Oracle® E-Business Suite

Cloud Manager Guide

Release 24.1.1

Part No. F35809-28

April 2024

Oracle E-Business Suite Cloud Manager Guide, Release 24.1.1

Part No. F35809-28

Primary Author: Clara Jaeckel, Tiffany Morales Romero, Mildred Wang

Contributing Author: Santiago Bastidas, Rama Doodala, Noby Joseph, Prasad Joshi, Sridhar Kulkarni, Saritha Merugu, Biplab Nayak, Shravan Kumar Nethi, Terri Noyes, Manoj Palivela, Sanyukta Palod, Praveen Pappu, Raja Sekhar Putchakayala, Feroz Shaik, Vijay Yarramsetti

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 customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

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

Part 2 Implement 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

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

5 Create a Backup of an On-Premises Oracle E-Business Suite Environment 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 19c or 12.1.0.2 (Commercial Cloud Regions Only)

Part 4 Manage Oracle E-Business Suite Environments Using Oracle E-Business Suite Cloud Manager

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 Discover an Oracle E-Business Suite Instance

11 Oracle E-Business Suite System Administration

12 Oracle E-Business Suite Lifecycle Management

13 Monitor Job Status

A Tasks in the Extensibility Framework

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

Send Us Your Comments

Oracle E-Business Suite Cloud Manager Guide, Release 24.1.1

Part No. F35809-28

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

Welcome to Release 24.1.1 of the *Oracle E-Business Suite Cloud Manager Guide.*

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 xii 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 customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

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 Environment 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 19c or 12.1.0.2 (Commercial Cloud Regions Only)

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 Discover an Oracle E-Business Suite Instance

11 Oracle E-Business Suite System Administration

12 Oracle E-Business Suite Lifecycle Management

13 Monitor Job 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.

- **Oracle E-Business Suite Documentation Web Library** - The web libraries, available on the Oracle Help Center, provide the latest updates to Oracle E-Business Suite documentation for Release 12.2 [https://docs.oracle.com/cd/E26401_01/index.htm] and Release 12.1 [https://docs.oracle.com/cd/E18727_01/index.htm]. Most documents are available in PDF and HTML formats.

- **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.

- **Oracle Electronic Technical Reference Manual -** The Oracle Electronic Technical Reference Manual (eTRM) contains database diagrams and a detailed description of database tables, forms, reports, and programs for each Oracle E-Business Suite product. This information helps you convert data from your existing applications and integrate Oracle E-Business Suite data with non-Oracle applications, and write custom reports for Oracle E-Business Suite products. The Oracle eTRM is available from 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.

Oracle Application Management Pack for Oracle E-Business Suite Metric Reference Manual

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:

- Welcome to Oracle Cloud Infrastructure [https://docs.cloud.oracle.com/en-us/iaas/Content/GSG/Concepts/baremetalintro.htm]

- Developer Tools and 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 any installation and configuration choices that are 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 adop 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.

- For Oracle E-Business Suite Release 12.1, *Oracle E-Business Suite System Administrator's Guide - Configuration* contains information on system configuration steps, including defining concurrent programs and managers, enabling Oracle Applications Manager features, and setting up printers and online help. *Oracle E-Business Suite System Administrator's Guide - Maintenance* provides information for frequent tasks such as monitoring your system with Oracle Applications Manager, managing concurrent managers and reports, using diagnostic utilities, managing profile options, and using alerts. *Oracle E-Business Suite System Administrator's Guide - Security* describes user management, data security, function security, auditing, and security configurations.

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

1

Introduction to Oracle E-Business Suite Cloud Manager

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 (OCI), including provisioning new environments, performing lifecycle management activities on those environments, and restoring environments from on-premises.

Oracle E-Business Suite Cloud Manager is available for use in select commercial and government cloud regions. For certification details, refer to the following sections 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]:

- Regions and Realms
- Cloud Automation Capabilities

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 latest release of the automation (24.1.1) 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, Cloning, and Refresh.

Oracle E-Business Suite Cloud Backup Module

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 Compute 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** - The use of predefined Network Profiles greatly simplifies provisioning for Oracle E-Business Suite Cloud Manager users (DBAs).
  - Network Profiles map compartments with Oracle Cloud Infrastructure network definitions to fulfill Oracle E-Business Suite network requirements.
  - You can either designate regional or availability domain-specific subnets for your Oracle E-Business Suite application tier, database tier, or load balancer.
  - Both network security groups (NSGs) and security lists can be used to control traffic at the packet level.

One-Click Provisioning

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

Select the demo install image in order to conduct demonstrations with example data and explore new features. Oracle Enterprise Command Center (ECC) Framework is included when you choose this option.

Select the fresh install image in order to tailor the resulting environment and data to your specific business needs.

Advanced Provisioning

Oracle E-Business Suite Cloud Manager Advanced Provisioning can be used to provision environments from customer backups. These backups are located in private object storage buckets and must be created by Cloud Manager from environments that it manages, or from on-premises environments using Oracle E-Business Suite Cloud Backup Module.

Alternatively, Advanced Provisioning can provision a Vision demo or fresh installation environment from pre-seeded backups.

> **Note:** To provision Vision demo or fresh install environments from pre-seeded backups using this feature, your Virtual Cloud Network (VCN) must be configured for public internet access, as is the case with commercial cloud regions (either with public subnets, or private subnets using a NAT Gateway).

Advanced Provisioning has the following traits:

- Selection of network topology.
- Support of both single availability domain and multiple availability domain

regions.

- Ability to define logical host names for the application tier and for the database tier running on Compute.

- Ability to choose the operating system for the application tier and for the database tier running on Compute.

- Placement of the database on one of the following: Oracle Cloud Infrastructure Compute Service, Oracle Base Database Service 1-Node DB System, Oracle Base Database Service 2-Node DB System, or Oracle Exadata Database Service on Dedicated Infrastructure.

  The operating system will be determined by the release update level.

- Choice of one or more application tiers, with either a shared (recommended) or non-shared file system. If you choose to deploy a shared file system, the Oracle Cloud Infrastructure File Storage service is automatically configured.

- Choice of one of the following:

  - Deploy Load Balancer as a Service (LBaaS).

  - Use an existing Oracle Cloud Infrastructure load balancer.

  - Use an existing, manually configured load balancer.

  - Configure your application tier node as the web entry point for your Oracle E-Business Suite environment.

- Choice of one or more internal and external zones.

- 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 upload and deploy public SSH keys during provisioning to support secure shell access.

Lift and Shift

Traditional Lift and Shift

The traditional lift and shift contains two phases:

1. In the first phase, you will use the Oracle E-Business Suite Backup Module to back up your on-premises environment to Oracle Cloud Infrastructure object storage.

2. In the second phase, you will use Oracle E-Business Suite Cloud Manager

Advanced Provisioning to provision an environment from that Oracle Cloud Infrastructure object storage backup.

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

Review "4.2.2 Lift and Shift Oracle E-Business Suite from On Premises" 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], for supported releases and mandatory requirements.

Reduced Downtime Lift and Shift (Commercial Cloud Regions Only)

You can create a standby of your on-premises Oracle E-Business Suite installation in Oracle Cloud Infrastructure Compute, and promote that standby to accomplish your lift and shift.

Review "4.2.2 Lift and Shift Oracle E-Business Suite from On Premises" 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], for supported releases and mandatory requirements.

Discovery

Oracle E-Business Suite Cloud Manager provides the capability to discover an Oracle Cloud Infrastructure environment that meets the standards described in My Oracle Support Knowledge Document 2656874.1, *Standards Used by the Oracle E-Business Suite Cloud Manager for Provisioning Oracle E-Business Suite on Oracle Cloud Infrastructure* [https://support.oracle.com/rs?type=doc&id=2656874.1].

Source environments will typically be environments that result from one of the following operations:

- A manual migration from on-premises to Oracle Cloud Infrastructure.
- A platform migration from on-premises to Oracle Cloud Infrastructure.
- An environment initially deployed by Cloud Manager, where either Oracle E-Business Suite or Oracle Database were upgraded.
- An environment initially deployed by Cloud Manager, where any of the following configuration changes were later made:
  - A load balancer was added.
  - A node was added or deleted.
  - The size of the block volume attached to an application or database tier node was increased.

- The File Storage service was manually configured. See My Oracle Support Knowledge Document 2794300.1, *Sharing the Application Tier File System in Oracle E-Business Suite Release 12.2 or 12.1.3 Using the Oracle Cloud Infrastructure File Storage Service*.

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 Service (Compute)
- Oracle Base Database Service 1-Node DB System - Single Instance
- Oracle Base Database Service 2-Node DB System - Oracle RAC
- Oracle Exadata Database Service on Dedicated Infrastructure - Oracle RAC

> **Note:** Oracle Database 12c Release 12.1.0.2 and Oracle Database 11g Release 11.2.0.4 are only available for new provisioning or lifecycle management on the Oracle Base Database and Oracle Exadata Database Services if you have subscribed to the Upgrade Support program. For more information, refer to My Oracle Support Knowledge Document 2996689.1, *Alert: Oracle E-Business Suite Cloud Customers and January 15, 2024 Database Services Desupport for Oracle Database Releases 12.1.0.2 and 11.2.0.4* [https://support.oracle.com/rs?type=doc&id=2996689.1].

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 perform the following:

- Provision a new environment.
- Lift and shift 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:

- Base Database Service 1-Node DB System

- Base Database Service 2-Node DB System
- Exadata Database Service Dedicated

In addition, you have the option to enable TDE for environments provisioned on Compute.

Shapes Supported for Compute Virtual Machines (VMs)

The following shapes are supported for all scenarios in which you can create or add an application tier node, or create a database tier node on Compute:

- VM.Standard.E5.Flex (AMD)
- VM.Standard.E4.Flex (AMD)
- VM.Standard.E3.Flex (AMD)
- VM.Standard3.Flex (Intel)
- VM.Standard2.x

> **Note:** Not all shapes are available in all regions.

These scenarios include: Advanced Provisioning, Adding an Application Tier Node, Cloning, and Standby Deployment (Reduced Downtime Lift and Shift).

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

Shapes Supported for DB Systems

The following shapes are supported by Oracle E-Business Suite Cloud Manager for Advanced Provisioning and Cloning scenarios in which you create a database tier node on a DB System:

- VM.Standard.E4.Flex (AMD)
- VM.Standard.E3.Flex (AMD)
- VM.Standard3.Flex (Intel)
- VM.Standard2.x

> **Note:** Not all shapes are available in all regions.

For more information, see About Virtual Machine DB Systems [https://docs.oracle.

com/en-us/iaas/dbcs/doc/virtual-machine-db-systems.html].

Middleware Licensing Model

You will select either a Bring Your Own License (BYOL) or a Universal Credit Management (UCM) model for middleware licensing when creating your application tier during Advanced Provisioning or Cloning. The same licensing model is used across all application tier nodes in your environment, and this model is inherited when you add a node.

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 Exadata Database Service Dedicated. This feature is not available for Exadata Database Service Dedicated 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 a new environment, 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 cloning capabilities of Oracle Cloud Infrastructure and associated database services.

Oracle E-Business Suite Cloud Manager Cloning is available for environments where the database tier is on Exadata Database Service Dedicated, a Base Database Service DB System, or Compute.

Oracle E-Business Suite Cloud Manager Cloning has the following characteristics:

- **Application Tier**
  - A single logical host name is used for the source and target VMs, reducing the time to clone.
  - For each application tier node, the boot volume is cloned to create the cloned application tier node, preserving the operating system configuration during the clone.
  - If the source environment is configured with a shared file system, the File Storage service volume mounted from the application tier nodes is cloned, and then mounted to the application tier nodes of the target system. For more information on File Storage service cloning, see Cloning File Systems [https://docs.oracle.com/en-us/iaas/Content/File/Tasks/cloningFS.htm].
  - If the source environment is configured with a non-shared file system, all block volumes attached to application tier nodes are cloned and subsequently attached to the target application tier nodes.
  - If you have added additional (custom) block volumes to your application tier nodes, the cloning process will clone these as well.
  - You have the option to choose different shapes for the target application tier nodes.
- **Database Tier on Compute**
  - The source system boot and block volume are cloned to create a new database system, preserving the operating system configuration and database code and data during the clone.
  - A single logical host name is used for the source and target VMs.
  - You have the option to choose a different shape for the target database tier node.
- **Database Tier on a Base Database Service DB System**
  - The Oracle E-Business Suite Cloud Manager Cloning feature for Oracle E-Business Suite with a DB System is available for Release 12.2 and 12.1.3 environments that use either an Oracle 19c or 12c database.

    - Oracle E-Business Suite Cloud Manager relies on the cloning capability of the database service, as described in Clone a DB System [https://docs.oracle.com/en-us/iaas/dbcs/doc/clone-db-system.html].

- **Database Tier on Exadata Database Service Dedicated**
    - The Cloning Using Exadata Snapshots feature provides a method to clone an Oracle E-Business Suite Release 12.2 environment with an Oracle 19c database on Exadata Database Service Dedicated.
    - Cloning Using Exadata Snapshots allows you to create a point-in-time, read-only snapshot of your source database, and then create clones from that snapshot. The cloned databases make efficient use of the space, because only the data that is different from the parent (snapshot) is stored on the disk. These sparse or thin clones are appropriate for non-production purposes such as development and testing.

- **Overall**
    - When creating your cloned environment, you can choose a compartment and a network that differ from that of the source by specifying these in the network profile.
    - You can choose one of the following for the web entry when creating your cloned environment:
        - Deploy Load Balancer as a Service (LBaaS).
        - Use an existing Oracle Cloud Infrastructure load balancer.
        - Use an existing manually configured load balancer.
        - Configure your application tier node as the web entry point.

Create a Backup

You can create backups of environments that meet one of the following criteria:

- The environments were provisioned using Oracle E-Business Suite Cloud Manager Advanced Provisioning.
- The environments were discovered using Oracle E-Business Suite Cloud Manager Discovery.
- The environments were provisioned using Oracle E-Business Suite Cloud Manager One-Click 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.

You have the option to define lifecycle policy rules to specify how a backup is managed in Object Storage after it is created. Using lifecycle policy rules can help you reduce storage costs as well as time taken to manage storage manually. See Using Object Lifecycle Management [https://docs.oracle.com/en-us/iaas/Content/Object/Tasks/usinglifecyclepolicies.htm#Using_Object_Lifecycle_Management] in the Oracle Cloud Infrastructure Documentation.

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.

Refresh an Oracle E-Business Suite Environment

The Refresh feature allows you to refresh an Oracle E-Business Suite environment from a backup. This feature works by replacing both the database contents and applications code in the target environment while preserving the target environment's infrastructure and topology. This can accelerate and simplify the refresh of environments such as UAT, dev and test, and result in both time and cost savings.

This feature is supported for Oracle E-Business Suite Release 12.2 environments that use Oracle Database 19c. See Refresh an Oracle E-Business Suite Environment, page 12-52 for additional information regarding key attributes and restrictions.

Add and Delete Nodes

A horizontal scaling capability allows you to add and delete application tier nodes. 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 back end 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 job 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 job.

The Extensibility Framework provides administrators the ability to add tasks to jobs 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 insert pauses between phases as you choose, and resume the job 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

2

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 (Commercial Cloud Regions Only)

Overview of Deploying Oracle E-Business Suite Cloud Manager

This chapter describes how to deploy Oracle E-Business Suite Cloud Manager version 24.1.1 on Oracle Cloud Infrastructure.

Note: This procedure is available in commercial cloud regions only.

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 (Commercial Cloud Regions Only), page 2-45 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, 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

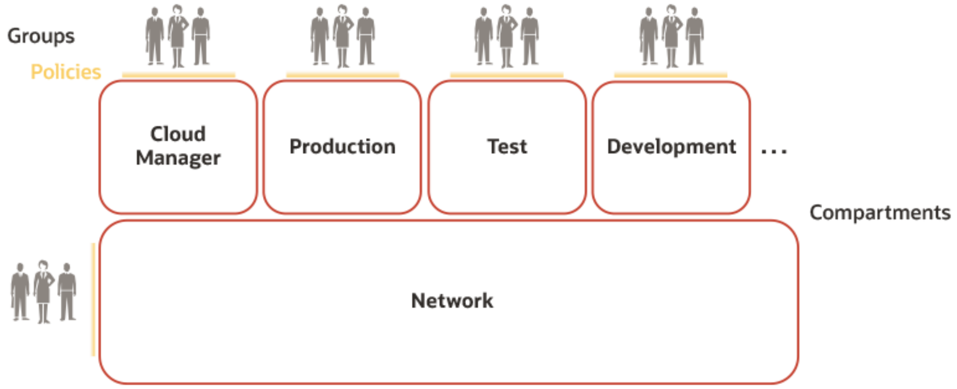
The following are four distinct categories of users referenced throughout this procedure and their roles:

- **Tenancy administrator** - Creates compartments, policies, groups, and users.

  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.

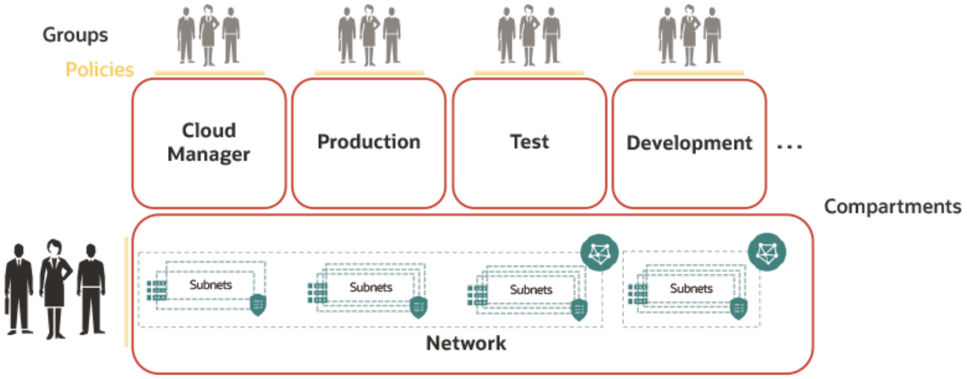
Example Tenancy Configuration Performed by Tenancy Administrators



- **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
    - Mount targets, if you plan to use the File Storage service for a shared file system for your Oracle E-Business Suite environments

  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.

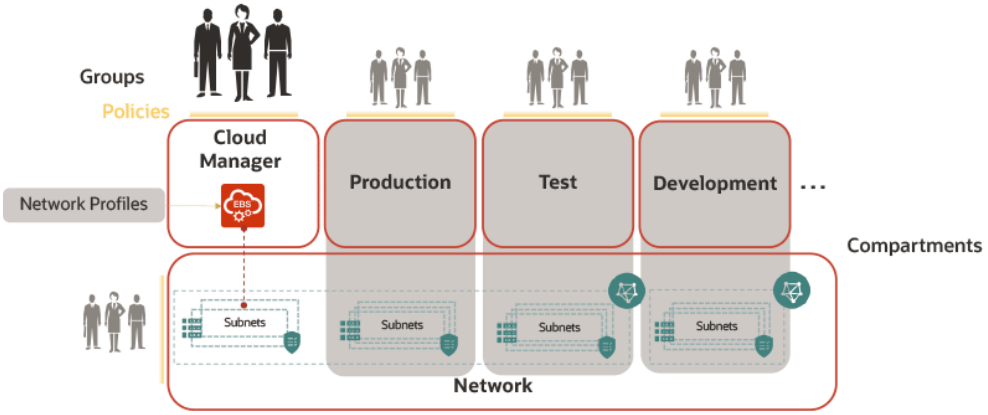
Example Network Configuration by Network Administrators



- **Oracle E-Business Suite Cloud Manager administrator** - Deploys 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 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.

