Suite Environment, page 11-26 and Delete a Backup, page 11-18.
Tasks in the Extensibility Framework

This appendix covers the following topics:

- Seeded Tasks in the Extensibility Framework
- Custom Task Scripts in the Extensibility Framework

Seeded Tasks in the Extensibility Framework

Oracle E-Business Suite Cloud Manager provides the following seeded tasks that you can add to extended activity plans in the Extensibility Framework.

Table A-1 - Seeded Tasks

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run AutoConfig on R12.2 Application Tier nodes</td>
<td>Stops the application tier services, runs Autoconfig, and brings the application tier services back up.</td>
</tr>
<tr>
<td>Run AutoConfig on R12.1 Application Tier nodes</td>
<td>Stops all application tier services, runs Autoconfig, and brings the application tier services back up.</td>
</tr>
<tr>
<td>Change database archive mode on R12.2 environments</td>
<td>Changes the database archive mode on R12.2 environments. All application tier services are restarted.</td>
</tr>
<tr>
<td>Change database archive mode on R12.1 environments</td>
<td>Changes the database archive mode on R12.1 environments. All application tier services are restarted.</td>
</tr>
<tr>
<td>Task Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Change database administrator users passwords on R12.2 environments</td>
<td>Changes the following database users passwords SYS, SYSTEM, DBSNMP. All application tier services are restarted.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> When you submit an activity that includes this task, ensure that the password you specify for the SYS user includes at least one special character. However, do not include the @ character in a password.</td>
</tr>
<tr>
<td>Change database administrator users passwords on R12.1 environments</td>
<td>Changes the following database users passwords SYS, SYSTEM, DBSNMP. All application tier services are restarted.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> When you submit an activity that includes this task, ensure that the password you specify for the SYS user includes at least one special character. However, do not include the @ character in a password.</td>
</tr>
<tr>
<td>Change APPS password on R12.2 environments</td>
<td>Changes the APPS password on R12.2 environments. All application tier services are restarted.</td>
</tr>
<tr>
<td>Change APPS password on R12.1 environments</td>
<td>Changes the APPS password on R12.1 environments. All application tier services are restarted.</td>
</tr>
<tr>
<td>Change Oracle Forms mode from Servlet to Socket on R12.1 environments</td>
<td>Changes Oracle Forms mode from Servlet to Socket on R12.1 environments, it runs an implicit AutoConfig. All application tier services are restarted.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> When you submit an activity that includes this task, ensure that you specify a port number higher than 1024 for the Forms port. This port should be free and should not be used for any other purpose.</td>
</tr>
<tr>
<td>Task Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Configure Oracle OHS PID and LOCK directory paths on R12.1 environments</td>
<td>Configures Oracle OHS PID and LOCK directory paths. All application tier services are restarted. AutoConfig variables s_web_pid_file and s_lock_pid_dir are set, Autoconfig is executed and all application tier Services are restarted.</td>
</tr>
<tr>
<td>Start Application Tier services for R12.2 environments</td>
<td>Starts all application tier services in all nodes of a R12.2 environment</td>
</tr>
<tr>
<td>Start Application Tier services for R12.1 environments</td>
<td>Starts all application tier services in all nodes of a R12.1 environment</td>
</tr>
<tr>
<td>Install RPM from Oracle central yum repository</td>
<td>Installs the given RPM from Oracle central yum repository</td>
</tr>
<tr>
<td>Create a new WebLogic Monitor user</td>
<td>Creates a new WebLogic Monitor user on EBS R12.2 environments</td>
</tr>
<tr>
<td>Enable license for products</td>
<td>Enables licensing for products determined by the end-user</td>
</tr>
<tr>
<td>Run Online Patching fs-clone phase on R12.2 environments</td>
<td>Runs Online Patching fs-clone phase on R12.2 environments</td>
</tr>
<tr>
<td>Grant EM Monitoring role to a database user</td>
<td>Grants the role em_oam_monitor_role to DBSNMP and to a specified user</td>
</tr>
<tr>
<td>Change sysadmin user password</td>
<td>Changes the sysadmin user password</td>
</tr>
<tr>
<td>Install Oracle Support Analyzers</td>
<td>Installs Oracle Support Analyzers</td>
</tr>
</tbody>
</table>

**Custom Task Scripts in the Extensibility Framework**

The Extensibility Framework lets you extend the activities performed by Oracle E-Business Suite Cloud Manager by adding tasks to meet your own requirements. If you create your own task, you must develop a script that defines the processing performed in the task. Follow these guidelines to develop your custom task script.

   - Parse input parameters, page A-8.
• Invoke other programs, page A-9.
• Source other scripts, page A-10.
• Run dos2unix (Windows only), page A-20.