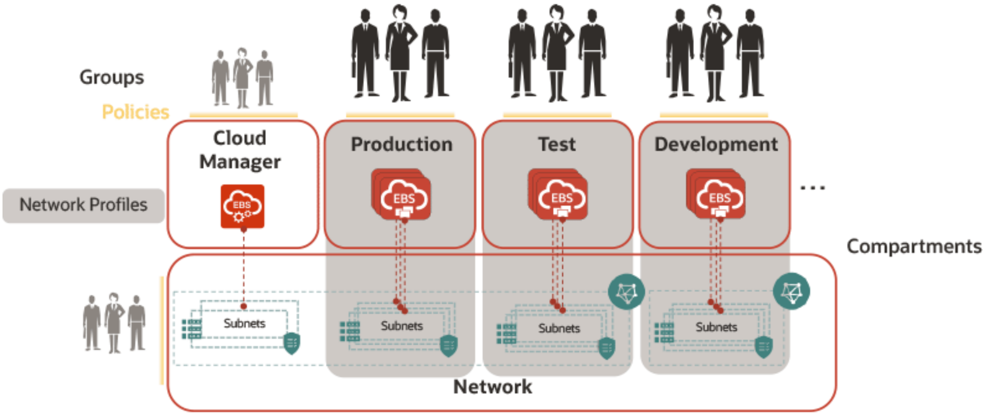
Example Deployment and Network Profile Configuration by Oracle E-Business Suite Cloud Manager Administrators



- **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



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 Groups, page 2-7

3. Assign Policies, page 2-8

4. Create Users with Oracle E-Business Suite Cloud Manager Administrator

Privileges, 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 Oracle E-Business Suite Cloud Manager, EBS environments, and the network.

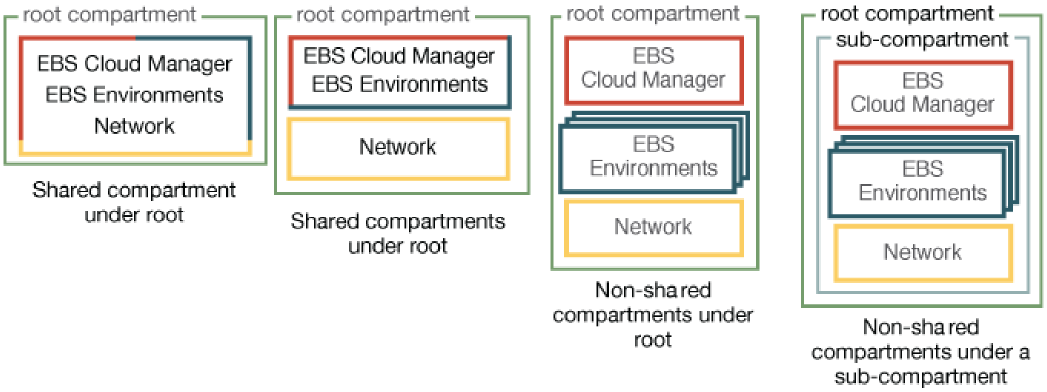
- Another certified hierarchy consists of multiple shared compartments under the root compartment including one compartment for Oracle E-Business Suite Cloud Manager and EBS environments, and another for the network.

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

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

The following diagram depicts these compartment hierarchies:

Certified Compartment Hierarchies



To create each compartment, perform the following:

1. While signed in to the Oracle Cloud Infrastructure Service Console, open the navigation menu and click **Identity & Security**. Under **Identity**, 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, `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**.

Create Groups:

The tenancy administrator is required to create the following groups:

- The network administrators group, such as `netadmin-grp`.

- The Oracle E-Business Suite Cloud Manager administrators group, such as `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 Manager Compute Instance, page 2-34.

Perform the following steps to create the two groups:

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click

Domains.

2. Select the root compartment in the **Compartment** drop-down list.

3. Within the list of domains, click the link for the "Default" domain.

4. Click **Groups**.

5. Click **Create group**.

6. 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.

7. Click **Create**.

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. Open the navigation menu and click **Identity & Security**. Under **Identity**, 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 the **Show manual editor** toggle switch. 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>
        ```

        If you plan to use the File Storage service for a shared file system for your Oracle E-Business Suite environments, then you must also add the following policy statement, substituting appropriate values for the variables designated by angle brackets.

        ```
        Allow group <network administrators group> to manage mount-
        targets 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.

    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 the **Show manual editor** toggle switch. 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 root compartment from the **Compartment** drop-down list.

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 the **Show manual editor** toggle switch. 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
     Allow group <Oracle E-Business Suite Cloud Manager
     administrators group> to inspect dynamic-groups in tenancy
     Allow group <Oracle E-Business Suite Cloud Manager
     administrators group> to use domains in tenancy
     ```

4. Click **Create Policy**.

Create Users with Oracle E-Business Suite Cloud Manager Administrator Privileges:

The tenancy administrator is required to create the users in this section.

While logged on to the Oracle Cloud Infrastructure Service Console as the tenancy administrator, create users who will have Oracle E-Business Suite Cloud Manager administrator privileges as follows.

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

1. Open the navigation menu, and click **Identity & Security**. Under **Identity**, click **Domains**.

2. Select the root compartment in the **Compartment** drop-down list.

3. Within the list of domains, click the link for the "Default" domain.

4. On the left hand side, click **Users**.

5. Click **Create User**.

6. In the Create User dialog box, enter the following:

- **First Name**: First name of the user.
- **Last Name**: Last name of the user.
- **Username / Email**: A valid email ID.
- **Groups**: Select the group that corresponds to the user you are creating. For example, if you are creating the Cloud Manager administrator, select the Cloud Manager administrators group. If you are creating the network administrator, select the network administrators group.

7. Click **Create**.
8. Grant the newly created user the Application Administrator role by following the steps in Assigning Users to Roles [https://docs.oracle.com/en-us/iaas/Content/Identity/users/about-managing-users.htm#assign-users-roles] in the Oracle Cloud Infrastructure Documentation.

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

> **Note:** Regarding host name resolution, be aware of the following important notes:
>
> 1. All virtual machines created by Oracle E-Business Suite Cloud Manager will have oraclevcn.com as the physical (network) host name.
> 2. These physical host names will be resolvable within the VCN and subnet in which they were created.
> 3. You can set the logical name (domain name) for these virtual machines as desired; however, these will be resolvable through the use of the /etc/hosts file only.

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 2-12.

Then dependent on the type of subnet you intend to use, either public or private, you will create associated network resources 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

    - Create an Internet Gateway, page 2-14
    - Create Route Tables, page 2-14
    - Configure Network Security, page 2-15
    - Create Security Rules, page 2-17
    - Create Subnets, page 2-19
- Create Network Resources for Use with Private Subnets, page 2-21
    - Create Network Address Translation (NAT) Gateway, page 2-22
    - Create a Service Gateway, page 2-22
    - Create Route Tables, page 2-23
    - Configure Network Security, page 2-25
    - Create Security Rules, page 2-29
    - Create Subnets, page 2-30

Oracle E-Business Suite Cloud Manager and associated load balancers work in regional and availability domain specific subnets. These subnets can be either public or private. Oracle recommends using regional and private subnets.

In a production environment, if you are not using FastConnect or IPsec VPN we recommend you deploy a dedicated bastion server. Use of a dedicated bastion server is strongly recommended when deploying Oracle E-Business Suite in government cloud regions. 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 Bastion Hosts: Protected Access for Virtual Cloud Networks [https://docs.oracle.com/en-us/iaas/Content/Resources/Assets/whitepapers/bastion-hosts.pdf] for more information about the architecture of the bastion server.

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 2-21.

To create a new Virtual Cloud Network (VCN):

1. Open the navigation menu. Click **Networking**, then 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.

   - **IPv4 CIDR Blocks**: Specify your choice of CIDR. For example, `10.0.0.0/16`.

   - Under **DNS Resolution**, select **Use DNS hostnames in this VCN**.

3. Click **Create VCN**.

4. Now, you must review and potentially modify the default DHCP options for your VCN.

   If your EBS environments need to contact a server in your local network that requires DNS name resolution, you must ensure your DHCP options include a custom DNS resolver. To do so, perform the following steps:

   1. Navigate to the DHCP options for your VCN and click on the name of the VCN you have just created.

   2. Under **Resources**, select **DHCP Options**.

   3. Review the Default DHCP Options for your VCN.

      If the DNS type for your default DHCP Options is Internet and VCN Resolver, perform the following steps:

      1. Click **Edit DHCP Options**.

      2. Change to Custom Resolver.

      3. Enter `169.254.169.254` for the IP address of the DNS Server (Note: This IP address corresponds to Oracle's VCN resolver.)

      4. Select **DNS Search Domain Type**.

         If you set your DNS Search Domain Type to "Customer Search Domain", you must confirm that when querying for host names, your DNS search domain returns fully qualified domain names (FQDN).

         To do so, use the command `hostname -f` on any of your Oracle E-Business Suite nodes to validate the host names.

         If your DNS search domain configuration does not result in FQDNs, you must set your DNS Search Domain Type to "Subnet Search Domain".

Create Network Resources for Use with Public Subnets (Conditional):

> **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 2-21.

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. Open the navigation menu. Under **Resources**, 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**.

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. Open the navigation menu. Under **Resources**, 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**.

Configure Network Security

In this section, you will establish network security either using network security groups (NSGs) or security lists.

Both NSGs and security lists use security rules to control traffic at the packet level. NSGs let you define a set of security rules that applies to a group of virtual network interface cards (VNICs) of your choice, while security lists let you define a set of security rules that applies to all the VNICs in an entire subnet.

Oracle recommends using NSGs instead of security lists because NSGs let you separate the VCN's subnet architecture from your application security requirements.

Follow the instructions in the applicable section to configure your method of network security:

- Network Security Groups, page 2-15
- Security Lists, page 2-16

Network Security Groups

To use network security groups (NSGs), create two separate NSGs. Their roles and some example names are shown in the following table:

Table 2-1 Network Security Groups

Component NSG Needed For	Example NSG Name
EBS Cloud Manager Load Balancer	ebscmlbaas-nsg
EBS Cloud Manager Virtual Machine	ebscmvm-nsg

For more information, see Network Security Groups [https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/networksecuritygroups.htm] in the Oracle Cloud Infrastructure Documentation.

To create an NSG:

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 **Network Security Groups**.

3. Click **Create Network Security Group**:

   - **Name**: Specify a name such as `ebscmlbaas-nsg` or `ebscmvm-nsg`.

   - **Create in Compartment**: Select your compartment name, such as **network-compartment**.

4. Click **Create**.

Create Security Lists (Optional If Not Using NSGs)

If you are not using NSGs, 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 ebscmlbaas-seclist, respectively.

To use security lists, create three to four separate security lists. Their roles and some example names are shown in the following table:

Table 2-2 Security Lists

Component Security List Needed For	Example Security List Name
EBS Cloud Manager Virtual Machine	ebscmvm-seclist
EBS Cloud Manager Load Balancer	ebscmlbaas-seclist

Create the Oracle E-Business Suite Cloud Manager Virtual Machine Security List

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

2. Open the navigation menu. Under **Resources**, 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.

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. Open the navigation menu. Under **Resources**, select **Security Lists**.

3. Click **Create Security List** and enter the required details of your security list:

   - **Name**: Specify a name such as `ebscmlbaas-seclist`.

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

Create Security Rules

In this section, you will add the mandatory security rules shown in the following tables to the chosen security mechanism --either network security group or security list-- created in Configure Network Security, page 2-15.

Create Security Rules for the EBS Cloud Manager Virtual Machine

1. 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`

2. 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`

3. Click **Create Security List**.

Create Security Rules for the EBS Cloud Manager Load Balancer

1. 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 2-36, when prompting for the Load Balancer Listener Port.

2. 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`

3. Click **Create Security List**.

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 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.

> **Note:** The Security Lists column in the following table is labeled "optional" as it is not applicable if you are using NSGs.

Table 2-3 Regional Public Subnet Example Names and Parameters

Subnet Name	CIDR Block	Route Table	Subnet Access	Security List (Optional)
ebscm-subnet-phx	10.0.0.0/24	ebscm-RouteTable	Public subnet	ebscmvm-seclist
lbaas-subnet-phx	10.0.1.0/24	lbaas-RouteTable	Public subnet	lbaas-seclist

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

> **Note:** The Security Lists column in the following table is labeled "optional" as it is not applicable if you are using NSGs.

Table 2-4 Availability Domain-Specific Public Subnet Example Names and Parameters

Subnet Name	Availability Domain (AD)	CIDR Block	Route Table	Subnet Access	Security List (Optional)
ebscm-subnet-ad1	AD-1	10.0.0.0/24	ebscm-RouteTable	Public subnet	ebscmvm-seclist

Subnet Name	Availability Domain (AD)	CIDR Block	Route Table	Subnet Access	Security List (Optional)
lbaas-subnet-ad1	AD-1	10.0.1.0/24	lbaas-RouteTable	Public subnet	lbaas-seclist
lbaas-subnet-ad2	AD-2	10.0.2.0/24	lbaas-RouteTable	Public subnet	lbaas-seclist

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. Open the navigation menu. Under **Resources**, 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.

   - **IPv4 CIDR Block**

   - **Route Table**: 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.

     Note: This parameter is not applicable if you are using NSGs.

4. Click **Create Subnet**.

Create Network Resources for Use with Private Subnets (Conditional):

Note: If you plan to use public subnets for Oracle E-Business Suite

Cloud Manager and a load balancer, do not perform the steps in this section. Instead, follow the steps in Create Network Resources for Use with Public Subnets, page 2-14.

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 (Conditional)

This step is mandatory when running Oracle E-Business Suite Cloud Manager in a commercial cloud region. When running in a government cloud region, to prevent any resource in the VCN from accessing the internet, skip this step.

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. Open the navigation menu. Under **Resources**, 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**.

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. Open the navigation menu. Under **Resources**, 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**.

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. Open the navigation menu. Under **Resources**, 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. (Conditional) Enable connectivity to public object storage if you plan to allow internet connectivity from your EBS environments. This is required in case you want to perform new installations using the Advanced Provisioning feature.
    1. Establish connectivity to object storage in required regions and home region.

        Oracle E-Business Suite Cloud Manager requires access to object storage in the following two regions, in addition to your home region:

        - US West (Phoenix)
        - US East (Ashburn)

        You have two options to establish this connectivity:

        - Enable the connectivity using the NAT gateway by performing the following steps to add a route rule:

            Click **+ Another Route Rule** and enter the route rule details as follows:

            - **Target Type**: Select NAT Gateway.

        - **Destination CIDR Block**: `134.70.0.0/16`. Note that the 134.70.0.0/16 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.

    - Alternatively, work with your network administrator to add a route rule in your private network to enable connectivity to the following CIDR block: `134.70.0.0/16`. You may also need to add firewall rules to allow connections to the following locations:

        - `https://objectstorage.us-phoenix-1.oraclecloud.com/`

        - `https://swiftobjectstorage.us-phoenix-1.oraclecloud.com/`

        - `https://objectstorage.us-ashburn-1.oraclecloud.com/`

2. Click **+ Another Route Rule** and enter route rule details as follows:

    - **Target Type**: Select NAT Gateway.

    - **Destination CIDR Block**: The CIDR for the Oracle Identity Cloud Service host being used. Note that the Oracle Identity Cloud Service host is of the format "idcs-xxxxxxxxxxxxxxxxxxxxxx.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.

5. 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 that XXX is a region-specific code such as IAD or LHR.

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

    - **Target Service Gateway**: Select the previously created service gateway.

6. Click **Create**.

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. Open the navigation menu. Under **Resources**, 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**.

Configure Network Security

In this section, you will establish network security either using network security groups (NSGs) or security lists when using private subnets.

Both NSGs and security lists use security rules to control traffic at the packet level. NSGs let you define a set of security rules that applies to a group of virtual network interface cards (VNICs) of your choice, while security lists let you define a set of security rules that applies to all the VNICs in an entire subnet.

Oracle recommends using NSGs instead of security lists because NSGs let you separate the VCN's subnet architecture from your application security requirements.

Follow the instructions in the applicable section to configure your method of network security:

- Network Security Groups, page 2-25
- Security Lists, page 2-26

Network Security Groups

To use network security groups (NSGs), create two NSGs. Their roles and some example names are shown in the following table:

Table 2-5 Network Security Groups

Component NSG Needed For	Example NSG Name
EBS Cloud Manager Load Balancer	ebscmlbaas-nsg
EBS Cloud Manager Virtual Machine	ebscmvm-nsg

For more information, see Network Security Groups [https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/networksecuritygroups.htm] in the Oracle Cloud Infrastructure Documentation.

To create an NSG:

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 **Network Security Groups**.

3. Click **Create Network Security Group**:

   - **Name**: Specify a name such as `ebscmlbaas-nsg` or `ebscmvm-nsg`.

   - **Create in Compartment**: Select your compartment name, such as **network-compartment**.

4. Click **Create**.

Security Lists (Optional If Not Using NSGs)

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.

To use security lists, create two separate security lists. Their roles and some example names are shown in the following table:

Table 2-6 Security Lists

Component Security List Needed For	Example Security List Name
EBS Cloud Manager Virtual Machine	ebscmvm-seclist

Component Security List Needed For	Example Security List Name
EBS Cloud Manager Load Balancer	ebscmlbaas-seclist

Create the Oracle E-Business Suite Cloud Manager Virtual Machine Security List

1. On the Virtual Cloud Networks screen, click the link with the name of your VCN, such as ebscm-vcn.
2. Open the navigation menu. Under **Resources**, 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`.

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. Open the navigation menu. Under **Resources**, 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`.

Create Security Rules for the EBS Cloud Manager Virtual Machine and Load Balancer

Create Security Rules for the EBS Cloud Manager Virtual Machine

In this section, you will add the mandatory security rules shown in the following steps to the chosen security mechanism --either network security group or security list--created in Configure Network Security When Using Private Subnets, page 2-25.

1. 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`

2. Under **Allow Rules for Egress**:

    1. (Conditional) If you plan to allow public internet connectivity from your EBS environments, click **+ Another Egress Rule** to add an egress rule to public object storage. Enter the following values:

        - **Destination Type**: `CIDR`

        - **Destination CIDR**: `134.70.0.0/16`. This particular CIDR 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**: 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
3. 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.
4. Click **+ Another Egress Rule** and enter the following values:
   - **Destination Type**: CIDR
   - **Destination CIDR**: VCN CIDR
   - **IP Protocol**: TCP
   - **Source Port Range**: All
   - **Destination Port Range**: 22
5. Click **Create Security List**.