For more information, see the following references.
Set Up the Extensibility Framework, page 8-8
Create a Task, page 8-10

Create a Wrapper Script

Each custom task that you want include in Oracle E-Business Suite Cloud Manager activities must have a wrapper script. The wrapper script is a shell script that contains the top-level definition of the processing performed in the task. When you create the task in the Extensibility Framework UI, you specify this script in the **Script to Run** field.

The file name for the wrapper script can only contain alphanumeric characters and must end with the file extension `.sh`.

The wrapper script can parse any input parameters specified for the task, access environment variables, and invoke other types of programs or source other scripts as appropriate for your processing. Except for certain programs available in all Oracle E-Business Suite environments, all the code invoked by the wrapper script must be included together with the wrapper script in a single source code library zip file for the task.

Example Wrapper Script

The following sample code shows an example of a wrapper script for a custom task. In this example, the task is to register a custom schema. This task requires the following input parameters:

• **appsPassword** - The password for the APPS user, considered a sensitive parameter

• **systemPassword** - The password for the SYSTEM user, considered a sensitive parameter

• **appsUser** - The user name for the APPS user, not considered a sensitive parameter
• **schemaName** - The name of the custom schema to register, not considered a sensitive parameter

  **Note:** For this script to succeed, the custom schema being registered must have the `CREATE SESSION` privilege.
#!/bin/bash
#
+=======================================================================
++++
# |
# | Copyright (c) 2020 Oracle and/or its affiliates.
# |               All rights reserved.
# |
+=======================================================================
++++
# |
FILE:
example/extensible_task/RegisterCustomSchema/registerCustomSchema.sh
# |
+=======================================================================
++++
# |
DESCRIPTION: This script calls $AD_TOP/patch/115/sql/ADZDREG.sql with required
# |
input parameters.
# |
USAGE     : { echo 'appsPassword=<apps schema password>'; echo
'systemPassword=<system user password>'; } |
sh registerCustomSchema.sh appsUser=<apps user
name> customSchemaName=<custom schema>
# |
+=======================================================================
++++
# |
Helper Function definitions
# |
+=======================================================================
++++
# Function to exit from a single point
function exitMain(){
  exit 1
}
# Function to exit with 0
function exitSuccess(){
  exit 0
}
function exitWithUsage(){
  echo "Usage : { echo 'appsPassword=<apps schema password>'; echo
'systemPassword=<system user password>'; } | sh registerCustomSchema.sh
appsUser=<apps user name> customSchemaName=<custom schema>"
  exitMain
}
# |
+=======================================================================
++++
# Main Script & Argument Parsing
# |
+=======================================================================

### NON Sensitive Parameter Parsing

Parse through the argument list each argument in form `<argument-name>=<value>`

```bash
function getNonSensitiveParameters()
{
  for i in "@"
    do
      key=`{ echo "$i"; } | awk -F '=' '{print $1}'`;
      value=`{ echo "$i"; } | awk -F '=' '{print $2}'`;
      # In task-definition - parameter names are "appsUser" and "customSchemaName"
      if [[ "$key" == "appsUser" ]]; then
        appsUser=$value;
      elif [[ "$key" == "customSchemaName" ]]; then
        customSchemaName=$value;
      else
        echo "Incorrect arguments password for Non Sensitive Parameters"
        exitWithUsage
      fi
    done
}
```

### Sensitive Parameter Parsing

Get the CONTEXT_FILE Environment variable

```bash
function getSensitiveParameters()
{
  while read key_password;
    do
      user_key=`{ echo "$key_password"; } | awk -F '=' '{print $1}'`;
      # In task-definition - parameter names are "appsPassword" and "systemPassword"
      if [[ "$user_key" == "appsPassword" ]]; then
        appsPwd=`{ echo "$key_password"; } | awk -F '=' '{print $2}'`;
      elif [[ "$user_key" == "systemPassword" ]]; then
        systemPwd=`{ echo "$key_password"; } | awk -F '=' '{print $2}'`;
      else
        echo "Incorrect arguments password for Sensitive Parameters"
        exitWithUsage
      fi
    done
}
```
Parse Input Parameters

When you create the task in the Extensibility Framework UI, you can specify input parameters required for the task. Oracle E-Business Suite administrators provide the values for these parameters when they submit an activity that includes this task.

You can optionally specify default values for these parameters when you create the task. An administrator can override the default values if necessary when submitting the activity.

Additionally, when you create the task, you can specify whether a parameter is considered sensitive or not. The values for sensitive parameters are masked in display in the UI, and are handled separately in processing from parameters that are not sensitive. Sensitive parameter values are passed to the wrapper script through stdin, while values for parameters that are not sensitive are passed as command line arguments.

When the parameter values are passed to the script, the order of the parameters is maintained, and each value is prefixed with the parameter name specified in the task definition, to ensure that each expected parameter has a corresponding value. The wrapper script should read and split the STDIN for sensitive parameters and the command line arguments for parameters that are not sensitive, using the field separator =, to obtain the parameter values.

For examples of how to parse input parameters, review the parameter sections of the example wrapper script.
Access Environment Variables

When you create the task in the Extensibility Framework UI, you can specify whether the task is to be run from all nodes, all database nodes, all application tier nodes, or only the primary application tier node. Before running the wrapper script for a task, the Extensibility Framework sources the environment appropriate for the nodes where the task is being run. For database nodes, the database environment file is sourced, and for application tier nodes, the application environment file is sourced. For Oracle Database 12c or 19c, the pluggable database (PDB) environment file is sourced. Consequently, you can access environment variables such as $CONTEXT_FILE or $APPL_TOP as usual in a shell script.

Because the environment is already sourced, the script can access the variables in the following format: $<variable_name>

For example, you can use the $CONTEXT_FILE variable to access the context file. As another example, if you want to start the admin server by running the adstrtal.sh script, you can use the $ADMIN_SCRIPTS_HOME variable to access the script in that directory:

```
{ echo $apps_user; echo $apps_pwd; echo $wls_pwd; } | sh
$ADMIN_SCRIPTS_HOME/adstrtal.sh -nopromptmsg
```

You can also use a function to retrieve an environment variable value. The following example shows how to get the AD_TOP environment variable using a function:

```bash
function getADTOPFromEnv(){
    echo $AD_TOP
}
```

The following example shows how to subsequently assign the value of the environment variable:

```bash
adTop=$(getADTOPFromEnv)
```

Invoke Other Programs

From the top-level wrapper script, which is a shell script, you can invoke different types of programs to perform the detailed processing for the task. For example, you can call SQL files, other shell scripts, Perl files, Java programs, and others.

The program file called from the wrapper script must be present in the specified location. Additionally, you must call the programs in non-interactive mode; that is, all the required parameters are passed to the program.

The following examples show sample code for calling a few types of programs. You can use similar code to call other types of programs not specifically shown here, such as Python files.

The following example shows sample code for calling a SQL file:

```
sqlplus -S apps/$appsPwd @$adTop/patch/115/sql/ADZDREG.sql $systemPwd $appsUser $customSchemaName
```

You can invoke another shell script using the `sh` command. The following example
shows sample code for calling a shell script. In this example, the variable \$apps_user has already been evaluated to the APPS user, the variable \$apps_pwd has already been evaluated to the password for the APPS user, and the variable \$wls_pwd has already been evaluated to the Oracle WebLogic Server password.

```bash
{ echo \$apps_user; echo \$apps_pwd; echo \$wls_pwd; } | sh
$ADMIN_SCRIPTS_HOME/adstrtal.sh -nopromptmsg
```

All the dependent Perl modules required to run a Perl file are available within the main script that Oracle E-Business Suite Cloud Manager uses to process activities. The following example shows sample code for calling a Perl file:

```bash
{ echo \$apps_pwd; } | $FND_TOP/bin/txkrun.pl -script=ChangeFormsMode -contextfile=$CONTEXT_FILE -mode=socket -runautoconfig=yes -port=$socketPort
```

If you want to call a Java program, that Java program must be in the CLASSPATH in your environments. Java and its dependent libraries are available for the main script to run the command. The following example shows sample code for calling a Java program:

```bash
{ echo \$apps_pwd; } | java -classpath .:$CLASSPATH oracle.apps.ad.licmgr.bobj.InstallProduct \$fndnam \$APPL_TOP "$products" \$apps_jdbc_url \$CONTEXT_FILE
```

**Source Other Scripts**

From the wrapper script, you can call a function from another shell file. You must first source the other shell file with its relative path. The following example shows sample code for sourcing another shell file:

```bash
source ./commonHelper.sh
```

In this example, the `commonHelper.sh` script is in the same directory as the script in which it is used.

The `commonHelper.sh` script is used in seeded tasks provided by Oracle. The common libraries that are used in these tasks are written as functions in the `commonHelper.sh` script. You can use this script as a reference to write your custom scripts. The following sample code shows the contents of the `commonHelper.sh` script.
#!/bin/bash
#
+=======================================================================+===+
# | Copyright (c) 2020 Oracle and/or its affiliates. All rights reserved.
# |
+=======================================================================+===+
# | FILE : example/extensible_task/RegisterCustomSchema/commonHelper.sh
# |
+=======================================================================+===+
# | DESCRIPTION: This script is used to provide utility methods to runtime scripts
# | USAGE      : This file is sourced by seeded tasks and acts like a library
# |
+=======================================================================+===+

# Global variables
SYSTEM_USER(system)
RETURN_FALSE=1
RETURN_TRUE=0
RETURN_NULL=""
APP_NODE_TYPE="app"
DB_NODE_TYPE="db"

# Function to exit from a single point
function exitMain(){
    exit $RETURN_FALSE
}

# Function to exit with 0
function exitSuccess(){
    exit $RETURN_TRUE
}

# Function to check if the variable passed is empty
function isNull(){
    retCode=$RETURN_FALSE
    if [ -z "$1" ]; then
        retCode=$RETURN_TRUE
    fi
    return $retCode
}