Create Security Rules for the Load Balancer Subnet

In this section, you will add the mandatory security rules shown in the following steps to the chosen security mechanism --either network security group or security list--created in Configure Network Security, page 2-25

1. 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 2-36, when prompting for the Load Balancer Listener Port.
2. 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`
3. Click **Create Security List**.

Create Subnets

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

- One regional or availability domain-specific private 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 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.

> **Note:** The Security Lists column in the following table is labeled "optional" as it is not applicable if you are using NSGs.

Table 2-7 Regional Private Subnet Example Names and Parameters

Subnet Name	CIDR Block	Route Table	Subnet Access	Security List (Optional)
ebscm-subnet-phx	10.0.0.0/24	ebscm-RouteTable	Private subnet	ebscmvm-seclist
lbaas-subnet-phx	10.0.1.0/24	lbaas-RouteTable	Private subnet	lbaas-seclist

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

> **Note:** The Security Lists column in the following table is labeled "optional" as it is not applicable if you are using NSGs.

Table 2-8 Availability Domain-Specific Private Subnet Example Names and Parameters

Subnet Name	Availability Domain (AD)	CIDR Block	Route Table	Subnet Access	Security List (Optional)
ebscm-subnet-ad1	AD-1	10.0.0.0/24	ebscm-RouteTable	Private subnet	ebscmvm-seclist
lbaas-subnet-ad1	AD-1	10.0.1.0/24	lbaas-RouteTable	Private subnet	lbaas-seclist

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.

   - **IPv4 CIDR Block**

   - **Route Table**

   - **Subnet Access**: Select **Private Subnet** or **Public Subnet** for the subnet you wish to create.

   - **Security Lists**: Select the security list that matches the subnet you are defining based on Table 2-6.

     Note: Specifying a security list is not necessary if you are using NSGs.

4. Click **Create Subnet**.

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.

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.

2. Open the navigation menu. Under **Marketplace**, click **All Applications**.

3. If prompted for the compartment, select the compartment where you wish to install Oracle E-Business Suite Cloud Manager.

4. Then, select the Oracle E-Business Suite Cloud Manager image.

5. In the **Version** drop-down list, ensure that the default of **Oracle-EBS-Cloud-Manager-24.1.1-<date>** is selected.

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

7. Review and accept the Oracle Standard Terms and Restrictions.

8. Click **Launch Instance**.

9. 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 **Primary VNIC Information**:

        1. Locate the Network subsection, click the "Change Compartment" hyperlink, and select the compartment where your VCN resides. For instance, following our example in Create Compartments, page 2-6, you would select the compartment network-compartment.

        2. Also within the Network subsection, choose your VCN from the **Select a Virtual Cloud Network** drop-down list. For example, ebscm-vcn.

        3. Locate the Subnet subsection, click the "Change Compartment" hyperlink, and select the compartment where your VCN resides. For example, network-compartment.

        4. Also within the Subnet subsection, specify the Oracle E-Business Suite Cloud Manager subnet from the **Select a subnet** drop-down list. 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.

        6. If you plan to use NSGs, perform the following steps to define the EBS Cloud Manager NSGs:

            1. Click **Show advanced options**.

        2. Under Advanced Options, select the **Use network security groups to control traffic** checkbox.

        3. Select the EBS Cloud Manager NSGs (for example, ebscmvm-nsg).

    7. Under **Add SSH Keys**, choose one of the following options for this procedure:

        1. Select the **Generate a key pair for me** radio button, then click the "Save Private Key" link to download the private key. Doing so allows the SSH connection to be established.

        2. Alternatively, select the **Upload public key files (.pub)** radio button and then drag and drop the file or browse to specify the file containing your SSH public key generated previously.

        3. Another option is to 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.

10. Click **Create**.

    Once the instance is created (provisioned), details of the new instance will appear on the screen. Full details, including IP addresses, can also be viewed by clicking on the instance name in the instance list.

    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 2-35

- Identify Credential Required for Configuration Scripts, page 2-36

- Run Oracle E-Business Suite Cloud Manager Configure Script For the First Time, page 2-36
- Register Oracle E-Business Suite Cloud Manager as a Confidential Application, page 2-41
- Run Oracle E-Business Suite Cloud Manager Configure Script For the Second Time, page 2-43
- Configure Oracle Cloud Infrastructure Email Delivery Service (Optional) , page 2-44

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 with Oracle E-Business Suite Cloud Manager Administrator Privileges, page 2-10.

   2. Click the user avatar icon, labeled with your name.

   3. Select **My Profile** from the context menu.

   4. Open the navigation menu. Under **Resources**, 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 2-36.

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. Open the navigation menu and select **Governance & Administration**. Under **Account Management**, click **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:

   ```
   Enter 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 Admin User OCID (Non-
   Federated) : ocid1.user.oc1..xxxxxxxxxx
   Enter Full path to API Private Signing Key           :
   /u01/install/APPS/.oci/oci_api_key.pem
   Enter Tenancy OCID                                   : ocid1.
   tenancy.oc1..xxxxxxxxxx
   ```

   > **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:

   Group Name            Description
   ----------            -----------
   1: ebsdevdba-grp      EBS Dev DBA Group
   2: ebscmadmin-grp     EBS Cloud Manager Admin Group
   3: ebsdemodba-grp     EBS Test DBA Group
   4: ebsqadba-grp       EBS QA DBA Group

   Choose Oracle E-Business Suite Cloud Manager Administration 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
     ```

     > **Note:** If you choose an existing load balancer, then the `configure.pl` script creates the necessary new resources under that load balancer, including "listener", "backend set", "backend", and "certificate". The creation of the new resources will not affect any existing resources under that load balancer.

   - Otherwise, if you choose option 2 (No), indicating that you 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.

- Enter the bandwidth for the flexible shape load balancer:

  ```
  Choose Size of Bandwidth for Flexible Shape Load Balancer:

  Enter Minimum Bandwidth in Mbps
  : 10
  Enter Maximum Bandwidth in Mbps
  : 10
  ```

- 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 2-21):

  ```
  Available List of Subnets

  Regional ( recommended ):
  ------------------------------
  1: lbaas-subnet-phx

  Availability Domain: CQIl:PHX-AD-1
  ------------------------------
  2: lbaas-subnet-ad1

  Availability Domain: CQIl:PHX-AD-2
  ------------------------------
  3: lbaas-subnet-ad2
  4: othersubnet1

  Availability Domain: CQIl: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 Oracle E-Business Suite Cloud Manager.

```
--------------------------------------------------------------------
--------------------
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
Fingerprint of API Public Key : xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:
xx:xx:xx:xx
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..xxxxxxxxxxxxxxx
Oracle E-Business Suite Cloud Administrator Group Name : ebscmadmin-
grp
Oracle E-Business Suite Cloud Administrator Group OCID : ocid1.
group.oc1..xxxxxxxxxxxxxxxxxxxx
Network Compartment Name : network-compartment
Network Compartment OCID : ocid1.compartment.oc1..
xxxxxxxxxxxxxxxxxxxx
Network VCN Name : ebscm-vcn
Network VCN OCID : ocid1.vcn.oc1.phx-subnet.
xxxxxxxxxxxxxxxxxxxxxxxxxx
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 : flexible
Load Balancer Minimum Bandwidth in Mbps: 10
Load Balancer Maximum Bandwidth in Mbps: 10
Load Balancer Subnet Name : Public
Load Balancer Subnet OCID : ocid1.subnet.oc1.phx-subnet1.
xxxxxxxxxxxxxxxxxxxx
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.

```
====================================================================
====================================
Load Balancer demolbaas1 configuration completed. Review screen
messages above to determine if security rules are missing and must
be added in order to access the load balancer URL.
====================================================================
====================================
====================================================================
====================================
Register confidential application in IDCS with the URL: https://xxx.
xxx.xx.xxx:xxx and then re-run this script to update your IDCS
configuration.
====================================================================
====================================
```

Register Oracle E-Business Suite Cloud Manager as a Confidential Application:

In this section, you will register Oracle E-Business Suite Cloud Manager as a confidential application.

As an Oracle E-Business Suite Cloud Manager administrator who has been previously granted the Application Administrator role (in Create Users with Oracle E-Business Suite Cloud Manager Administrator Privileges, page 2-10), register Oracle E-Business Suite Cloud Manager as a confidential application using the following steps.

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Domains**.
2. Select the root compartment in the **Compartment** drop-down list.
3. Within the list of domains, click the link for the "Default" domain.
4. Click **Integrated applications** in the menu on the left.
5. Click **Add application**.
6. Select **Confidential Application** in the dialog box.
7. Click **Launch Workflow**.
8. Under Add application details, enter the following:
   - **Name**: Enter a name.
   - **Description**: Enter a description.
9. Click **Next**.
10. Under Configure OAuth:
    1. Click **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 2-36 in the following format: `<Your Load Balancer URL>/cm/auth/callback`. For example: `https://xxx.xxx.xx.xxx:xxx/cm/auth/callback`

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

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

   6. Under Client Type, ensure that the **Confidential** radio button is selected.

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

   8. Under Token Issuance Policy, select the **Add app roles** checkbox.

      1. Click **Add roles**.

      2. Select **Authenticator Client and Me**.

      3. Click **Add**, and then click **Next**.

11. Under Configure policy, click **Finish**.

12. Make a note of the following values under General Information:

    - Client ID

    - Client secret (In order to view, click **Show secret**.)

13. Click **Activate** and confirm to activate the confidential application.

14. Record the Domain URL found in the Overview page for the domain.

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 Domain application details, as shown in the following example.

   ```
   Enter Oracle E-Business Suite Cloud Manager Admin Password  :

   Enter IDCS Client ID        : <client id> (in a format similar to
   xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)
   Enter IDCS Client Secret    : <client secret> (in a format similar
   to xxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx)
   Enter IDCS URL              : <client url> (in a format similar to
   idcs-xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)
   ```

   The values you will need to enter for client ID and client secret were established when you registered Oracle E-Business Suite Cloud Manager as a confidential application in Register Oracle E-Business Suite Cloud Manager as a Confidential Application, page 2-41.

   To find the IDCS URL:

   1. In the OCI Console menu, navigate to **Identity & Security**, then **Domains**.

   2. Select the root compartment.

   3. Click on Default domain.

   The IDCS URL can be found in the Identity Domain settings page under Domain URL. For commercial cloud regions, the format is similar to `https://idcs-xxxxxxxxx.identity.oraclecloud.com:443`; For government cloud regions, the formatting is similar to `https://idcs-xxxxxxxx.<regional-idcs-instance>.identity.oci.<realm>.com:443`.

4. You will see a summary screen containing the information you specified earlier. The following is example output for a tenancy in a commercial cloud region:

```
--------------------------------------------------------------------
--------------------
Summary of Inputs
--------------------------------------------------------------------
--------------------
IDCS Client ID         : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
IDCS Client Secret     : xxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
IDCS URL               : https://idcs-xxxxxxxxxxxxxxxxxxxxxx.
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.

```
====================================================================
====================
Finished Configuring Oracle E-Business Suite Cloud Manager VM.
Login URL : https://xxx.xxx.xx.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 Update the Oracle E-Business Suite Cloud Manager Load Balancer URL, page 4-10.

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 4-16 and Disable Mailer Configuration, page 4-16.

Update to Latest Version of Oracle E-Business Suite Cloud Manager

To obtain the latest fixes, update to the latest version by following the instructions in Update Oracle E-Business Suite Cloud Manager to the Latest Version, 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/configuresmtpconnection.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:

   ```
   $ 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 (Commercial Cloud Regions Only)

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 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. 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.

Prepare Your Tenancy for Oracle E-Business Suite Cloud Manager Stack for Demos:

Follow the instructions detailed in Register Oracle E-Business Suite Cloud Manager as a Confidential Application, page 2-41. After completing these instructions, continue with the steps in Oracle E-Business Suite Cloud Manager Deployment and Configuration, page 2-46.

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 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 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. While signed in to the Oracle Cloud Infrastructure Service Console, open the navigation menu. Click **Marketplace** and then **All Applications**.

2. In the **Search** field, search for `Oracle E-Business Suite Cloud Manager Stack for Demos` and then click the **Oracle E-Business Suite Cloud Manager Stack for Demos** listing.

3. In the **Version** drop-down list, ensure that the default is selected. For example, Oracle-EBS-Cloud-Manager-RM-XX.X.X.X-XXXX.XX.XX.

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 Oracle standard Terms and Restrictions.

6. Click **Launch Stack**.

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

   1. Under **Setup Details**:

   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** checkbox selected.

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

2. Under **EBS Cloud Administrator Details**:

   1. Enter the user name corresponding to the EBS Cloud Manager administrator created in step 5 of Prepare Your Tenancy for Oracle E-Business Suite Cloud Manager Stack for Demos, page 2-46.

   2. Enter the email address of the EBS Cloud Manager administrator.

   3. Make sure the **Create new REST API Key** checkbox is selected.

3. Under **EBS Cloud Manager Instance Details**:

   1. Enter the load balancer URL you provided in step 10 (3) of Register Oracle E-Business Suite Cloud Manager as a Confidential Application, page 2-41.

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

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

   4. 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 [https://docs.oracle.com/en-us/iaas/Content/GSG/Tasks/creatingkeys.htm] in the Oracle Cloud Infrastructure Documentation.

   5. Choose the availability domain that ends in -1 from the list under EBS Cloud Manager Availability Domain.

4. Under **EBS Cloud Manager Network Details**:

   1. Leave the **Custom CIDR Ranges** checkbox deselected.

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

   3. 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, page 2-41.

8. On the Review screen, verify the information and click **Create**.

9. 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**.

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

11. 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.

12. 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. Right-click on Notepad and select the option to 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 in to Oracle E-Business Suite Cloud Manager using your Oracle Identity Cloud Service credentials.

   Once logged in, you are on the Environments page.

3

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

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.

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:** Oracle strongly recommends upgrading Oracle E-Business Suite

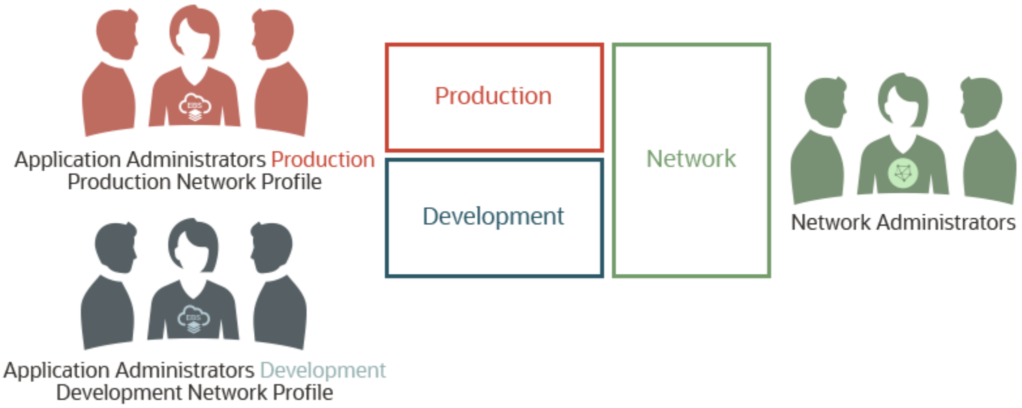
Cloud Manager to the latest version at your earliest convenience. To upgrade Oracle E-Business Suite Cloud Manager, follow the instructions in Update Oracle E-Business Suite Cloud Manager to Latest Version, page 4-1.

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


Application Administrators Production
Production Network Profile
Production
Network
Development
Network Administrators
Application Administrators Development
Development Network Profile

You may choose to define a new network compartment, or use the one that was defined while deploying 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.

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.

Process for Setting Up Your Tenancy to Host Oracle E-Business Suite Environments

Use the following steps to set up your tenancy to host Oracle E-Business Suite environments.

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

2. Create a group in the Default identity domain that will operate on the ebsprod-compartment compartment.

3. Create policies that allow the previously created group to manage resources in the ebsprod-compartment compartment.

4. Create users in the Default identity domain and make them members of the previously defined group.

5. Create network resources for the new set of Oracle E-Business Suite environments.

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

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

When preparing the tenancy to deploy your Oracle E-Business Suite production environments, 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. First, use single sign-on to log in to your cloud account using your tenancy administrator credentials. Do not use Oracle Cloud Infrastructure Direct Sign-In.

2. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Compartments**.

3. On the Compartments page, click **Create Compartment**.

4. In the dialog window, enter the required details:

   - **Name**: Enter the compartment name. For example, `ebsprod-compartment`.

   - **Description**: Enter a description of your choice.

5. Click **Create Compartment**.

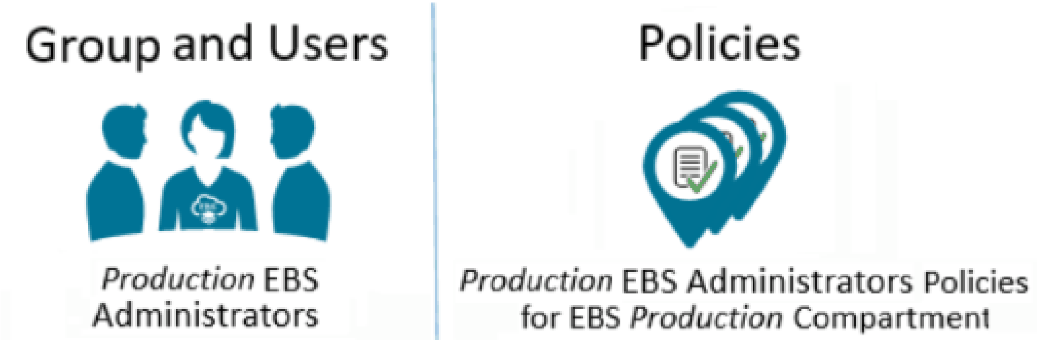
   For information on creating compartments and related policies for network resources and Oracle E-Business Suite Cloud Manager, see Deploy Oracle E-Business Suite Cloud Manager on Oracle Cloud Infrastructure, page 2-1.

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


Group and Users
Policies
Production EBS Administrators
Production EBS Administrators Policies for EBS *Production* Compartment

Perform the following steps to create the Oracle E-Business Suite administrators group and assign the required policies.

1. Create the Oracle E-Business Suite Administrators Group, page 3-5
2. Assign Policies, page 3-5

Create the Oracle E-Business Suite Administrators Group:

1. In the Oracle Cloud Infrastructure Console, open the navigation menu and click **Identity & Security**. Under **Identity**, click **Domains**.
2. Select the root compartment in the **Compartment** drop-down list.
3. Within the list of domains, click the link for the "Default" domain.
4. Click **Groups**.
5. Click **Create Group**.
6. In the dialog window, enter the required details:
   - **Name**: Enter the name for the group. For example, `ebscm-proddba-grp`.
   - **Description**: Enter a description of your choice.
7. Click **Create**.

Assign Policies:

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, 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**: Enter a name. For example, `networkcompartment-policy`.

        - **Description**: Enter a description of your choice.

        - In the Policy Builder section, click the **Show manual editor** toggle switch. Add the following policy statement, 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
          ```

          If you plan to use the File Storage service for a shared file system for your Oracle E-Business Suite environments, then you must also 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 manage export-sets in
          compartment network-compartment
          Allow group ebscm-proddba-grp to use mount-targets in
          compartment network-compartment
          Allow group ebscm-proddba-grp to use file-systems 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.

- In the Policy Builder section, click the **Show manual editor** toggle switch. Add the following policy statements, substituting your own group name in place of ebscm-proddba-grp, if appropriate.