# Function to convert a variable to lower case
function convertToLower()=>
    var=$1
    echo $var | tr '[[:upper:]]' '[[:lower:]]'

# Function to Check if $CONTEXT_FILE exists or not
function checkForContextFile(){
retCode=$RETURN_FALSE

    if [ -f "$CONTEXT_FILE" ]; then
        retCode=$RETURN_TRUE
    fi

    return $retCode

# Check if sqlplus exist
function checkIfSqlPlusExist()
{
    retCode=$RETURN_FALSE
    sqlplus_path=$(which sqlplus)
    if [ "$?" -eq "$RETURN_TRUE" ]; then
        if [ -f "$sqlplus_path" ]; then
            retCode=$RETURN_TRUE
        fi;
    fi
    return $retCode
}

# Get the value from $CONTEXT_FILE
function getCtxValue()
{
    ctxVar=$1
    ctxVal=$(grep "$ctxVar" $CONTEXT_FILE | sed "s/\.*$ctxVar[^>\.*]\([^<]*\)<.*/\1/g; s/ *$//g"
    echo $ctxVal
}

# If the File edition is run returns true else false
function isRunFileSystem()
{
    retCode=$RETURN_FALSE
    file_edition_type=$(getCtxValue s_file_edition_type)
    isNull $file_edition_type
    if [ "$?" -ne "$RETURN_TRUE" ]; then
        if [[ "$file_edition_type" -eq "run" ]]; then
            retCode=$RETURN_TRUE
        fi
    fi
    return $retCode
}

# Get apps version, returns empty if not found
function getAppsVersion()
{
    version=$RETURN_NULL
    apps_version=$(getCtxValue s_apps_version)
    isNull $apps_version
    if [ "$?" -ne "$RETURN_TRUE" ]; then
        version=$apps_version
    fi
    echo $version
}

# Gets the nodeType
# Returns app/db/empty string
function getNodeType(){
    node_type=$RETURN_NULL

    context_type=$(getCtxValue s_contexttype)

    if [ "?" -eq "$RETURN_TRUE" ]; then
        echo "CONTEXT_FILE may have missing or NULL entry for s_contexttype."
        echo "Please check if the CONTEXT_FILE is corrupted"
    else
        if [[ "${context_type}" == "APPL_TOP Context" ]]; then
            node_type=$APP_NODE_TYPE
        else
            node_type=$DB_NODE_TYPE
        fi
    fi

    echo $node_type
}

# Gets the apps user name from context_file if exists else returns empty string
function getAppsUser()
{
    apps_user=$(getCtxValue s_apps_user)
    echo $apps_user
}

# Function to return value if key received is same as in keyvalue pair
# Otherwise returns empty string
# Example : keyValuePair : apps_password=<apps credentials>
#           keyReceived  : apps_password
function getInputValue()
{
    keyValuePair=$1
    keyReceived=$2
    value=$RETURN_NULL

    key=${{ echo "$keyValuePair"; | awk -F '=' '{print $1}' }}
    if [[ "${key}" == "$keyReceived" ]]; then
        value=${{ echo "$keyValuePair"; | awk -F '=' '{print $2}' }}
    fi

    echo $value
}

# Read apps password from stdin, format of the input :
# apps_password=value
function getAppsPassword()
{
    read apps_password
    password=$(getInputValue $apps_password "apps_password")
    echo $password
}

# Connect with apps user and apps password
function validateAppsPassword() {
    apps_user=$1
    apps_pwd=$2
    retCode=$RETURN_FALSE

isNull $apps_user
if [ "$?" -ne "$RETURN_TRUE" ]; then
isNull $apps_pwd
if [ "$?" -ne "$RETURN_TRUE" ]; then
checkDBConnection $apps_user $apps_pwd
    if [ "$?" -eq "$RETURN_TRUE" ]; then
        retCode=$RETURN_TRUE
    fi
fi
fi
return $retCode
}

# Checks user connection
function checkDBConnection()
{
    user_name=$1
    user_pwd=$2
    retCode=$RETURN_FALSE

    sqlplus -s /nolog > /dev/null 2>&1 <<EOF
    whenever sqlerror exit failure
    connect $user_name/$user_pwd
    EOF
    if [ "$?" -eq "0" ]; then
        retCode=$RETURN_TRUE
    else
        echo "Database connection could not be established. Either the
database is down or the $user_name credentials supplied are wrong."
    fi

    return $retCode
}

# To read system password from stdin, Format : system_password=value
function getSystemPassword()
{
    read system_password
    password=$(getInputValue $system_password "system_password")
    echo $password
}