  ```
  Allow group ebscm-proddba-grp to inspect buckets 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'
  Allow group ebscm-proddba-grp to inspect dynamic-groups in
  tenancy
  ```

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.

      - In the Policy Builder section, click the **Show manual editor** toggle switch. Add the following policy statements, substituting your own group name and compartment name if different from those in this 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 manage objects in compartment
ebsprod-compartment
Allow group ebscm-proddba-grp to manage buckets 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
```

If you plan to use the File Storage service for a shared file system for your Oracle E-Business Suite environments, then you must also add the following policy statements:

```
Allow group ebscm-proddba-grp to manage file-systems in
compartment ebsprod-compartment
Allow group ebscm-proddba-grp to manage export-sets in
compartment ebsprod-compartment
```

Additionally, if you want to use a different compartment for backups, then you must also add the following policy statements, substituting your own group name and the name of the compartment where you want to enable administrators to create backups:

```
Allow group ebscm-proddba-grp to manage objects in compartment
<compartment>
Allow group ebscm-proddba-grp to manage buckets in compartment
<compartment>
```

To create lifecycle rules for a bucket, add the following policy statement:

```
Allow service objectstorage-<region_identifier> to manage
object-family in tenancy
```

You can also define the same policy at the compartment level for a restricted access, by substituting your own object storage name and compartment name:

```
Allow service objectstorage-<region_identifier> to manage
object-family in compartment <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 make sure the user running the script is a member of the network administrators group. Refer to Assign Policies, page 2-8 under Create Oracle Cloud Infrastructure Accounts and Resources in the "Deploy Oracle E-Business Suite Cloud Manager on Oracle Cloud Infrastructure" chapter.

Create Oracle E-Business Suite Environment Administrators

You will create users as Oracle E-Business Suite environment administrators. These users will create and own the Oracle Cloud Infrastructure resources that run your Oracle E-Business Suite production environments.

Use the following steps to create Oracle E-Business Suite environment administrators.

1. Open the navigation menu, and click **Identity & Security**. Under **Identity**, click **Domains**.
2. Select the root compartment in the **Compartment** drop-down list.
3. Within the list of domains, click the link for the "Default" domain.
4. On the left hand side, click **Users**.
5. For each Oracle E-Business Suite production administrator to be added, for example the members of ebscm-proddba-grp, perform the following steps:
    1. Click **Create User**.
    2. In the Create User dialog box, enter the following:
        - **First Name**: First name of the user.
        - **Last name**: Last name of the user.
        - **Username / Email**: A valid email ID.
    3. Click **Create**.

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 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 environments' 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 - The network administrator creates a default network and two default network profiles, one for One-Click Provisioning and one for Advanced Provisioning, using provided scripts. The Oracle E-Business Suite Cloud Manager administrator will subsequently upload the network profiles for One-Click Provisioning and Advanced Provisioning.

  Note that the default network supports internal zones only, does not support File Storage service, and does not leverage network security groups. To take advantage of advanced options, you must create your own custom network profile.

- Use a Custom Network, page 3-16 - The network administrator has an option to create custom network elements and subsequently use these elements in the definition of custom network profiles.

  Note that the default network supports internal zones only, does not support File Storage Service, and does not leverage network security groups. To take advantage of advanced options, you must create your own custom network profile.

  Note that you must use a custom network if you plan to deploy an environment with multiple application tier nodes using a shared file system, which uses the File Storage service (FSS).

Use a Default Network with Automated Scripts:

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.

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 3-11.

  - Default network profile names are DEFAULT_PROFILE_ONECLICK and DEFAULT_PROFILE_ADVANCED, respectively, for either public or private subnet access.

- `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 3-15.

Prerequisites for Default Network Creation (Conditional)

If you plan to configure the default network with private subnet access, you must first follow these steps:

1. Ensure that there is a service gateway associated with your VCN. See Create a Service Gateway (Conditional), page 3-18 in "Use a Custom Network" for instructions.

2. (Commerical cloud regions only) Ensure that there is a NAT gateway associated with your VCN. See Create a NAT Gateway, page 3-17 in "Use a Custom Network" for instructions.

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.

2. Click the user avatar icon, labeled with your name.

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 the user avatar icon, labeled with your name, on the top right 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 3-12.

Run ProvisionOCINetwork.pl

The network administrator performs the tasks described in this section. This script defines security lists for controlling traffic at the packet level and deploys public 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..xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

   Validating user and fetching OCI metadata...

   Enter subnet access (public/private)                : private
   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/DEFAULT_PRIVATE_PROFILE_ADVANCED.json
   OneClick Network Profile JSON Path: /u01/install/APPS/apps-
   unlimited-ebs/build/ebscmnet/DEFAULT_PRIVATE_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 Manager Compute instance after running the `ProvisionOCINetwork.pl` script.

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

Post Requisites for Default Network Creation (Conditional)

If you are using private subnets and your tenancy belongs to a commercial realm, use the following steps to complete your default network configuration.

Note that where indicated, you will substitute the name of the unique network identifier that you supplied earlier when running the `ProvisionOCINetwork.pl` script ("ebscmnet" in our example).

Add Route Rules to Allow Internet Access to Private Subnets

1. Navigate to the route tables for the application tier and database tier subnets, created as part of the default network.

   1. From the OCI Console, open the navigation menu. Click **Networking** and then click **Virtual cloud networks**.

   2. Click on the name of your VCN.

   3. Under Resources, click **Route Tables**.

2. Add a new route rule to the route tables for the application tier and database tier subnets:

   1. Click on the name of the route table, which will be of the form <unique network

identifier>_<tier>_routetable, where tier is "apps" or "db" (for example, ebscmnet_apps_routetable or ebscmnet_db_routetable).

2. Click **+ Another Route Rule** and enter details as follows:
   - **Target Type**: Select **NAT Gateway**.
   - **Destination CIDR Block**: `134.70.0.0/17`
   - **Compartment**: Select the compartment.
   - **Target NAT Gateway**: Select the NAT Gateway (for example, ebs-ngw).

Add Egress Rules to Enable Private Subnets to Access Required Public Object Storage

1. Navigate to the security lists for the application tier and database tier subnets, created as part of the default network.
   1. From the OCI Console, open the navigation menu. Click **Networking** and then click **Virtual cloud networks**.
   2. Click on the name of your VCN.
   3. Under **Resources**, click **Security Lists**.
2. Add a new egress rule to the security lists for the application tier and database tier subnets:
   1. Click on the name of the security list, which will be of the form <unique network identifier>_<tier>_seclist, where tier is "apps" or "db" (for example, ebscmnet_apps_seclist or ebscmnet_db_seclist).
   2. Under **Resources**, click **Egress Rules**.
   3. Click **Add Egress Rules** and enter details as follows:
      - **Destination Type**: CIDR
      - **Destination CIDR**: `134.70.0.0/17`
      - **IP Protocol**: TCP
      - **Source Port Range**: All
      - **Destination Port Range**: All
   4. Click **Add Egress Rules** again to submit your changes.

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 3-12, 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.

Follow the steps as shown in this example to upload the One-Click 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:

   ```
   Log File : /u01/install/APPS/apps-unlimited-
   ebs/out/UploadOCINetworkProfile_Thu_Jul_11_13_55_49_2019.log
   ```

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/DEFAULT_PRIVATE_PROFILE_ONECLICK.json
   Enter OCID of EBS Cloud Manager administrator user       : ocid1.
   user.oc1..xxxxxxxxxx
   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..xxxxxxxxxxxxxxxxx
   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 3-12.

4. When the profile has been updated, you will see a success message similar to the following:

   ```
   Executing: ebscm_add_default_network_profile API for
   DEFAULT_PROFILE_ADVANCED
   Executing Stored Procedure: ebscm_add_default_network_profile
   RetCode: 0
   Row count: 0