# Function tries to connect to system user with the password passed
function validateSystemPassword()
{
    system_pwd=$1
    retCode=$RETURN_FALSE

   isNull $system_pwd
if [ "$?" -ne "$RETURN_TRUE" ]; then
    checkDBConnection $SYSTEM_USER $system_pwd
    if [ "$?" -eq "$RETURN_TRUE" ]; then
        retCode=$RETURN_TRUE
    fi
fi

    return $retCode
}

# To read weblogic password from stdin, Format : weblogic_password=value
# Key is weblogic_password and value is password
function getWlsPassword()
{
    read weblogic_password
    password=$(getInputValue $weblogic_password "weblogic_password")
    echo $password
}

# Validate WLS Admin credentials
# ebs-get-serverstatus returns status code of 0 for running mode, 3 is NOT running, 9 Invalid Credentials
function validateWLSAdminCredentials()
{
    wls_pwd=$1
    context_file=$2
    retCode=$RETURN_FALSE
    perl_bin=$(getCtxValue s_adperlprg)
    ad_top=$(getCtxValue s_adtop)
    if [ -f "$perl_bin" ]; then
        if [ -f "$ad_top/patch/115/bin/adProvisionEBS.pl" ]; then
            ( echo $wls_pwd; ) | $perl_bin
            $ad_top/patch/115/bin/adProvisionEBS.pl ebs-get-serverstatus -contextfile=$context_file -servername=AdminServer -promptmsg=hide
            retStatus=""$?
            if [ "$retStatus" -eq "3" ]; then
                echo "Admin Server is NOT running"
            elif [ "$retStatus" -eq "9" ]; then
                echo "Invalid WebLogic Admin Server user credentials supplied."
            elif [ "$retStatus" -eq "$RETURN_TRUE" ]; then
                echo "Validated Admin Server Credentials successfully"
                retCode=$RETURN_TRUE
            else
                echo "Invalid return status from $ad_top/patch/115/bin/adProvisionEBS.pl"
            fi
        else
            echo "ERROR : Not able to find adProvisionEBS.pl file in the PATH."
            echo "Please check if the environment is sourced."
            fi
        else
            echo "Not able to find $perl_bin executable."
        fi
    fi
    return $retCode
}

# Function to check if it is Primary App Node
function isPrimaryAppNode()
{
    retCode=$RETURN_FALSE
    admin_server_status=$(getCtxValue s_adminserverstatus)
    web_admin_status=$(getCtxValue s_web_admin_status)
    if [[ "$admin_server_status" == "enabled" && "$web_admin_status" == "enabled" ]]; then
        retCode=$RETURN_TRUE
    fi
    return $retCode
}
# Starting the Weblogic Admin Server

```bash
function startWLSAdminServer()
{
    apps_pwd=$1
    wls_pwd=$2
    retCode=$RETURN_FALSE
    isPrimaryAppNode;
    if [ "$?" -eq "$RETURN_TRUE" ] ; then
        if [ -f "$ADMIN_SCRIPTS_HOME/adadminsrvctl.sh" ]; then
            { echo $wls_pwd; echo $apps_pwd; }|
            $ADMIN_SCRIPTS_HOME/adadminsrvctl.sh start -nopromptmsg
            if [ "$?" -eq "2" ]; then
                echo "Admin Server is already running"
                retCode=$RETURN_TRUE
            elif [ "$?" -eq "$RETURN_TRUE" ]; then
                echo "Admin Server started successfully"
                retCode=$RETURN_TRUE
            else
                echo "Starting Admin server failed. Please check if valid credentials are passed"
            fi
        else
            echo "Not able to find the adadminsrvctl.sh"
        fi
    else
        echo "Not a Primary Node"
    fi
    return $retCode
}
```

# To check if the Domain is editable or not

```bash
function isDomainEditable()
{
    wls_pwd=$1
    retCode=$RETURN_FALSE
    s_wls_home=$(getCtxValue s_wls_home)
    s_wls_admin_user=$(getCtxValue s_wls_admin_user)
    s_wls_admin_host=$(getCtxValue s_wls_admin_host)
    s_wls_admin_domain=$(getCtxValue s_wls_admin_domain)
    s_wls_adminport=$(getCtxValue s_wls_adminport)
    s_wls_admin_url="$s_wls_admin_host.$s_wls_admin_domain:$s_wls_adminport"
    if [[ ! -z "$s_wls_admin_host" && ! -z "$s_wls_admin_domain" && ! -z "$s_wls_admin_port" && -z "$s_wls_admin_user" ]]; then
        echo "Either one or more of the variables s_wls_admin_host s_wls_admin_domain s_wls_admin_port NULL"
    else
        echo "Please check if environment is sourced"
    fi
}
```
if [-f "${AD_TOP}/patch/115/bin/txkValidateDomainInRC.py"]
  then
    echo $wls_pwd; | java weblogic.WLST
    $AD_TOP/patch/115/bin/txkValidateDomainInRC.py --adminuser=$s_wls_admin_user --verify=domainEditModeEnabled --
    adminurl="${wls_admin_url}" | grep -o 'DomainEditable.*1'
    if [ "$?" -eq "$RETURN_TRUE" ]; then
        echo "Domain is editable"
        retCode=$RETURN_TRUE
    else
        echo "Domain is in editable mode"
        retCode=$RETURN_TRUE
    fi
    else
        echo "Not able to find file txkValidateDomainInRC.py"
        echo "Please check if environment is sourced"
    fi
fi

return $retCode

# Function to shutdown DB on Non RAC Instance
function shutDownNonRacDB()
{
    retCode=$RETURN_FALSE
    sqlplus -s / as sysdba <<END
    whenever sqlerror exit failure rollback;
    shutdown immediate;
    exit;
    END
    if [ "$?" -eq "$RETURN_TRUE" ]; then
        retCode=$RETURN_TRUE
    fi
    return $retCode
}

# Function to startup DB in Mount mode on Non RAC Instance
function startupNonRacDBMount()
{
    retCode=$RETURN_FALSE
    sqlplus -s / as sysdba <<END
    whenever sqlerror exit failure rollback;
    startup mount;
    exit;
    END
    if [ "$?" -eq "$RETURN_TRUE" ]; then
        retCode=$RETURN_TRUE
    fi
    return $retCode
}

# Function to startup DB on Non RAC Instance
function startupNonRacDB()
{
    retCode=$RETURN_FALSE
    sqlplus -s / as sysdba <<END
    whenever sqlerror exit failure rollback;
    startup;
exit;
END
if [ "$?" -eq "$RETURN_TRUE" ]; then
  retCode=$RETURN_TRUE
fi
return $retCode

# Function to open Database on Non RAC Instance
function openNonRacDB()
{
  retCode=$RETURN_FALSE
  sqlplus -s / as sysdba <<END
  whenever sqlerror exit failure rollback;
  alter database open;
  exit;
  END
  if [ "$?" -eq "$RETURN_TRUE" ]; then
    retCode=$RETURN_TRUE
  fi
  return $retCode
}

# Function to get source cdb environment File
# Initially pdb environment is sourced, if required to change passwords/archivelog we need to source cdb environment
# Returns the environment if present otherwise NULL is passed to the caller
function getCDBEnvironmentFile()
{
  cdb_env_file=$RETURN_NULL
  instance_name=$(getCtxValue s_instName)
  host_name=$(getCtxValue s_hostname)
  if [[ -z "$instance_name" || -z "$host_name" ]]; then
    echo "Either or one of the environment variable s_instName, s_hostname is NULL."
  else
    cdb_env_file_path=$ORACLE_HOME"$instance_name"_"$host_name".env
    if ! -f $cdb_env_file_path; then
      echo "Not able to find the cdb_env_file. Please check if pdb environment has been sourced."
    else
      cdb_env_file=$cdb_env_file_path
    fi
  fi
  echo $cdb_env_file
}

# Function to check if storage type is ASM or not
function isStorageTypeASM()
{
  retCode=$RETURN_FALSE
  host_name=$(getCtxValue s_hostname)
  srvctl_path=$(which srvctl)
  if [ "$?" -eq "$RETURN_TRUE" ]; then
    if [ -f "$srvctl_path" ]; then
      ret=$(srvctl status asm -n $host_name | grep -o 'ASM.'
/*running*/
    if [ "$?" -eq "$RETURN_TRUE" ]; then
        retCode=$RETURN_TRUE
    fi
fi;
fi
return $retCode
}

# Function to find if the database is pdb enabled or not
function isPDBEnabled()
{
    retCode=$RETURN_FALSE
    is_pdb_enabled=$(getCtxValue s_pluggable_database)
    if [[ $is_pdb_enabled == true* || $is_pdb_enabled == TRUE* ]]; then
        retCode=$RETURN_TRUE
    fi
    return $retCode
}

# Function to check if RAC is enabled or not on the instance
function isRACEnabled()
{
    retCode=$RETURN_FALSE
    israc=$(getCtxValue s_dbCluster)
    if [[ $israc == true* || $israc == TRUE* ]]; then
        retCode=$RETURN_TRUE
    fi
    return $retCode
}

# Function to get ORACLE_UNQNAME from environment file
function getOracleUnqName()
{
    db_unique_name=$RETURN_NULL
    db_unique_name=$(sqlplus -s / as sysdba <<END
    set feedback off heading off
    select db_unique_name from sys.v$database;
    exit;
    END
    )
    echo $db_unique_name
}