   ONECLICK Network Profile uploaded successfully.
   ```

Repeat steps 1-4 for the Advanced Provisioning network profile, making sure to specify the JSON file absolute path for that profile (such as `/u01/install/APPS/apps-unlimited-ebs/build/ebscmnet/ebscmnet_DEFAULT_PROFILE_ADVANCED.json`) in step 4.)

> **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 environment 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/255817f83956f1f9a3ab903e11465e8b4dde1957/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 3-17
- Create an Internet Gateway (Conditional), page 3-17
- Create a NAT Gateway (Conditional), page 3-17
- Create a Service Gateway (Conditional), page 3-18
- Create Route Tables, page 3-19
- Configure Network Security, page 3-21
- Create Subnets, page 3-23
- Create Mount Targets (Conditional), page 3-26
- Create Security Rules, page 3-26

> **Note:** If you are using Exadata Database Service Dedicated, you should have already set up required route rules, security lists, and subnets required for the database tier. Review the corresponding resources created in this section for the database tier and add any missing resources.

Establish Your VCN

You have the option to create your own Virtual Cloud Network (VCN) or use an existing VCN (such as the VCN where 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 2-12.

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 2-11.

Create a NAT Gateway (Conditional)

If you plan to use a private subnet for your Oracle Oracle E-Business Suite environments and your tenancy is in a commercial cloud region, this step is mandatory. If you want to prevent the environments from connecting to the internet, skip this section.

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. Click **Networking**, then 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**:

   - **Name**: Specify a suitable name (for example, `ebs-ngw`).

   - **Create in Compartment**: Select your network compartment (for example, `network-compartment`).

   - 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 must create a service gateway. Note that object storage, the yum repository, and other required services are enabled through this gateway when deployed in private subnets.

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 to four separate route tables. Their roles and example names are shown in the following table:

Table 3-1 Route Tables

Component Route Table Needed For	Example Route Table Name
Load Balancer	ebslbaas-RouteTable
Oracle E-Business Suite Application Tier	apps-RouteTable
FSS Mount Target **Note:** This route table is required if you plan to implement a shared file system, which uses FSS.	fssmt-RouteTable
Oracle E-Business Suite Database Tier	db-RouteTable

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`, `fssmt-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** 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`, `fssmt-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** 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. (Note that if you have chosen to prevent your environments from having access to the public internet, you will not have a NAT gateway and therefore can skip creating this route rule.)

      - **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. Create another route rule by clicking **+ Another Route Rule**.
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 Service Gateway (for example, ebs-srvgw).
7. Click **Create** at the bottom of the window.

Configure Network Security

In this section, you will establish network security using one of the following options:

- A combination of network security groups (NSGs) and security lists
- Security lists only

Both NSGs and security lists use security rules to control traffic at the packet level. NSGs let you define a set of security rules that applies to a group of virtual network interface cards (VNICs) of your choice, while security lists let you define a set of security rules that applies to all the VNICs in an entire subnet.

Oracle recommends using NSGs instead of security lists because NSGs let you separate the VCN's subnet architecture from your application security requirements.

If you plan to use NSGs, follow the instructions in both Network Security Groups, page 3-21 and Security Lists, page 3-22.

Network Security Groups

The usage of network security groups (NSGs) is introduced in Oracle E-Business Suite Cloud Manager version 23.3.1.

To use NSGs, create three to four separate NSGs. Their roles and some example names are shown in the following table:

Table 3-2 Network Security Groups

Component NSG Needed For	Example NSG Name
Load Balancer	ebslbaas-nsg
Oracle E-Business Suite Application Tier	apps-nsg
FSS Mount Target **Note:** This NSG is required if you plan to implement a shared file system, which uses FSS.	fssmt-nsg
Oracle E-Business Suite Database Tier	db-nsg

For more information, see Network Security Groups [https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/networksecuritygroups.htm] in the Oracle Cloud Infrastructure Documentation.

To create an NSG:

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 **Network Security Groups**.

3. Click **Create Network Security Group**:

   - **Name**: Specify a name such as `ebslbaas-nsg`, `apps-nsg`, `fssmt-nsg`, or `db-nsg`.

   - **Create in Compartment**: Select your compartment name, such as **network-compartment**.

4. Click **Create**.

Security Lists

To use security lists, create three to four separate security lists. Their roles and some example names are shown in the following table:

Table 3-3 Security Lists

Component Security List Needed For	Example Security List Name
Load Balancer	ebslbaas-seclist
Oracle E-Business Suite Application Tier	apps-seclist
FSS Mount Target **Note:** This security list is required if you plan to implement a shared file system, which uses FSS.	fssmt-seclist
Oracle E-Business Suite Database Tier	db-seclist

For more information, see Security Lists [https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/securitylists.htm] in the Oracle Cloud Infrastructure Documentation.

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**:

   - **Name**: Specify a name such as `ebslbaas-seclist`, `apps-seclist`, `fssmt-seclist`, or `db-seclist`.

   - Create in Compartment: Select your compartment name, such as **network-compartment**.

   - If default rules named `Ingress Rule 1` and `Egress Rule 1` appear, remove these rules.

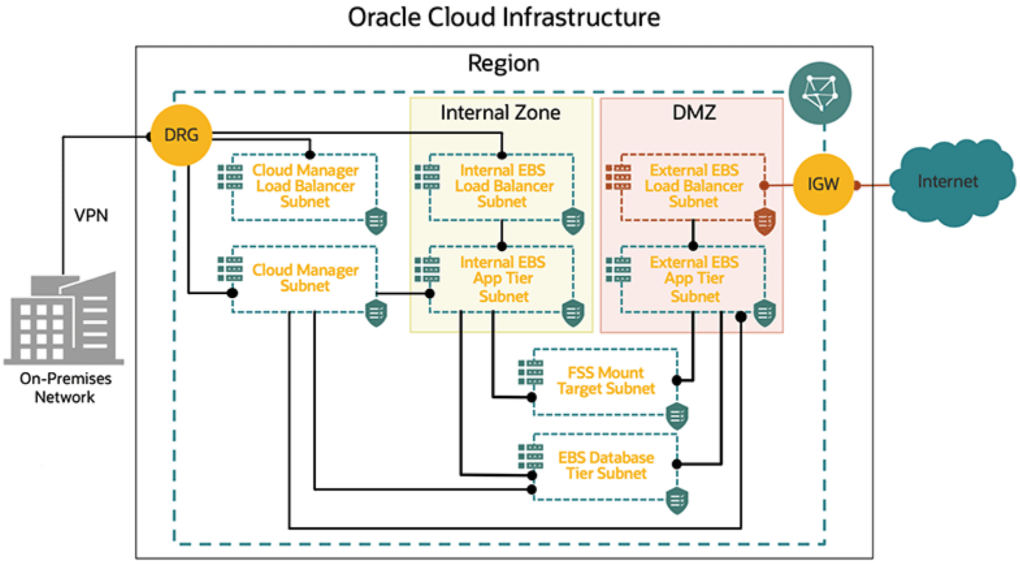
4. Click **Create Security List**.

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).

Oracle E-Business Suite Cloud Manager Network Profile Maps and Internal and External Subnets


Oracle Cloud Infrastructure
Region
Internal Zone
DMZ
DRG
VPN
On-Premises Network
Cloud Manager Load Balancer Subnet
Cloud Manager Subnet
Internal EBS Load Balancer Subnet
Internal EBS App Tier Subnet
External EBS Load Balancer Subnet
External EBS App Tier Subnet
IGW
Internet
FSS Mount Target Subnet
EBS Database Tier Subnet

This diagram maps the network profiles of two types of users: internal users who are typically the organization's employees and using the on-premises network, and external users who are partners such as suppliers or business-to-business (B2B) customers. Each type of user has its own web entry URL and dedicated application tier nodes to handle their requests. These application tier nodes are grouped by zones.

In this example, the internal zone handles all of the requests from internal users (employees), while the DMZ zone in the example handles all requests coming from external users. From a networking standpoint, the different subnets that support this topology are shown. There is a dedicated subnet for the internal load balancer, internal application tier nodes, external load balancer, external application tier nodes, FSS mount target, and database tier. The only subnet that is public is the external load balancer subnet. In this example, all subnets belong to a single VCN.

If you choose to use regional subnets, see the following table with example values for guidance.

Table 3-4 Examples of Regional Subnets

Subnet Name	CIDR Block	Route Table	Subnet Access	Security List
internal-ebslbaas-subnet-phx	10.0.3.0/24	ebslbaas-RouteTable	Public or private subnet	internal-ebslbaas-seclist
internal-apps-subnet-phx	10.0.4.0/24	apps-RouteTable	Public or private subnet	internal-apps-seclist
external-ebslbaas-subnet-phx (optional)	10.0.5.0/24	ebslbaas-RouteTable	Public or private subnet	external-ebslbaas-seclist
external-apps-subnet-phx	10.0.6.0/24	apps-RouteTable	Public or private subnet	external-apps-seclist
fssmounttarget-subnet-phx **Note:** This subnet is required if you plan to implement a shared file system, which uses FSS	10.0.7.0/24	fssmt-RouteTable	Public or private subnet	fssmt-seclist
db-subnet-phx	10.0.8.0/24	db-RouteTable	Public or private subnet	db-seclist

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.

- **IPv4 CIDR Block**
- **Route Table**: Select the route table you defined earlier.
- **Subnet Access**: As mentioned for 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 Lists**: Select the security lists you created previously.

4. Click **Create Subnet**.

Create Mount Targets (Conditional)

You can optionally use the Oracle Cloud Infrastructure File Storage service (FSS) for a shared file system for your Oracle E-Business Suite environments. Oracle Cloud Infrastructure File Storage service provides a durable, scalable, secure, enterprise-grade network file system that you can optionally choose to use in place of block volume storage. See Overview of File Storage [https://docs.oracle.com/en-us/iaas/Content/File/Concepts/filestorageoverview.htm#Overview_of_File_Storage].

If you plan to use the File Storage service, then you must now create the mount targets that your environments will use. A mount target is an NFS endpoint that resides in a VCN subnet of your choice and provides network access for file systems. The mount target provides the IP address or DNS name that is used together with a unique export path to mount the file system. The mount target must reside in the network compartment and should use the same VCN as the network profile. You can use the same mount target for multiple Oracle E-Business Suite file systems; the mount target serves to logically group together related file systems. For detailed instructions, see Managing Mount Targets [https://docs.oracle.com/en-us/iaas/Content/File/Tasks/managingmounttargets.htm#Managing_Mount_Targets] and Creating a Mount Target [https://docs.oracle.com/en-us/iaas/Content/File/Tasks/create-mount-target.htm#top].

Create Security Rules

In this section, you will add the mandatory security rules shown in the following tables to the chosen security mechanism --either network security group or security list--created in Configure Network Security, page 3-21.

Internal Load Balancer Security Rules

This section includes the following security rules for the internal load balancer security list:

Table 3-5 Ingress Rules for Both Public and Private Subnets

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

Table 3-6 Egress Rules When Using a Public Subnet

Destination Type	Destination	IP Protocol	Source Port Range / Type and Code	Destination Port Range / Type and Code
CIDR	0.0.0.0/0	TCP	All	All
CIDR	0.0.0.0/0	ICMP	N/A	N/A

Table 3-7 Egress Rules When Using a Private Subnet

Destination Type	Destination	IP Protocol	Source Port Range / Type and Code	Destination Port Range / Type and Code
CIDR	<Internal application tier subnet CIDR>	TCP	All	All
CIDR	0.0.0.0/0	ICMP	N/A	N/A

External Load Balancer Security Rules (Optional)

This section includes the following security rules for the external load balancer security list:

Table 3-8 Ingress Rules for Both Public and Private Subnets

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

Table 3-9 Egress Rules When Using a Public Subnet

Destination Type	Destination	IP Protocol	Source Port Range / Type and Code	Destination Port Range / Type and Code
CIDR	0.0.0.0/0	TCP	All	All
CIDR	0.0.0.0/0	ICMP	N/A (leave **Type and Code** blank)	N/A

Table 3-10 Egress Rules When Using a Private Subnet

Destination Type	Destination	IP Protocol	Source Port Range / Type and Code	Destination Port Range / Type and Code
CIDR	<External application tier subnet CIDR>	TCP	All	All
CIDR	0.0.0.0/0	ICMP	N/A	N/A

Application Tier Security Rules for Internal Subnets

This section includes the following security rules for the application tier security list for internal subnets:

Table 3-11 Ingress Rules for Both Public and Private Internal Subnets

Source Type	Source	IP Protocol	Source Port Range / Type and Code	Destination Port Range / Type and Code
CIDR	<Internal application tier subnet CIDR>	TCP	All	All
CIDR	<EBS Cloud Manager subnet CIDR>	ICMP	N/A (leave **Type and Code** blank)	N/A (leave **Type and Code** blank)
CIDR	<Internal load balancer subnet CIDR>	ICMP	N/A (leave **Type and Code** blank)	N/A (leave **Type and Code** blank)
CIDR	<EBS Cloud Manager subnet CIDR>	TCP	All	22
CIDR	<External application tier subnet CIDR>	TCP	All	111
CIDR	<External application tier subnet CIDR>	TCP	All	2049
CIDR	<Database tier subnet CIDR>	ICMP	N/A (leave **Type and Code** blank)	N/A (leave **Type and Code** blank)
CIDR	<Internal application tier subnet CIDR>	ICMP	N/A (leave **Type and Code** blank)	N/A (leave **Type and Code** blank)
CIDR	<External application tier subnet CIDR>	TCP	All	7001-7003
CIDR	<External application tier subnet CIDR>	TCP	All	6801-6802

Source Type	Source	IP Protocol	Source Port Range / Type and Code	Destination Port Range / Type and Code
CIDR	<External application tier subnet CIDR>	TCP	All	16801-16802
CIDR	<External application tier subnet CIDR>	TCP	All	12345
CIDR	<External application tier subnet CIDR>	TCP	All	36501-36550
CIDR	<Internal load balancer subnet CIDR>	TCP	All	8000
CIDR	<Mount target subnet CIDR> See footnote [1]	TCP	All	111
CIDR	<Mount target subnet CIDR> See footnote [1]	TCP	All	2048-2050
CIDR	<Mount target subnet CIDR> See footnote [1]	UDP	All	111
CIDR	<Mount target subnet CIDR> See footnote [1]	UDP	All	2048

Footnote for Table 3-11:

1. Only required if you plan to implement a shared file system, which uses FSS.

Table 3-12 Egress Rules When Using a Public Subnet

Destination Type	Destination	IP Protocol	Source Port Range / Type and Code	Destination Port Range / Type and Code
CIDR	0.0.0.0/0	TCP	All	All
CIDR	0.0.0.0/0	ICMP	N/A	N/A
CIDR	<Mount target subnet CIDR> See footnote [1]	UDP	All	111
CIDR	<Mount target subnet CIDR> See footnote [1]	UDP	All	2048
CIDR	<Mount target subnet CIDR> See footnote [1]	TCP	All	111
CIDR	<Mount target subnet CIDR> See footnote [1]	TCP	All	2048-2050

Footnote for Table 3-12:

1. Only required if you plan to implement a shared file system, which uses FSS.

Table 3-13 Egress Rules When Using a Private Subnet

Destination Type	Destination	IP Protocol	Source Port Range / Type and Code	Destination Port Range / Type and Code
CIDR	134.70.0.0/17 See footnote [1]	TCP	All	All

Destination Type	Destination	IP Protocol	Source Port Range / Type and Code	Destination Port Range / Type and Code
Service	All <XXX> Services in the Oracle Services Network (XXX is a region-specific code, such as IAD or LHR)	TCP	All	All
Service	All <XXX> Services in the Oracle Services Network (XXX is a region-specific code, such as IAD or LHR)	ICMP	N/A	N/A
CIDR	<External application tier subnet CIDR>	TCP	All	All
CIDR	<Internal application tier subnet CIDR>	TCP	All	All
CIDR	<Database tier subnet CIDR>	TCP	All	1521-1524
CIDR	<EBS Cloud Manager subnet CIDR>	TCP	All	443
CIDR	0.0.0.0/0	ICMP	N/A	N/A
CIDR	<Mount target subnet CIDR> See footnote [2]	UDP	All	111

Destination Type	Destination	IP Protocol	Source Port Range / Type and Code	Destination Port Range / Type and Code
CIDR	<Mount target subnet CIDR> See footnote [2]	UDP	All	2048
CIDR	<Mount target subnet CIDR> See footnote [2]	TCP	All	111
CIDR	<Mount target subnet CIDR> See footnote [2]	TCP	All	2048-2050

Footnote for Table 3-13:

1. Only required if you plan to provide access to public internet.
2. Only required if you plan to implement a shared file system, which uses FSS.

Application Tier Security Rules for External Subnets (Optional)

This section includes the following security rules for the application tier security list for external subnets:

Table 3-14 Ingress Rules for Application Tier Subnet 2 (appSubnet2)

Source Type	Source	IP Protocol	Source Port Range / Type and Code	Destination Port Range / Type and Code
CIDR	<External application tier subnet CIDR>	TCP	All	All
CIDR	<EBS Cloud Manager subnet CIDR>	ICMP	N/A (leave **Type and Code** blank)	N/A (leave **Type and Code** blank)

Source Type	Source	IP Protocol	Source Port Range / Type and Code	Destination Port Range / Type and Code
CIDR	<External load balancer subnet CIDR>	ICMP	N/A (leave **Type and Code** blank)	N/A (leave **Type and Code** blank)
CIDR	<EBS Cloud Manager subnet CIDR>	TCP	All	22
CIDR	<Internal application tier subnet CIDR>	TCP	All	111
CIDR	<Internal application tier subnet CIDR>	TCP	All	2049
CIDR	<Internal application tier subnet CIDR>	ICMP	N/A (leave **Type and Code** blank)	N/A (leave **Type and Code** blank)
CIDR	<Database tier subnet CIDR>	ICMP	N/A (leave **Type and Code** blank)	N/A (leave **Type and Code** blank)
CIDR	<External application tier subnet CIDR>	ICMP	N/A (leave **Type and Code** blank)	N/A (leave **Type and Code** blank)
CIDR	<Internal application tier subnet CIDR>	TCP	All	22
CIDR	<Internal application tier subnet CIDR>	TCP	All	5556-5557
CIDR	<Internal application tier subnet CIDR>	TCP	All	7201-7202

Source Type	Source	IP Protocol	Source Port Range / Type and Code	Destination Port Range / Type and Code
CIDR	<Internal application tier subnet CIDR>	TCP	All	17201-17202
CIDR	<Internal application tier subnet CIDR>	TCP	All	7401-7402
CIDR	<Internal application tier subnet CIDR>	TCP	All	17401-17402
CIDR	<Internal application tier subnet CIDR>	TCP	All	7601-7602
CIDR	<Internal application tier subnet CIDR>	TCP	All	17601-17602
CIDR	<Internal application tier subnet CIDR>	TCP	All	7801-7802
CIDR	<Internal application tier subnet CIDR>	TCP	All	17801-17802
CIDR	<Internal application tier subnet CIDR>	TCP	All	6801-6802
CIDR	<Internal application tier subnet CIDR>	TCP	All	16801-16802
CIDR	<Internal application tier subnet CIDR>	TCP	All	9999-10000

Source Type	Source	IP Protocol	Source Port Range / Type and Code	Destination Port Range / Type and Code
CIDR	<Internal application tier subnet CIDR>	TCP	All	1626
CIDR	<Internal application tier subnet CIDR>	TCP	All	12345
CIDR	<Internal application tier subnet CIDR>	TCP	All	36501-36550
CIDR	<Internal application tier subnet CIDR>	TCP	All	6100-6101
CIDR	<Internal application tier subnet CIDR>	TCP	All	6200-6201
CIDR	<Internal application tier subnet CIDR>	TCP	All	6500-6501
CIDR	<External load balancer subnet CIDR>	TCP	All	8000
CIDR	<Mount target subnet CIDR> See footnote [1]	TCP	All	111
CIDR	<Mount target subnet CIDR> See footnote [1]	TCP	All	2048-2050
CIDR	<Mount target subnet CIDR> See footnote [1]	UDP	All	111

Source Type	Source	IP Protocol	Source Port Range / Type and Code	Destination Port Range / Type and Code
CIDR	<Mount target subnet CIDR> See footnote [1]	UDP	All	2048

Footnote for Table 3-14:

1. Only required if you plan to implement a shared file system, which uses FSS.

Table 3-15 Egress Rules When Using a Public Subnet

Destination Type	Destination	IP Protocol	Source Port Range / Type and Code	Destination Port Range / Type and Code
CIDR	0.0.0.0/0	TCP	All	All
CIDR	0.0.0.0/0	ICMP	N/A	N/A
CIDR	<Mount target subnet CIDR> See footnote [1]	UDP	All	111
CIDR	<Mount target subnet CIDR> See footnote [1]	UDP	All	2048

Footnote for Table 3-15:

1. Only required if you plan to implement a shared file system, which uses FSS.

Table 3-16 Egress Rules When Using a Private Subnet

Destination Type	Destination	IP Protocol	Source Port Range / Type and Code	Destination Port Range / Type and Code
CIDR	134.70.0.0/17 See footnote [1]	TCP	All	All
CIDR	<External application tier subnet CIDR>	TCP	All	All
CIDR	<Database tier subnet CIDR>	TCP	All	1521-1524
CIDR	<EBS Cloud Manager subnet CIDR>	TCP	All	443
CIDR	0.0.0.0/0	ICMP	N/A	N/A
CIDR	<Internal application tier subnet CIDR>	TCP	All	All
Service	All <XXX> Services in the Oracle Services Network (XXX is a region-specific code, such as IAD or LHR)	TCP	All	All
Service	All <XXX> Services in the Oracle Services Network (XXX is a region-specific code, such as IAD or LHR)	ICMP	N/A	N/A

Destination Type	Destination	IP Protocol	Source Port Range / Type and Code	Destination Port Range / Type and Code
CIDR	<Mount target subnet CIDR> See footnote [2]	UDP	All	111
CIDR	<Mount target subnet CIDR> See footnote [2]	UDP	All	2048
CIDR	<Mount target subnet CIDR> See footnote [2]	TCP	All	111
CIDR	<Mount target subnet CIDR> See footnote [2]	TCP	All	2048-2050

Footnote for Table 3-16:

1. Only required if you plan to provide access to public internet.

2. Only required if you plan to implement a shared file system, which uses FSS.

FSS Mount Target Security Rules

The following security rules must be added for the FSS mount target security list. If you have established an external zone, these rules must be created for both your internal application tier subnet and for your external application tier subnet.

Table 3-17 Ingress Rules for Both Public and Private Subnets

Source Type	Source	IP Protocol	Source Port Range / Type and Code	Destination Port Range / Type and Code
CIDR	<Application tier subnet CIDR>	TCP	All	111

Source Type	Source	IP Protocol	Source Port Range / Type and Code	Destination Port Range / Type and Code
CIDR	<Application tier subnet CIDR>	TCP	All	2048
CIDR	<Application tier subnet CIDR>	TCP	All	2049
CIDR	<Application tier subnet CIDR>	TCP	All	2050
CIDR	<Application tier subnet CIDR>	UDP	All	111
CIDR	<Application tier subnet CIDR>	UDP	All	2048

Table 3-18 Egress Rules for Both Public and Private Subnets

Source Type	Source	IP Protocol	Source Port Range / Type and Code	Destination Port Range / Type and Code
CIDR	<Application tier subnet CIDR>	TCP	All	111
CIDR	<Application tier subnet CIDR>	TCP	All	2048
CIDR	<Application tier subnet CIDR>	TCP	All	2049
CIDR	<Application tier subnet CIDR>	TCP	All	2050
CIDR	<Application tier subnet CIDR>	UDP	All	111
CIDR	<Application tier subnet CIDR>	UDP	All	2048

Database Tier Security Rules

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

Table 3-19 Ingress Rules for Both Public and Private Subnets

Source Type	Source	IP Protocol	Source Port Range / Type and Code	Destination Port Range / Type and Code
CIDR	<EBS Cloud Manager subnet CIDR>	ICMP	N/A (leave **Type and Code** blank)	N/A (leave **Type and Code** blank)
CIDR	<Database tier subnet CIDR>	ICMP	N/A (leave **Type and Code** blank)	N/A (leave **Type and Code** blank)
CIDR	<EBS Cloud Manager subnet CIDR>	TCP	All	22
CIDR	<Internal application tier subnet CIDR>	TCP	All	1521-1524
CIDR	<Internal application tier subnet CIDR>	ICMP	N/A (leave **Type and Code** blank)	N/A (leave **Type and Code** blank)
CIDR	<External application tier subnet CIDR>	TCP	All	1521-1524
CIDR	<External application tier subnet CIDR>	ICMP	N/A (leave **Type and Code** blank)	N/A (leave **Type and Code** blank)
CIDR	<Database tier subnet CIDR>	TCP	All	22
CIDR	<Database tier subnet CIDR>	TCP	All	1521-1524

Table 3-20 Egress Rules When Using a Public Subnet

Destination Type	Destination	IP Protocol	Source Port Range / Type and Code	Destination Port Range / Type and Code
CIDR	0.0.0.0/0	TCP	All	All
CIDR	0.0.0.0/0	ICMP	N/A	N/A

Table 3-21 Egress Rules When Using a Private Subnet

Destination Type	Destination	IP Protocol	Source Port Range / Type and Code	Destination Port Range / Type and Code
CIDR	134.70.0.0/17 See footnote [1]	TCP	All	All
CIDR	<EBS Cloud Manager subnet CIDR>	TCP	All	443
CIDR	<Database tier subnet CIDR>	TCP	All	1521-1524
CIDR	<Database tier subnet CIDR>	TCP	All	22
CIDR	0.0.0.0/0	ICMP	N/A	N/A
Service	All <XXX> Services in the Oracle Services Network (XXX is a region-specific code, such as IAD or LHR)	TCP	All	All

Destination Type	Destination	IP Protocol	Source Port Range / Type and Code	Destination Port Range / Type and Code
Service	All <XXX> Services in the Oracle Services Network	ICMP	All	All

Footnote for Table 3-21:

1. Only required if you plan to provide access to public internet.

Oracle E-Business Suite Cloud Manager Security Rules

> **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 2-11

Table 3-22 Ingress Rules

Source Type	Source	IP Protocol	Source Port Range / Type and Code	Destination Port Range / Type and Code
CIDR	<Application tier subnet CIDR>	TCP	All	443
CIDR	<Database tier subnet CIDR>	TCP	All	443

Table 3-23 Egress Rules

Destination Type	Destination	IP Protocol	Source Port Range / Type and Code	Destination Port Range / Type and Code
CIDR	<Application tier subnet CIDR>	TCP	All	22

Destination Type	Destination	IP Protocol	Source Port Range / Type and Code	Destination Port Range / Type and Code
CIDR	<Database tier subnet CIDR>	TCP	All	22

Create Network Profiles

A network profile maps Oracle Cloud Infrastructure network definitions with the Oracle E-Business Suite environment network requirements. Before 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. Oracle E-Business Suite administrators can then select those network profiles when performing processes such as advanced provisioning or cloning. Only Oracle E-Business Suite Cloud Manager administrators can create network profiles.

In our example, the administrators are members of the ebs-proddba-grp group.

To create a new network profile, see Create a Network Profile, page 8-6.

Create Exadata Infrastructure and Associated VM Cluster for Exadata Database Service on Dedicated Infrastructure (Conditionally Required)

If you plan to use Oracle E-Business Suite Cloud Manager with Oracle Exadata Database Service on Dedicated Infrastructure, you must first create the Exadata infrastructure and associated VM Cluster.

Create Exadata Infrastructure:

1. You will first create a network profile which maps to the region and availability domain which you plan to use while creating your Exadata infrastructure. This same region and availability domain will be used for all OCI resources associated with your Oracle E-Business Suite environments:

2. Then, follow the steps in Creating an Exadata Cloud Infrastructure Instance [https://docs.oracle.com/en-us/iaas/exadatacloud/exacs/ecs-create-instance.html#GUID-2296ECC1-3D58-4C42-8C5B-849087323D7D] to create your new infrastructure.

3. After the Exadata infrastructure resource is provisioned and available, you must create an Exadata VM cluster.

Note: Oracle E-Business Suite Cloud Manager 23.2.1 and later support infrastructure containing multiple VM clusters. When provisioning, you will select the VM cluster on which to provision the database from the available options.

Create an Exadata VM Cluster:

1. Follow the steps in To Create a Cloud VM Cluster Resource [https://docs.oracle.com/en-us/iaas/exadatacloud/exacs/manage-vm-clusters.html#GUID-11C092BB-2B85-4342-B143-8FC5FC80ECA3] to create your VM cluster while specifying the following properties:

   - **Configure Exadata storage** - When configuring Exadata storage, you must select the option "Allocate storage for Exadata sparse snapshots". If you do not enable this option during the configuration of the cluster, you will need to delete the cluster and recreate it with this option enabled in order to use the Oracle E-Business Suite Cloud Manager Cloning Using Exadata Snapshots feature. A cluster with this option enabled will have "Storage for Exadata sparse snapshots" listed as Enabled on the Cluster details page under the Resource allocation section.

   - **Configure the network settings** - When configuring the network settings, you must ensure that your choices for VCN and subnet match what you specified in the network profile.

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
- 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

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. Check Space Requirements, page 4-3

4. Update to the Latest Codelevel, page 4-3

5. Switch to File Storage Service, page 4-6

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.

How you proceed will depend on your current Oracle E-Business Suite Cloud Manager version:

- If you are on Oracle E-Business Suite Cloud Manager version 22.1.1 or later, you will see a message that a later version is available than the one you have installed, and can proceed with the rest of this procedure by performing the steps in Create a Backup of Oracle E-Business Suite Cloud Manager Virtual Machine, page 4-2, followed by Check Space Requirements, page 4-3 and then Update to the Latest Codelevel, page 4-3.

- If you are on an Oracle E-Business Suite Cloud Manager version earlier than 22.1.1, 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.

The latest version is 24.1.1.

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.

Check Space Requirements:

Before updating Oracle E-Business Suite Cloud Manager to the latest version, ensure that you have at least 5 GB of available disk space.

While logged in to the Oracle E-Business Suite Cloud Manager virtual machine, run the following commands:

```
cd /u01
df -kh .
```

If the available disk space is less than 5 GB, you can free up space by removing older files from the following directories:

- `/u01/install/APPS/backup`

- `/u01/install/APPS/apps-unlimited-ebs/diagnostics`

If the available disk space is still less than 5 GB, you must resize the boot volume of Oracle E-Business Suite Cloud Manager before proceeding with the migration to the latest codelevel. To resize the boot volume, follow the instructions in Extending the Partition for a Boot Volume [https://docs.oracle.com/en-us/iaas/Content/Block/Tasks/extendingbootpartition.htm] in the Oracle Cloud Infrastructure Documentation.

After the volume is provisioned, for the volume resize to take effect, you need to:

1. Run the applicable rescan commands. See Rescanning the Disk for a Block Volume or Boot Volume [https://docs.oracle.com/en-us/iaas/Content/Block/Tasks/rescanningdisk.htm].

2. Extend the partition manually. See Extending the Partition for a Boot Volume [https://docs.oracle.com/en-us/iaas/Content/Block/Tasks/extendingbootpartition.htm].

After confirming that you have sufficient available disk space, you can proceed to the steps in Update to the Latest Codelevel, page 4-3.

Update to the Latest Codelevel:

After you have created the backup of the virtual machine and confirmed the available disk space, you can proceed to update your deployment.

Run the Self Update utility to update Oracle E-Business Suite Cloud Manager to the latest version, which is 24.1.1.

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. The Self Update Utililty first checks for public object storage connectivity.

   1. If you do not have connectivity to public object storage, the script will update using a local tarball file instead. When prompted, provide the complete path of the local tarball file as well as the stage location in which to extract the tarball file contents. Then, enter Y to continue and perform the upgrade.

      ```
      Checking public object storage connectivity.
      No connectivity to public object storage.
      Will attempt to update using local tarball instead.
      Enter complete path of local tarball file :
      /u01/install/APPS/EBSCloudAdminTools_v24.1.1.tgz
      Enter stage location to extract tarball
      [/u01/install/APPS/updates]:
      Using default stage location: /u01/install/APPS/updates
      Validating specified tarball. Please wait.
      Validation successful for specified tarball.
      Do you want to continue and perform the upgrade? [Y/N]? Y
      ```

   2. If connectivity to public object storage is in place, choose the Oracle E-Business Suite Cloud Manager version from the choices provided:

      ```
      Available Oracle E-Business Suite Cloud Manager release versions:


      1: 24.1.1

      Choose release version to upgrade to 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 should have already followed the steps in Configure Oracle E-Business Suite Cloud Manager Compute Instance, page 2-34, to configure your VM. At this prompt, enter the Oracle E-Business Suite Cloud Manager administrator password you specified at that time.

5. Next, the Self Update utility prompts you to confirm that you have created a backup of the Oracle E-Business Suite Cloud Manager Virtual Machine following the instructions in Create a Backup of Oracle E-Business Suite Cloud Manager Virtual Machine, page 4-2.

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

   ```
   Before update, you must create a backup of the Oracle E-Business
   Suite Cloud
   Manager Virtual Machine as per the instructions in the section
   "Update to Latest Version
   of Oracle E-Business Suite Cloud Manager" of Oracle E-Business Suite
   Cloud Manager Guide.

   To continue, you must confirm you have created a backup of your
   Oracle E-Business
   Suite Cloud Manager Virtual Machine or the update process will exit.

   Backup created [Y/N]?
   ```

   > **Note:** If you have not yet created your backup, enter N at the prompt. In this case, the utility exits to allow you to create the backup before proceeding with the update process.

6. Before continuing with the update, you should also ensure that there are no jobs in your Oracle E-Business Suite Cloud Manager with a status of In Progress, Scheduled, Paused, or Failed. See Monitor Job Status, page 13-1.

   It is recommended that you allow In Progress and Scheduled jobs to complete before continuing, resume any Paused jobs, and restart any Failed jobs 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 job. If there are still any jobs with a status of Failed when you perform the update, their status will be changed to Aborted. In this case, you must manually clean up any incomplete resources from the job after the update.

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

   ```
   Before upgrading, ensure there are no In Progress, Scheduled,
   Paused, or
   Failed jobs. You must remove any incomplete artifacts (resources)
   associated
   with a failed job before you continue with the upgrade. Any failed
   jobs will
   be marked as aborted by the upgrade process and cannot be restarted.

   Do you want 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 update.

```
====================================================================
==========================================
Oracle E-Business Suite Cloud Manager VM setup successful.
Version: 24.1.1
Refer to /u01/install/APPS/apps-unlimited-ebs/out/self-update-
<date>_<time>.log for complete details.
====================================================================
==========================================
```

Switch to File Storage Service:

As of version 22.2.1, Oracle E-Business Suite Cloud Manager uses the File Storage service (FSS) to create shared application tier file systems. After you update to Oracle E-Business Suite Cloud Manager version 22.2.1 or later, you must follow the instructions in these sections to enable FSS:

1. Assign FSS-related policies. See Assign Policies, page 2-8, Create Oracle Cloud Infrastructure Accounts and Resources, and Assign Policies, page 3-5, Create the Oracle E-Business Suite Administrators Group and Assign Policies.

2. Create custom FSS-related network resources. See Use a Custom Network, page 3-16.

   - Create an FSS mount target route table. See Create Route Tables, page 3-19.

   - Configure the FSS mount target network security. See Configure Network Security, page 3-21.

   - Create an FSS mount target subnet. See Create Subnets, page 3-23.

   - Create mount targets. See Create Mount Targets, page 3-26.

   - Create FSS-related security rules. See Create Security Rules, page 3-26.

3. Create an FSS-enabled network profile. See Create Network Profiles, page 3-44 and Create a Network Profile, page 8-6.

   Note: Note that when provisioning an FSS-based shared application tier file system, Oracle E-Business Suite Cloud Manager sets the APPLLDM variable to "product" so that concurrent manager log files are placed in a corresponding product directory under $APPLCSF.

Oracle E-Business Suite Cloud Manager will continue to support preexisting environments which do not use FSS. However, we strongly recommend that you convert your environments to FSS. You can do so by first backing up the preexisting environment, and then provisioning a new environment from that backup using an FSS-enabled network profile. See Create a Backup of a Cloud-Based Oracle E-Business Suite Environment, page 12-37 and Advanced Provisioning, page 9-7. Alternatively, if you manually configured FSS in an Oracle E-Business Suite environment, you can now use the Oracle E-Business Suite Cloud Manager Discovery feature to register that environment. See Discover an Oracle E-Business Suite Instance, page 10-1.

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 four sections:

- **Manage Services** - The `ebscloudmgrctl.sh` script is used to manage services, which include the following tasks:
    - Start Services, page 4-8
    - Stop Services, page 4-9
    - Abort Running Jobs, page 4-9
- **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 4-9
    - Change the Oracle E-Business Suite Cloud Manager Administration Password, page 4-11
    - Change the Oracle E-Business Suite Cloud Manager Administrator Group, page 4-11
    - View a List of Compatible Load Balancers, page 4-12
    - Change the Load Balancer Associated with Your Oracle E-Business Suite Cloud Manager VM, page 4-12
    - Update the Oracle E-Business Suite Cloud Manager Load Balancer URL, page 4-10
    - Update the Oracle E-Business Suite Cloud Manager Load Balancer Fully Qualified Domain Name (FQDN), page 4-13
    - Update the Oracle Identity Service Cloud Configuration, page 4-14
    - Change the Parallel Worker Count, page 4-15
    - Create a User Profile, page 4-15
    - Enable Mailer Configuration, page 4-16

  - Disable Mailer Configuration, page 4-16
  - Tag an Oracle E-Business Suite Environment, page 4-17

- **Resume Job Execution After Manual Intervention** - The `ebscmadmin` utility can be used to enable resumption of a failed job after steps have been taken to correct the underlying issue.
  - Resume Job Execution When Retry Button is Not Enabled, page 4-17
  - Resume Job Execution When Retry Button is Enabled, page 4-17

- **Standalone Tasks**
  - Replace the Self-Signed Certificate for the Oracle E-Business Suite Cloud Manager Load Balancer with a Certificate Authority Issued Certificate, page 4-17

> **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`:

```
$ { 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.

```
$ 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.

   ```
   $ 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 -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 in 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.

9. Expand **Client Configuration**.

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.
   xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

   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:

   ```
   $ 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.
   xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
   2: ebs1-lbaas -- ocid1.loadbalancer.oc1.uk-london-1.
   xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
   3: ebs2-lbaas -- ocid1.loadbalancer.oc1.uk-london-1.
   xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
   ```

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:

   ```
   $ 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:
   xxx
   Use "ebscmadmin update-load-balancer-url" command to update Oracle
   E-Business Suite Cloud Manager URL (Optional)
   ```

2. Now, sign in 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/ebscmadmin/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..
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

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.
Stopping Node and Job Server if running.
Starting Node and Job Server.
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 in 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 `ebscmadmin` with the `update-idcs-configuration` command.

   For example:

```
$ sudo su - oracle
$ cd /u01/install/APPS/apps-unlimited-ebs/bin
$ ./ebscmadmin update-idcs-configuration <argument>
```

Run `./ebscmadmin 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
$ ./ebscmadmin create-user-profile <argument>
```

Run ./ebscmadmin 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 ebscmadmin with the enable-mailer command.

For example:

```
$ sudo su - oracle
$ cd /u01/install/APPS/apps-unlimited-ebs/bin
$ ./ebscmadmin enable-mailer <argument>
```

Run ./ebscmadmin 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 ebscmadmin with the disable-mailer command.

For example:

```
$ sudo su - oracle
$ cd /u01/install/APPS/apps-unlimited-ebs/bin
$ ./ebscmadmin disable-mailer <argument>
```

Run ./ebscmadmin 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.
```

Resume Job Execution After Manual Intervention:

Resume Job Execution When Retry Button is Not Enabled

In the case where the **Retry** button is not enabled, you can use the following commands to update the status of a failed task to **Successful** in order to skip the task and enable the **Retry** button.

```
$ sudo su - oracle
$ cd /u01/install/APPS/apps-unlimited-ebs/bin
$ ./ebscmadmin update-task-status --env-name=<environment_name>
```

Then, click **Retry** to resume the job.

Resume Job Execution When Retry Button is Enabled

In the case where the **Retry** button is enabled but the retry fails (as it tries to rerun the failed task), the `force` option can be used to skip to the next task:

```
$ sudo su - oracle
$ cd /u01/install/APPS/apps-unlimited-ebs/bin
$ ./ebscmadmin update-task-status --env-name=<environment_name> --
force=true
```

Then, click **Retry** to resume the job.

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 4-10.

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.

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 Environments to Oracle Cloud Infrastructure

5

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

This chapter covers the following topics:

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 9-7.

Note: Although this process is intended primarily for on-premises source environments, 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 Environment, page 12-37.

- 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 environment 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 5-11

4. Install the Oracle E-Business Suite Cloud Backup Module., page 5-11

5. Create an advanced configuration parameters file (optional)., page 5-12

6. Create a backup with the Oracle E-Business Suite Cloud Backup Module., page 5-14

7. Troubleshoot backup issues., page 5-25

Related Topics

Backing Up a Database to Object Storage Using RMAN [https://docs.cloud.oracle.com/en-us/iaas/Content/Database/Tasks/backingupOSrman.htm]

Oracle Database Backup and Recovery User's Guide 19c [https://docs.oracle.com/en/database/oracle/oracle-database/19/bradv/toc.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 environment 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 Cloud 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, see: Configuring the ntpd Service [https://docs.oracle.com/en/operating-systems/oracle-linux/7/network/ol7-nettime.html#section_m5p_j1h_pp] in *Oracle Linux 7: Setting Up Networking*. For Oracle Linux Release 6, see Configuring the ntpd Service [https://docs.oracle.com/cd/E37670_01/E41138/html/section_m5p_j1h_pp.html] in the *Oracle Linux Administrator's Guide for Release 6*.

- 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 Transparent Data Encryption (TDE) is enabled for the source environment, then the TDE wallet must be located on your regular file system. The Oracle E-Business Suite Cloud Backup Module and Oracle E-Business Suite Cloud Manager do not support wallets located on an Oracle Automatic Storage Management (ASM) disk.

- 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.

  - 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 5.1: Apply Required Updates and Patches.

  - 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 5.1: Apply Required Updates and Patches.

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 Base Database Service 1-Node or 2-Node DB System, you can choose from the following database edition options:

  - Base Database Service 1-Node DB System (Single Instance):

        - Enterprise Edition
        - Enterprise Edition High Performance
        - Enterprise Edition Extreme Performance
    - Base Database Service 2-Node DB System (Oracle RAC)
        - Enterprise Edition Extreme Performance

- For creating a backup with the target database tier on Exadata Database Service Dedicated: Exadata Database Service Dedicated provides Oracle RAC support.

- 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 Environment 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 About Oracle Base Database Service [https://docs.oracle.com/en-us/iaas/dbcs/doc/bare-metal-and-virtual-machine-db-systems.html#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 Base Database Service or Exadata Database Service Dedicated 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 Database Service Dedicated 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/`

Table 5-1 Cloud Services Minimum Resource Recommendations

Description	Machine Type	Number of Nodes	OCPUs Allocated	Memory	Storage	External IPs
Oracle Cloud Infrastructure Backup Service	Not applicable	Not applicable	Not applicable	Not applicable	Size of application tier backup + database backup (object)	Not applicable
Oracle E-Business Suite Cloud Manager	VM	1	1	7 GB	Required: 55 GB (block)	1

Description	Machine Type	Number of Nodes	OCPUs Allocated	Memory	Storage	External IPs
A load balancer (You can use your own load balancer or Load Balancer as a Service [LBaaS])	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	1
Application tier	VM	n (where 'n' is the number of application tier nodes in the target environment)	n*m (where 'm' is the number of OCPUs in the shape selected for the application tier; the minimum for 'm' is 1)	Release 12.2 = 14 GB per VM Release 12.1 = 7 GB per VM	Strictly dependent on your on-premises environment. The minimum requirements are as follows: 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)	n

Description	Machine Type	Number of Nodes	OCPUs Allocated	Memory	Storage	External IPs
Database tier on Oracle Cloud Infrastructure Compute	VM	1	2	14 GB	Vision demo: 300 GB	1
Database tier on Base Database Service 1-Node DB System (Single Instance)	VM	1	1	15 GB	Vision demo: 256 GB Total storage: 712 GB [1]	1
Database tier on Base Database Service 2-Node DB System (Oracle RAC)	VM	2	2 per VM	30 GB per VM	Vision demo: 256 GB Total storage: 912 GB [1]	2
Database tier on Exadata Database Service Dedicated (Oracle RAC) [2]	See footnote [2]	See footnote [2]	See footnote [2]	See footnote [2]	See footnote [2]	See footnote [2]

Footnotes for Table 5-4:

1. The Available Storage Size and Total Storage Size are different. For more information, see About Oracle Base Database Service [https://docs.oracle.com/en-us/iaas/dbcs/doc/bare-metal-and-virtual-machine-db-systems.html#StorageConsiderations].

2. For a database tier on Exadata Database Service Dedicated, the minimum requirement is an Exadata X9M, X8M, X7 or X6 base model with a 2-node Oracle

RAC.

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 100". 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.

1. Download Patch 36331515 [https://updates.oracle.com/download/36331515.html] from My Oracle Support to the backup module server.

2. Using the following commands, change to the directory where you downloaded the patch file and extract the downloaded patch.

   ```
   $ cd <download_folder>
   $ unzip p36331515_R12_GENERIC.zip
   ```

   Unzipping the patch zip file creates a directory named `36331515/RemoteClone`.

3. Change to the `RemoteClone` directory and change the permission to "execute" for all the downloaded scripts.

   ```
   $ cd 36331515/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 Database Service Dedicated subscriptions, and in Base Database Service 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 `4G`. 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 5-25. 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 environment 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.

   ```
   $ 3pt/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 9-7.

     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

====================================================================
=

[Ctrl-B: Back, Ctrl-H: Main Menu]

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/12.1.0/appsutil/EBSDB_apps.xml
OS Time Zone                                        :
America/Los_Angeles
Database Transparent Data Encrypted ( TDE ): ( Yes | No ) yes
Wallet 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/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 Source Application 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                  :
```

9. 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.

   - If Oracle E-Business Suite System Schema Migration has been completed on the source environment, then enter the EBS_SYSTEM password. For more information, see My Oracle Support Knowledge Document 2755875.1, *Oracle E-Business Suite Release 12.2 System Schema Migration* [https://support.oracle.com/rs?type=doc&id=2755875.1].

```
=====================================================================
====
               Migrate Oracle E-Business Suite - Enter Source
Application Tier Details

=====================================================================
====

[Ctrl-B: Back, Ctrl-H: Main Menu]

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

EBS System 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 5-12, 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.

```
               ================================================
               Enter Oracle Cloud Infrastructure 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                   :
```

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 Base Database Service 1-Node or 2-Node DB System, enter **Base Database Service DB System**.

        - For Exadata Database Service Dedicated, enter **Exadata Database Service**.

```
====================================================================
========
               Migrate Oracle E-Business Suite - Enter Oracle Cloud
Infrastructure Details

====================================================================
========

[Ctrl-B: Back, Ctrl-H: Main Menu]

Oracle Cloud User OCID : ocid1.user.oc1..
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Oracle Cloud Fingerprint : xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:
xx:xx:xx
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..
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Oracle Cloud Region : xx-xxxxxx-1
Oracle Cloud Tenant Name : example
Oracle Cloud Compartment OCID : ocid1.compartment.oc1..
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Target Database Type - ( Compute | Base Database Service DB System |
Exadata Database Service ): Base Database Service 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 Base Database Service or Exadata Database Service Dedicated

    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
               =========================================

[Ctrl-B: Back, Ctrl-H: Main Menu]




Mode                           : BMCS_CDB


Source Database Details:

Host Name                      : demo.example.com
Custom Private Key Location    : /home/oracle/.ssh/id_rsa
OS User Name                   : oracle
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..
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Oracle Cloud Fingerprint                       : xx:xx:xx:xx:xx:xx:
xx:xx:xx:xx:xx:xx:xx:xx:xx:xx
Oracle Cloud Tenancy OCID                      : ocid1.tenancy.oc1..
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Oracle Cloud Region                            : xx-xxxxxx-1
Oracle Cloud Tenant Name                       : example
Oracle Cloud Compartment OCID                  : ocid1.compartment.
oc1..xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Target Database Type                           : Base Database
Service DB System



                ============================
                Proceed With Selected Action
                ============================

[Ctrl-B: Back, Ctrl-H: Main Menu]
```

```
1: Yes
2: No

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.