# Function to return password file
function getPasswordFileLocation()
{
    orapw_file=$RETURN_NULL
    isStorageTypeASM
    if [ "$?" -eq "$RETURN_FALSE" ]; then
        # Compute Flows
        orapw_file=$ORACLE_HOME/dbs/orapw$ORACLE_SID
    else
        # Platform Flows
        isPDBEnabled
    fi
}
if [ "$?" -eq "$RETURN_TRUE" ]; then
    # Platform Plugable RAC/Non RAC
dataloc=$(echo $(getCtxValue s_dbhome1) | awk -F '/' '{print $1}')
dataloc=$(getCtxValue s_dbhome1)
dbname=$(getCtxValue s_cdb_name)
orapw_file=$dataloc/$ORACLE_UNQNAME/orapw$dbname
else
    # Non Plugable database. For 11204 Flows
    isRACEnabled
    if [ "$?" -eq "$RETURN_TRUE" ]; then
        orapw_file="$ORACLE_HOME/dbs/orapw$ORACLE_SID"
    else
        # Non RAC
        orapw_file="$ORACLE_HOME/dbs/orapw$ORACLE_SID"
    fi
fi

echo $orapw_file
}

# Script executes SQL file as sysdba
# First argument is FileName and others are parameters
function executeSQL()
{
    retCode=$RETURN_FALSE
    if [ ! -f "$1" ]; then
        echo "Sql file to execute $1 does not exist"
    else
        sqlplus -s / as sysdba @$1 ${@:2}
        if [ "$?" -eq "$RETURN_TRUE" ]; then
            retCode=$RETURN_TRUE
        fi
    fi

    return $retCode
}

Run dos2unix (Windows Only)

If you edit the scripts for your task on Windows, then you may encounter issues with control characters. For example, the following error message indicates a failure caused by a control character:

execution failed with ""/bin/bash^M: bad interpreter: No such file or directory"

To avoid these errors, run the dos2unix command on all the relevant files before you begin packaging the source code for the task. You may need to install dos2unix first if it is not already present on your system. See dos2unix [https://docs.oracle.com/cd/E19683-01/816-0210/6m6nb7m7q/index.html].

For example, the following command runs dos2unix on the example wrapper script:

dos2unix registerCustomSchema.sh

Test the Script

It is recommended that you test your custom script by running directly it on a test
instance before you package it for inclusion in a task definition. Before performing the
test, source the appropriate environment file and make sure that the prerequisites for
the script are present. The following example shows a sample command for testing a
script:

```bash
{ echo 'appsPassword=<apps schema password>'; echo
'systemPassword=<system user password>'; } | sh registerCustomSchema.sh
appsUser=<apps user name> customSchemaName=<custom schema>
```

---

**Package the Script in a Zip File**

When you finish developing the code for your task, you must package the wrapper
script in a zip file together with all its supporting files.

1. Create a directory to hold the code files for the task.
   
   For example, for the task to register a custom schema, you could create a directory
   named `RegisterCustomSchema`.

2. Move the wrapper script for the task into this directory, along with all the
   supporting files on which the wrapper script has a dependency.
   
   For the example task, the wrapper script is `registerCustomSchema.sh`, and it
   has a dependency on the `commonHelper.sh` script for some functions, so you
   would move both these files into the `RegisterCustomSchema` directory.

3. Create a zip file of the entire directory.
   
   The following example shows the zip command to use for the example task:
   ```bash
   zip -r RegisterCustomSchema.zip RegisterCustomSchema/
   ```

4. When you create the task in the Extensibility Framework UI, upload this zip file in
   the **Source Code Library** field. See Create a Task, page 8-10.
Time Zone Support in Oracle E-Business Suite Cloud Manager

Time Zone Support in Oracle E-Business Suite Cloud Manager

When using Advanced Provisioning to provision an environment, or when creating a standby environment, you are prompted for the operating system time zone you want to use for your instance. This appendix describes how default values for the operating system time zone are derived, as well as the implications of overriding the default values.

When taking a backup of an on-premises environment, you will be prompted for the operating system time zone that you wish to use when restoring the backup in Oracle Cloud Infrastructure. This value will be saved as backup metadata in a property called SRC_OS_TIMEZONE.

When provisioning a new environment from a backup, the default value for the operating system time zone is derived based on the following logic:

- The value of the Oracle E-Business Suite profile option Server Timezone (code SERVER_TIMEZONE_ID) is used, if it exists.
- Otherwise, if the Server Timezone profile option is not set, then the default value is derived from the value of the SRC_OS_TIMEZONE property in the backup’s metadata, if it exists.
- Otherwise, if both of the prior values are unavailable, then the default value becomes ‘UTC’.

The following table illustrates some examples of scenarios with the default value for the field Operating system time zone as well as the time zone to be set in Cloud Manager.

In these examples, the user has chosen not to bypass the Server Timezone profile validation.

In this table, the property SRC_OS_TIMEZONE is taken from the backup’s metadata. The
Oracle E-Business Suite profile option Server Timezone is referred to by its code, SERVER_TIMEZONE_ID.

Table B-1 Examples of Time Zone Values for Advanced Provisioning

<table>
<thead>
<tr>
<th>Backup Metadata</th>
<th>Default Value Shown in UI</th>
<th>User-Selected Value</th>
<th>Time Zone to be set on Compute-VM</th>
<th>Time Zone to be set on VMDB</th>
<th>Exadata Infrastructure Time Zone</th>
<th>Time Zone Variable (TZ) to be set on the Exadata Cloud Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRC_OS_TIMEZONE = NOVALUE</td>
<td>UTC</td>
<td>America/New_York</td>
<td>America/New_York</td>
<td>America/New_York</td>
<td>Europe/London</td>
<td>Time zone is America/New_York</td>
</tr>
<tr>
<td>Profile option SERVER_TIMEZONE_ID = NOVALUE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SRC_OS_TIMEZONE = Asia/Kolkata</td>
<td>Asia/Kolkata</td>
<td>Asia/Kolkata</td>
<td>Asia/Kolkata</td>
<td>Asia/Kolkata</td>
<td>Europe/London</td>
<td>Time zone is Asia/Kolkata</td>
</tr>
<tr>
<td>Profile option SERVER_TIMEZONE_ID = NOVALUE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SRC_OS_TIMEZONE = (GMT+05:30) India Time</td>
<td>IST</td>
<td>IST</td>
<td>IST</td>
<td>IST</td>
<td>Europe/London</td>
<td>Time zone is IST</td>
</tr>
</tbody>
</table>
Backup Metadata | Default Value Shown in UI | User-Selected Value | Time Zone to be set on Compute-VM | Time Zone to be set on VMDB | Exadata Infrastructure Time Zone | Time Zone Variable (TZ) to be set on the Exadata Cloud Service
--- | --- | --- | --- | --- | --- | ---
SRC_OS_TIMEZONE = IST | America/New_York | America/New_York | America/New_York | America/New_York | Europe/London | Time zone is America/New_York
Profile option SERVER_TIMEZONE_1D = (GMT - 5) Eastern Time

Note the following:

- In the first example, neither the backup’s metadata nor the profile option has a time zone specified, so the default value is UTC.

- In the second example, the backup’s metadata includes a time zone but the profile option does not; therefore, the metadata’s time zone becomes the default.

- In the third example, the backup’s metadata does not specify a time zone but the profile option does; therefore, the time zone specified by the profile option is used as the default.

- In the fourth example, both the backup’s metadata and the profile option specify a time zone, but different ones. In this case, the Server Timezone profile option takes precedence, and its value becomes the default value.

In the case of environments on an Exadata Cloud Service, where there is one system with many databases on it, Cloud Manager can’t use the operating system time zone for a given environment, but instead uses the time zone defined in the Exadata Cloud Service infrastructure.

Alternatively, you might choose to bypass the Server Timezone profile validation.

In the examples in the following table, the user has chosen to override the default value for the time zone, and has chosen to bypass the validation.
### Table B-2 Examples of Time Zone Values Bypassing Server Time Zone Profile Validation

<table>
<thead>
<tr>
<th>Metadata</th>
<th>Default Value Shown in UI</th>
<th>User-Selected Value</th>
<th>Time Zone to be set on Compute-VM</th>
<th>Time Zone to be set on VMDB</th>
<th>Exadata Cloud Service Infrastructure Time Zone</th>
<th>Time Zone Variable to be set on the Exadata Cloud Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SRC_OS_TIMEZONE = Asia/Kolkata</td>
<td>America/Los_Angeles (Override)</td>
<td>America/Los_Angeles</td>
<td>America/Los_Angeles</td>
<td>Europe/London</td>
<td>Not Set</td>
<td></td>
</tr>
<tr>
<td>Profile option</td>
<td>SERVER_TIMEZONE_ID = NOVALUE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SRC_OS_TIMEZONE = NOVALUE</td>
<td>America/Los_Angeles (Override)</td>
<td>America/Los_Angeles</td>
<td>America/Los_Angeles</td>
<td>Europe/London</td>
<td>Not Set</td>
<td></td>
</tr>
<tr>
<td>Profile option</td>
<td>SERVER_TIMEZONE_ID = (GMT+05:30) India Time</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SRC_OS_TIMEZONE = America/New_York</td>
<td>America/Los_Angeles (Override)</td>
<td>America/Los_Angeles</td>
<td>America/Los_Angeles</td>
<td>Europe/London</td>
<td>Not Set</td>
<td></td>
</tr>
<tr>
<td>Profile option</td>
<td>SERVER_TIMEZONE_ID = (GMT+05:30) India Time</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In the case of environments on an Exadata Cloud Service, where there is one system with many databases on it, Cloud Manager cannot use the operating system time zone...
for a given environment, but instead uses the time zone defined in the Exadata Cloud Service infrastructure. The time zone variable is not set.

In the case of creating a standby environment from an on-premises environment, the default value will be derived based on the Oracle E-Business Suite profile option Server Timezone (code SERVER_TIMEZONE_ID), if it exists. Otherwise, 'UTC' will be used.