15. You can use Oracle E-Business Suite Cloud Manager to provision an environment on Oracle Cloud Infrastructure based on the backup you created. See Review Backups, page 12-46, Review Environment Details, page 11-7, and Advanced Provisioning, page 9-7.

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 Delete a Backup, page 12-49.

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 5-12 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 instructions in Create a Backup with the Oracle E-Business Suite Cloud Backup Module, page 5-14, 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 during a traditional lift and shift 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 environment 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 5-12.

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.

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 19c or 12.1.0.2 (Commercial Cloud Regions Only)

This chapter covers the following topics:

- Overview
- Requirements for Creating a Standby Environment
- Preparations for Creating a Standby Environment
- Create a Standby Environment for Oracle Cloud Infrastructure from an On-Premises Environment

Overview

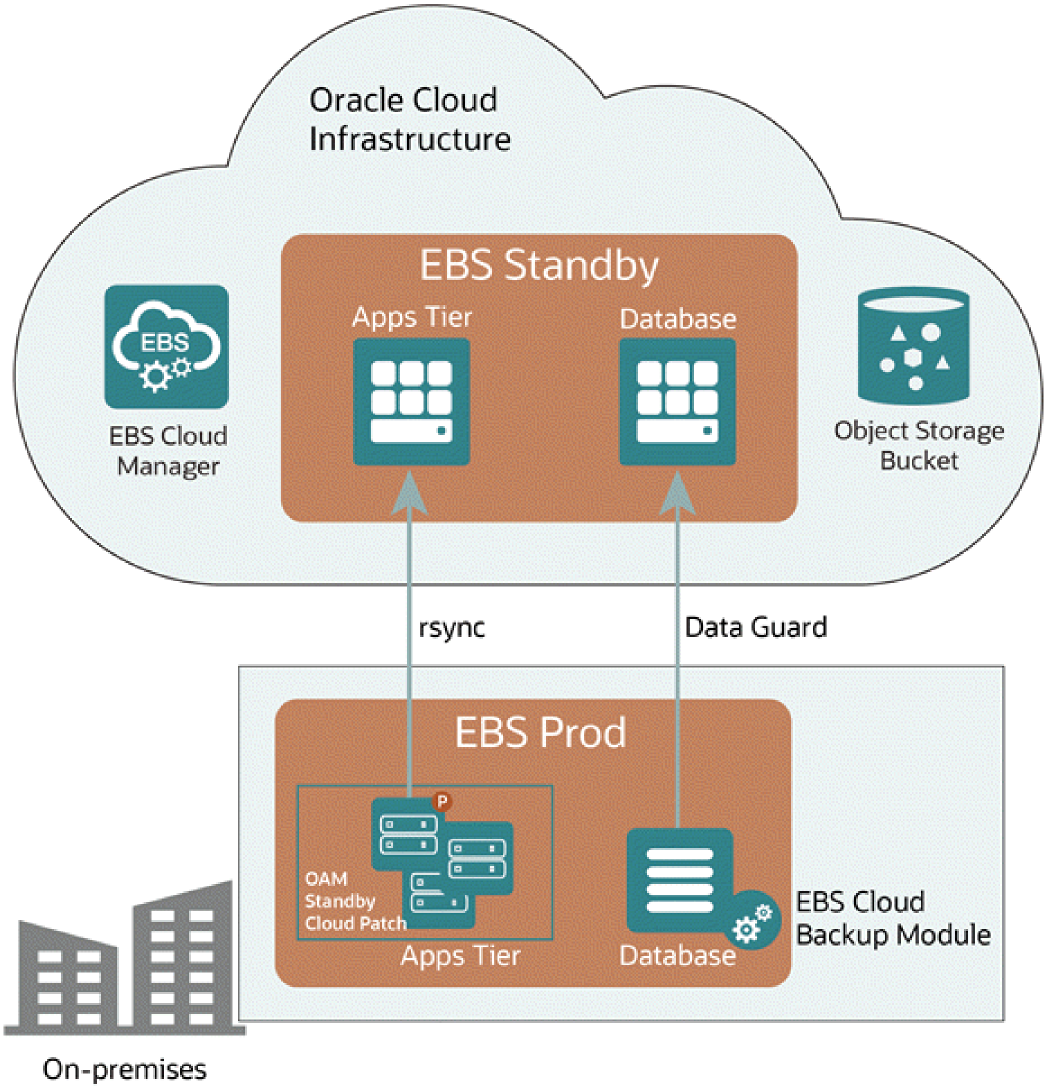
This chapter describes how you can use Oracle E-Business Suite automation (and in particular, the on-premises Oracle Applications Manager combined with the Oracle E-Business Suite Cloud Manager) to create a standby environment in Oracle Cloud Infrastructure.

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 Environment 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 Releases 19c and 12.1.0.2, with the target of Compute.

Overview of Creating a Standby Environment



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.

An Oracle Applications Manager standby cloud patch must be applied to your application tier and the Oracle E-Business Suite Cloud Backup module must be installed in your database tier. See 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] for more information.

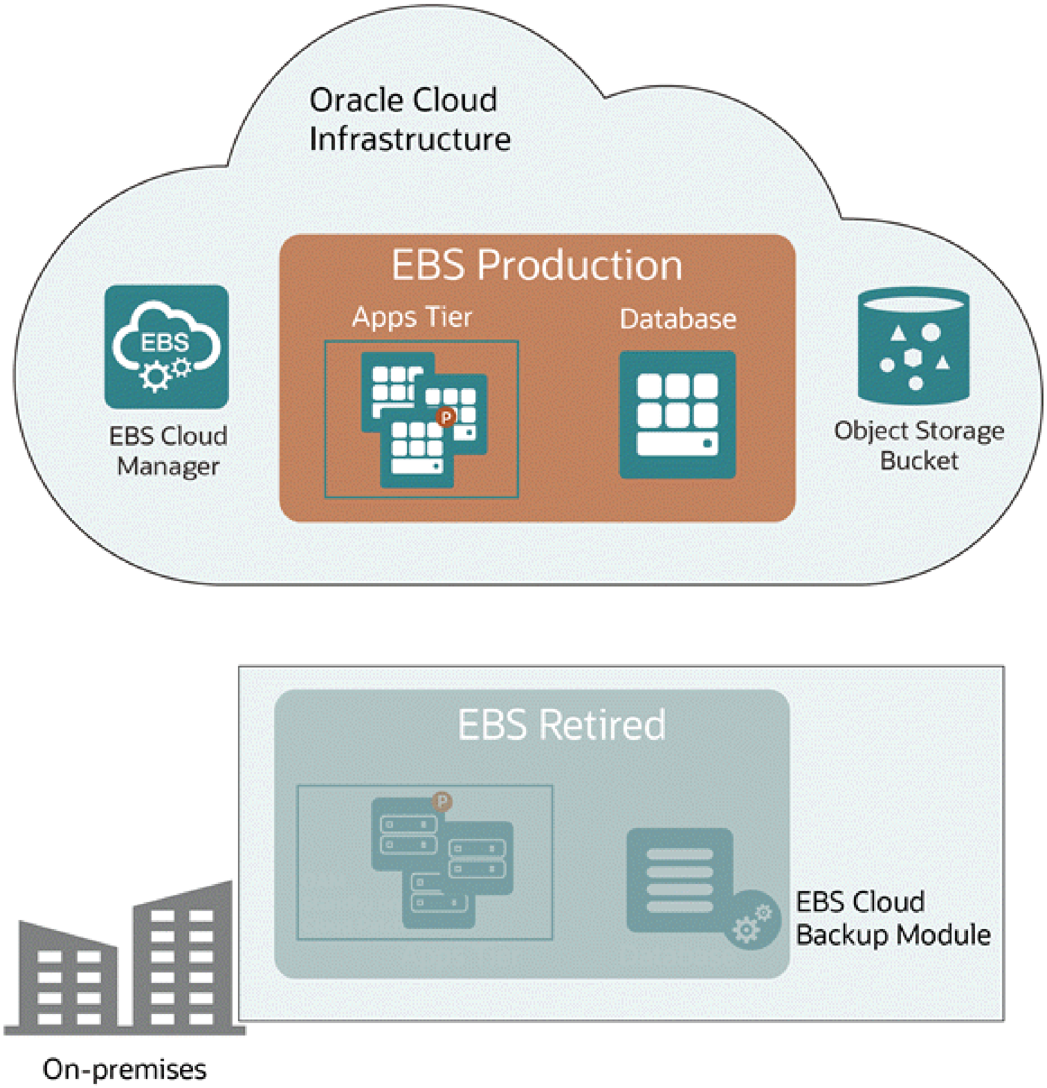
The Oracle E-Business Suite Cloud Backup Module is used to introspect the database tier, create a backup of the Database Oracle Home in Oracle Cloud Infrastructure Object

Storage and configure Oracle Data Guard on the source database.

The utility `rsync` is used to transfer the files on the applications tier, and Oracle Data Guard helps create and maintain the standby database. Once the standby environment is created in OCI using an Oracle Cloud Infrastructure Storage bucket to store its objects in a compartment, Oracle E-Business Suite Cloud Manager can manage the standby.

Once the standby environment is created in OCI, you can promote it to production using Oracle E-Business Suite Cloud Manager. The on-premises environment is then retired.

A Standby Environment Promoted to Production



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 6-1 Cloud Services Minimum Resource Recommendations

Description	Machine Type	Number of Nodes	OCPUs Allocated	Memory	Storage	External IPs
Oracle Cloud Infrastructure Backup Service	Not applicable	Not applicable	Not applicable	Not applicable	Size of the database Oracle home in the source environment (object)	Not applicable
Oracle E-Business Suite Cloud Manager	VM	1	1	7 GB	Required: 55 GB (block)	1
Application tier	VM	1	1	14 GB per VM	Strictly dependent on your on-premises environment. The minimum requirements are as follows: 170 GB	1
Database tier on Oracle Cloud Infrastructure Compute	VM	1	2	14 GB	Vision demo: 300 GB	1

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.

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 6-6.

2. Ensure that you have applied all required patches listed for "Lift and Shift Oracle E-Business Suite from On-Premises" 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].

3. Apply Patch 36272638 [https://updates.oracle.com/download/36272638.html] to the source application tier using adop.

4. After completing the adop cycle, run `adpreclone.pl` on the new run filesystem on the source application tier.

Set Up the Source Database Tier

1. Ensure that the database is in Archive log mode.

2. Create wallet and autologin files if the database does not already have them.

   For Database Release 12.1.0.2, ensure that the `sqlnet.ora` file in the context directory is updated with the correct wallet location. For Database 19c, ensure that the `sqlnet.ora` files of both the multitenant container database (CDB), `NATIVE_TNS_ADMIN/sqlnet.ora`, and the pluggable database (PDB), `TNS_ADMIN/sqlnet.ora`, are updated with the correct wallet location.

   If your database is Release 12.1.0.2, then sample commands are as follows:

```
$ sqlplus '/as sysdba'
SQL> ADMINISTER KEY MANAGEMENT CREATE KEYSTORE
'<ORACLE_HOME>/admin/<SID>/<tde_wallet>' IDENTIFIED BY
<Wallet_password>;
SQL> ADMINISTER KEY MANAGEMENT SET KEYSTORE OPEN IDENTIFIED BY
<Wallet_password>;
SQL> ADMINISTER KEY MANAGEMENT SET KEY IDENTIFIED BY
<Wallet_password> WITH BACKUP;
SQL> ADMINISTER KEY MANAGEMENT CREATE AUTO_LOGIN KEYSTORE FROM
KEYSTORE '<ORACLE_HOME>/admin/<SID>/<tde_wallet>' IDENTIFIED BY
<Wallet_password>;
```

If your database is Release 19c, connect to the CDB. The sample commands are as follows:

```
sqlplus '/as sysdba'
SQL> ADMINISTER KEY MANAGEMENT CREATE KEYSTORE
'<ORACLE_HOME>/admin/<CDB_SID>/<tde_wallet>' IDENTIFIED BY
<Wallet_password>;
SQL> ADMINISTER KEY MANAGEMENT SET KEYSTORE OPEN IDENTIFIED BY
<Wallet_password> CONTAINER=ALL;
SQL> ADMINISTER KEY MANAGEMENT SET KEY IDENTIFIED BY
<Wallet_password> WITH BACKUP CONTAINER=ALL;
SQL> ADMINISTER KEY MANAGEMENT CREATE AUTO_LOGIN KEYSTORE FROM
KEYSTORE '<ORACLE_HOME>/admin/<SID>/<tde_wallet>' IDENTIFIED BY
<Wallet_password>;
```

Ensure that the `sqlnet.ora` files (in `$ORACLE_HOME/network/admin` and `$ORACLE_HOME/network/admin/<context_dir>`) have an ENCRYPTION_WALLET_LOCATION entry like below:

```
ENCRYPTION_WALLET_LOCATION = (SOURCE=(METHOD=FILE)(METHOD_DATA=
(DIRECTORY=<ORACLE_HOME>/admin/<SID>/<tde_wallet>)))
```

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, take a backup and 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. For Database Release 12.1.0.2, run the script:

        ```
        $ $ORACLE_HOME/perl/bin/perl $ORACLE_HOME/appsutil/scripts/
        <CONTEXT_NAME>/adpreclone.pl dbTier
        ```

For Database 19c, source the PDB_context.env file and then run the script:

```
$ $ORACLE_HOME/perl/bin/perl $ORACLE_HOME/appsutil/scripts/
<CONTEXT_NAME>/adpreclone.pl dbTier
```

Perform Maintenance on the Standby Environments

Make sure you delete or promote all existing standby environments before performing maintenance activities on the source environment.

Install the Oracle E-Business Suite Cloud Backup Module

1. 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 5-11 for more information.

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:

    1. Copy the `democert.crt` 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/ca
        certs -file democert.crt -alias sample2021webentry
        ```

        ```
        $ keytool -import -trustcacerts -keystore
        /u01/install/APPS/fs2/EBSapps/comn/util/jdk64/jre/lib/security/ca
        certs -file democert.crt -alias sample2021webentry
        ```

        > **Note:** You might need to grant write permissions to the `cacerts` file using the command:
        >
        > `$ chmod u+w <cacerts_file>`
        >
        > The write permissions can be revoked after running the above `keytool` command using:
        >
        > `$ chmod u-w <cacerts_file>`
        >
        > If prompted, enter the keystore password. See: The `cacerts` Certificate File [https://docs.oracle.com/javase/8/docs/technotes/tools/unix/keytool.html#cacerts].
        >
        > For more information on managing the JDK `cacerts` file, refer

> to My Oracle Support Knowledge Document 1367293.1, *Enabling TLS in Oracle E-Business Suite Release 12.2*.

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. For configuring self-signed certificates for Cloud Manager URLs with IP address, refer to Manual Steps For a Self-Signed Certificate (Conditionally Required), page 6-10.

To learn more about running the `ebscmadmin` utility to update the FQDN, see: Update the Oracle E-Business Suite Cloud Manager Load Balancer Fully Qualified Domain Name, page 4-13.

1. Run the `ebscmadmin` 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:

   ```
   $ sudo su - oracle
   $ cd /u01/install/APPS/apps-unlimited-ebs/bin
   $ ./ebscmadmin update-load-balancer-fqdn <argument>
   ```

2. Import the certificate to your source application tier nodes:

   1. Copy the `democert.crt` 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/ca
      certs -file democert.crt -alias sample2021webentry
      ```

      ```
      $ keytool -import -trustcacerts -keystore
      /u01/install/APPS/fs2/EBSapps/comn/util/jdk64/jre/lib/security/ca
      certs -file democert.crt -alias sample2021webentry
      ```

      > **Note:** You might need to grant write permissions to the `cacerts` file using the command:
      >
      > ```
      > $ chmod u+w <cacerts_file>
      > ```

The write permissions can be revoked after running the above `keytool` command using:

```
$ chmod u-w <cacerts_file>
```

If prompted, enter the keystore password. See: The `cacerts` Certificate File [https://docs.oracle.com/javase/8/docs/technotes/tools/unix/keytool.html#cacerts].

For more information on managing the JDK `cacerts` file, refer to My Oracle Support Knowledge Document 1367293.1, *Enabling TLS in Oracle E-Business Suite Release 12.2*.

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).

   For example, say you are using the IP address of the load balancer as your web entry point. Log in to the Cloud Manager VM and run the command as in the following example:

   ```
   $ 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-instance-prov-vm-lbaas`

   2. Select the corresponding load balancer in the OCI Console. Under **Resources**, click **Certificates**. From the **Certificate Resource** list, select the **Load Balancer Managed Certificate** certificate resource type. Click **Add Certificate**.

   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 `democert.crt` 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/ca
   certs -file democert.crt -alias sample2021webentry
   ```

   ```
   $ keytool -import -trustcacerts -keystore
   /u01/install/APPS/fs2/EBSapps/comn/util/jdk64/jre/lib/security/ca
   certs -file democert.crt -alias sample2021webentry
   ```

   > **Note:** You might need to grant write permissions to the `cacerts` file using the command:
   >
   > `$ chmod u+w <cacerts_file>`
   >
   > The write permissions can be revoked after running the above `keytool` command using:
   >
   > `$ chmod u-w <cacerts_file>`
   >
   > If prompted, enter the keystore password. See:The `cacerts` Certificate File [https://docs.oracle.com/javase/8/docs/technotes/tools/unix/keytool.html#cacerts].
   >
   > For more information on managing the JDK `cacerts` file, refer to My Oracle Support Knowledge Document 1367293.1, *Enabling TLS in Oracle E-Business Suite Release 12.2*.

5. Stop and start the Oracle E-Business Suite instance.

Set Up Networking:

Reserved Public IP Addresses

For information on managing public IP addresses, see: Public IP Addresses [https://docs.cloud.oracle.com/en-us/iaas/Content/Network/Tasks/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.

Opening Ports

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.

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.

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)

   The following are example commands to open the local firewall for Standby (Oracle Linux 7). The command could vary depending on the operation system version.

   ```
   sudo firewall-cmd --zone=public --add-rich-rule 'rule family=ipv4
   source address=<standby-oci-db-reserved-ip> port port=<active db
   listener port, eg. 1521> protocol=tcp accept' --permanent
   ```

   ```
   sudo firewall-cmd --zone=public --add-rich-rule 'rule family=ipv4
   source address=<standby-oci-db-reserved-ip> port port=<active db
   listener port, eg. 1521> protocol=tcp accept
   ```

4. From the Source application tier, access the Oracle E-Business Suite Cloud Manager URL.

Reserved Private IP Addresses

Creating a reservation is unnecessary in this scenario.

1. 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.

Create a Standby Environment for Oracle Cloud Infrastructure from an On-Premises Environment

> **Important:** Before configuring a standby environment, ensure that there is an ingress rule defined in the Oracle E-Business Suite Cloud Manager LBaaS security list that allows connectivity from the on-premises Oracle E-Business Suite application tier node IP address. Otherwise, validation will not occur.
>
> Ensure that the proxy values are set in the context file accordingly, run AutoConfig, and stop and start the application tier services.
>
> If the proxy is used, set values for `s_proxyhost`, `s_proxyport`, `s_proxybypassdomain`, `s_nonproxyhosts` in the context file. If the

proxy is not used, ensure these context values are cleared. To remove any proxy settings and also retain the null values for the proxy settings, set the following context variables as described below and run AutoConfig:

```
<proxyhost oa_var="s_proxyhost"></proxyhost>
<proxyport oa_var="s_proxyport" customized="yes"
></proxyport>
<proxybypassdomain oa_var="s_proxybypassdomain"
customized="yes"></proxybypassdomain>
<nonproxyhosts oa_var="s_nonproxyhosts"></nonproxyhosts>
```

To run AutoConfig:

```
cd $ADMIN_SCRIPTS_HOME ; ./adautocfg.sh
```

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 2-41.

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, including the port if needed.

  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. We recommend you choose a Network Profile enabled for the File Storage service. See Create a Network Profile, page 8-6 for instructions.
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
- OS User
- Application Top directory
- Middleware Licensing model
- File System Type

  For a shared file system, the File Storage Mount Target and Mount Options are shown.

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 5-11.

2. Run the `db-introspect.sh` script. For example:

   ```
   $ RemoteClone/bin/db-introspect.sh --action introspect --context-
   file <context file, for example: /u01/install/APPS/12.1.0
   /appsutil/demosid_demo1221ccomp1db.xml> --standby-name <standby
   environment name given in the Introspect Application Tier page> --
   standby-reserved-ip <standby reserved IP or private IP depending on
   the --standby-reserved-ip-type> --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>
   --session-dir <absolute path session log directory, for example:
   /home/oracle/session>
   ```

   Note the following for the parameters for the script:

   - 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 6-13.
   - If the `--standby-reserved-ip-type` value is Public, then the `--standby-reserved-ip` value must be a Public IP reservation created in OCI. If `--standby-reserved-ip-type` value is Private, then the `--standby-reserved-ip` value must be a Private IP that belongs to the DB Subnet CIDR Block and is not already assigned.
   - For `-active-db-ip <active database IP reachable from target network>`: This IP is used to connect to the active database from standby and

also this IP is used to open local firewall on the standby database. Depending on the network configuration (Public or Private), use the active DB IP that is reachable from the standby to active and also for the successful communication from active to standby when this IP is allowed in the local firewall of the standby.

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.

   Flexible shapes are supported for both application and database tiers. Flexible shapes allow you to customize the number of OCPUs and the amount of memory when launching or resizing your VM.

3. Choose a middleware licensing model, either BYOL or UCM. If you choose BYOL, you are indicating that you have purchased or transferred the perpetual licenses required for customized Oracle E-Business Suite Applications. If you choose UCM, you are adopting the Universal Credits subscription-based model, and paying for usage as you go. Make sure you understand the cost associated with this choice.

4. For Storage, choose the **File System Type**: Non-Shared or Shared.

   If you choose Shared, then you are prompted for the File Storage Mount Target. Select a mount target from the list shown; this list of values is dependent on the network profile you selected during application tier introspection.

   You can also specify Mount Options. Default parameters are shown. You can edit these options, but specifying a mount option or parameter that is not supported or recommended for a shared storage file system deployment may result in a provisioning failure. Exercise extreme caution when editing these parameters; options are not validated in this page.

5. 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 11-13.

From Oracle E-Business Cloud Manager, you can also:

- Promote a Standby Environment, page 12-56
- Delete a Standby Environment, page 12-63

Part 4

Manage Oracle E-Business Suite Environments Using Oracle E-Business Suite Cloud Manager

7

Access Oracle E-Business Suite Cloud Manager

This chapter covers the following topics:

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 1-2.

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].

- A minimum of 10 GB of free disk space in order to run Oracle E-Business Suite Cloud Manager jobs, including provisioning, discovery, configuration, and all lifecycle management activities.

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 7-6

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 avatar icon, labeled with your name, 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 avatar icon, labeled with your name, 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 realm where your Oracle E-Business Suite Cloud Manager instance is located, either Commercial Cloud (OC1) or US Government Cloud (OC2), and whether the Oracle E-Business Suite Cloud Manager instance uses metadata available through a public internet connection or local metadata.

   For a Commercial Cloud instance, the 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. In the Oracle E-Business Suite Cloud Manager header, set the **EBS Compartment** field to the compartment in which you want to work. Oracle E-Business Suite Cloud Manager displays only resources and administration details pertaining to that compartment. By default, the compartment is set to the root compartment of your Oracle Cloud Infrastructure account.

   > **Note:** The header also displays the region and the tenancy in which your Oracle E-Business Suite Cloud Manager instance is located.

2. To review and manage your Oracle E-Business Suite environments, click the **Navigator** icon, and then select **Environments**. See Review Environments, page 7-6.

3. 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 12-46.

   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 Environment on Oracle Cloud Infrastructure, page 5-2 and Create a Backup of a Cloud-Based Oracle E-Business Suite Environment, page 12-37.

   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 11-7.

4. To monitor the status of the jobs performed in Oracle E-Business Suite Cloud Manager, click the **Navigator** icon, and then select **Jobs**. See Monitor Job Status, page 13-1.

   You can also review a list of the jobs performed for a particular environment in the environment details page for that environment. See Review Environment Details, page 11-7.

5. 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.

   > **Note:** To have Oracle E-Business Suite Cloud Manager administrator privileges, a user must be a member of the Oracle E-Business Suite Cloud Manager administrator group that was specified during configuration of this Oracle E-Business Suite Cloud Manager instance. For more details, see Configure Oracle E-Business Suite Cloud Manager Compute Instance, page 2-37.

6. If you are logged in as an Oracle E-Business Suite Cloud Manager administrator, then to extend Oracle E-Business Cloud Manager jobs to meet your own requirements, click the **Navigator** icon, select **Administration**, and then select **Extensibility**. You can create extended job definitions for provisioning, cloning, and promoting standby environments. See Set Up the Extensibility Framework, page 8-10.

> **Note:** To have Oracle E-Business Suite Cloud Manager administrator privileges, a user must be a member of the Oracle E-Business Suite Cloud Manager administrator group that was specified during configuration of this Oracle E-Business Suite Cloud Manager instance. For more details, see Configure Oracle E-Business Suite Cloud Manager Compute Instance, page 2-37.

7. To submit a discovery request for a manually deployed environment or an upgraded environment, click the **Navigator** icon, select **Administration**, and then select **Discovery**. See Discover an Oracle E-Business Suite Instance, page 10-1.

8. To set up scheduling policies for backups, click the **Navigator** icon, select **Administration**, and then select **Scheduling Policies**. See Set Up Scheduling Policies, page 8-17.

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 reside within the compartment that is selected in the **EBS Compartment** field in the Oracle E-Business Suite Cloud Manager header.

   > **Note:** To have Oracle E-Business Suite Cloud Manager administrator privileges, a user must be a member of the Oracle E-Business Suite Cloud Manager administrator group that was specified during configuration of this Oracle E-Business Suite Cloud Manager instance. For more details, see Configure Oracle E-Business Suite Cloud Manager Compute Instance, page 2-37.

   > **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 upgrade that environment to Oracle Database 19c, then you must unregister and rediscover the upgraded environment to update its metadata within Oracle E-Business Suite Cloud Manager. Similarly, if you used Oracle E-

Business Suite Cloud Manager to deploy an Oracle E-Business Suite Release 12.1.3 environment, and you upgrade that environment to Release 12.2, then you must unregister and rediscover the upgraded environment. See Discover an Oracle E-Business Suite Instance, page 10-1.

After performing rediscovery, you can continue managing the environment through Oracle E-Business Suite Cloud Manager.

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
   - Last job 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 9-4 or Advanced Provisioning, page 9-7.

4. To review additional details for an environment, including any backups created from that environment and jobs 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 11-7 and Review Standby Environment Details, page 11-13.

5. To review details for the last job performed for an environment, click the job status link. See Monitor Job Status, page 13-1.

6. To clone an environment, click the **Actions** icon next to that environment, and then select **Clone**. Note that you can use this cloning method only for an existing environment that was successfully provisioned on Compute or Base Database Service DB System. See Clone an Oracle E-Business Suite Instance, page 12-5.

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 Environment, page 12-37.

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 12-56.

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 12-62.

8

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 environments.

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.

> **Note:** The default network created by the `ProvisionOCINetwork.pl` script supports internal zones only, does not support the File Storage Service, and does not leverage network security groups. To take advantage of advanced options, you must create your own custom network profile.

- Review Network Profiles, page 8-2
- Create a Network Profile, page 8-6
- Delete a Network Profile, page 8-10
- Known Limitation, page 8-10

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, within the compartment that is selected in the **EBS Compartment** field in the Oracle E-Business Suite Cloud Manager header. 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
   - Virtual Cloud Network (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 8-6.

- 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 8-6.
- 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.

> **Note:** To have Oracle E-Business Suite Cloud Manager administrator privileges, a user must be a member of the Oracle E-Business Suite Cloud Manager administrator group that was specified during configuration of this Oracle E-Business Suite Cloud Manager instance. For more details, see Configure Oracle E-Business Suite Cloud Manager Compute Instance, page 2-37.

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
   - Virtual Cloud Network (VCN)
   - Network profile description
   - Oracle E-Business Suite compartment
   - Subnet type
   - Network compartment
   - Availability domain

6. In the Database Tier Subnet Mapping region, review the following properties:

   - Database tier subnet access, either Public or Private
   - Database tier subnet
   - Database tier network security group

7. In the Applications Tier Subnet Mapping region, review the following properties:

   - Application tier internal zone
     - Application tier nodes subnet access, either Public or Private
     - Application tier nodes subnet
     - Application tier nodes network security group
     - 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)
     - Load balancer network security group
   - 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
     - Application tier nodes network security group
     - 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)
     - Load balancer network security group
   - Storage (displayed only if support for the File Storage service is enabled for this

network profile)

- Mount target subnet access, either Public or Private
- Mount target subnet

8. 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 8-6.
   - 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.

   > **Note:** To have Oracle E-Business Suite Cloud Manager administrator privileges, a user must be a member of the Oracle E-Business Suite Cloud Manager administrator group that was specified during configuration of this Oracle E-Business Suite Cloud Manager instance. For more details, see Configure Oracle E-Business Suite Cloud Manager Compute Instance, page 2-37.

Create a Network Profile:

You must be logged in as an Oracle E-Business Suite Cloud Manager administrator to perform the steps in this section.

> **Note:** To have Oracle E-Business Suite Cloud Manager administrator privileges, a user must be a member of the Oracle E-Business Suite Cloud Manager administrator group that was specified during configuration of this Oracle E-Business Suite Cloud Manager instance. For more details, see Configure Oracle E-Business Suite Cloud Manager Compute Instance, page 2-37.

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.

When you create a network profile, you must specify subnet mappings for the database tier and for application tier nodes in internal zones. You can optionally enable external zones for the application tier and specify the corresponding subnet mappings.

If you want to use security rules that apply only for a particular VM, rather than for the entire subnet, you can optionally specify network security groups for the database tier and application tier nodes and for the load balancer. You can select a maximum of five network security groups for each tier.

Additionally, you can optionally enable the File Storage service for the application tier of your Oracle E-Business Suite environments and specify the subnet mapping for the File Storage service mount target. If you plan to use this option, ensure that you have set up your custom network to support the File Storage service, including creating the necessary mount targets. See 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 Network Profile region of the Provision Network Profiles page, enter the following details:

   - **Network Profile Name**: Enter a name for the network profile, such as `ebsprodlondonad1-profile`. The name should represent the logical grouping of environments that will be provisioned using this network profile.

   - **Network Profile Description**: Optionally enter a description for the network profile.

   - **EBS Compartment**: Select the Oracle E-Business Suite compartment for this profile, such as `ebsprod-compartment`.

     > **Note:** The compartments you can select are determined by policies defined in Oracle Cloud Infrastructure Identity and Access Management.

3. In the Network Mapping, region, enter the following details:

   - **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.

- **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`.

- **Virtual Cloud Network**: Select a Virtual Cloud Network (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 Base Database Service resources will be created, such as `POKh:UK-LONDON-1-AD-1`.

4. In the Database Tier Subnet Mapping 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`.

   - **Network Security Group**: Optionally select one or more network security groups for the database tier, up to a maximum of five.

5. In the Applications Tier Subnet Mapping 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`.

   - **App Nodes Network Security Group**: Optionally select one or more network security groups for the application tier nodes in internal zones, up to a maximum of five.

   - **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.

- **Load Balancer Network Security Group**: Optionally select one or more network security groups for the application tier load balancer in internal zones, up to a maximum of five.

6. After entering the internal zone details, optionally click the **Support for External Zones** toggle switch in the Applications Tier Subnet Mapping region to enable external zones for this network profile. If you do so, additional detail fields appear. 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`.

   - **App Nodes Network Security Group**: Optionally select one or more network security groups for the application tier nodes in external zones, up to a maximum of five.

   - **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.

   - **Load Balancer Network Security Group**: Optionally select one or more network security groups for the application tier load balancer in external zones, up to a maximum of five.

7. After entering the zone details, optionally click the **Support for File Storage Service** toggle switch in the Applications Tier Subnet Mapping region to enable the File Storage service for this network profile. If you do so, additional detail fields appear. Enter the following details for the File Storage service mount target:

   - **Mount Target Subnet Access**: Select either **Public** or **Private**.

- **Mount Target Subnet**: Select the subnet for the File Storage service mount target, such as `apps-subnet-ad1`.

  > **Note:** It is recommended that you use the same subnet for the application tier of an Oracle E-Business Suite environment and for its file system mount target. However, you can select any available subnet for the mount target.

8. By default, during creation of the network profile, Oracle E-Business Suite Cloud Manager validates the security rules associated with the security lists that are attached to the subnets defined for the network profile, and ensures that all necessary ingress and egress rules are in place to allow communication between the subnets. If you do not want to perform this validation, select the **Skip Network Validation** checkbox.

   If you define a network security group for any level of the network profile, then the **Skip Network Validation** checkbox is selected by default and you cannot change this setting.

9. Click **Submit**.

10. You can check the status of the job to create the network profile in the Jobs page. Locate the `create-network-profile` job that you want to monitor, and click the job name link to go to the Job Details page. See Monitor Job Status, page 13-1.

    When you create a network profile, unless you have chosen to skip network validation, the `create-network-profile` job 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 Job 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 job 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` job from the Job Details page. See Monitor Job Status, page 13-1.

    - 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` job. See Monitor Job Status, page 13-1.

> **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 must be logged in as an Oracle E-Business Suite Cloud Manager administrator to perform the steps in this section.

> **Note:** To have Oracle E-Business Suite Cloud Manager administrator privileges, a user must be a member of the Oracle E-Business Suite Cloud Manager administrator group that was specified during configuration of this Oracle E-Business Suite Cloud Manager instance. For more details, see Configure Oracle E-Business Suite Cloud Manager Compute Instance, page 2-37.

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 jobs performed by Oracle E-Business Suite Cloud Manager by adding tasks to meet your own requirements. You can create extended job definitions for jobs including Advanced Provisioning, cloning, promoting standby environments, and refreshing environments.

Oracle E-Business Suite Cloud Manager provides several seeded tasks for commonly required processing, which you can add to an extended job definition 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 job definitions. 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-4.

> **Note:** You must be logged in as a user with Oracle E-Business Suite Cloud Manager administrator privileges to manage tasks and extended job definitions in the Extensibility Framework.
>
> To have Oracle E-Business Suite Cloud Manager administrator privileges, a user must be a member of the Oracle E-Business Suite Cloud Manager administrator group that was specified during configuration of this Oracle E-Business Suite Cloud Manager instance. For more details, see Configure Oracle E-Business Suite Cloud Manager Compute Instance, page 2-37.

- Review and Manage Tasks, page 8-11
- Create a Task, page 8-13
- Review and Manage Extended Job Definitions, page 8-14
- Extend a Job Definition, page 8-16
- Use an Extended Job Definition in Oracle E-Business Suite Cloud Manager Processing, page 8-17

Review and Manage Tasks:

1. To review and manage the tasks available for use in extended job definitions, 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.
   >
   > To have Oracle E-Business Suite Cloud Manager administrator privileges, a user must be a member of the Oracle E-Business Suite Cloud Manager administrator group that was specified during configuration of this Oracle E-Business Suite Cloud Manager

instance. For more details, see Configure Oracle E-Business Suite Cloud Manager Compute Instance, page 2-37.

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 8-13.

5. To edit a custom task, click the **Actions** icon next to that task, and then select **Edit**. See Create a Custom Task, page 8-13.

   > **Note:** You cannot edit seeded tasks.
   >
   > Additionally, you cannot edit a custom task that is part of the running job definition while a provisioning, cloning, or standby promotion job is in progress.

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 job definition. You must first delete all custom extended job definitions 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 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 job 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 Job Definitions:

1. To review and manage extended job definitions, click the **Navigator** icon, select **Administration**, and then select **Extensibility**. Then click the **Extended Job Definitions** tab.

> **Note:** You must be logged in as a user with Oracle E-Business Suite Cloud Manager administrator privileges to manage extended job definitions in the Extensibility Framework.
>
> To have Oracle E-Business Suite Cloud Manager administrator privileges, a user must be a member of the Oracle E-Business Suite Cloud Manager administrator group that was specified during configuration of this Oracle E-Business Suite Cloud Manager instance. For more details, see Configure Oracle E-Business Suite Cloud Manager Compute Instance, page 2-37.

2. The Extended Job Definitions page displays a list of the extended job definitions that have been created 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 extended job definitions whose properties contain that value. You can search by the following properties shown in this page:

   - Extended job definition name

   - The base job definition that this job definition extends, either `EBS Provisioning`, `EBS Clone`, `EBS Promote Standby`, or `EBS Refresh`.

   - The user who created the extended job definition

   - Creation date and time

3. To review additional details for an extended job definition, click the extended job definition name link. In the extended job definition details window, review the list of phases included in the extended job definition and the tasks included in each phase. The extended job definition details window also displays whether each phase and task is seeded or custom.

4. To create a new extended job definition, click **Extend Job Definition**. See Extend a Job Definition, page 8-16.

5. To edit an extended job definition, click the **Actions** icon next to that extended job definition, and then select **Edit**. See Extend a Job Definition, page 8-16.

   > **Note:** You cannot edit an extended job definition that is currently in use by an in-progress job.

6. To delete an extended job definition, click the **Actions** icon next to that extended job definition, and then select **Delete**.

Note: You cannot delete an extended job definition that is currently in use by an in-progress job.

Extend a Job Definition:

The steps for creating a new extended job definition and for editing an existing extended job definition are the same, except that you cannot change the name or template for an existing extended job definition.

1. Click the **Navigator** icon, select **Administration**, and then select **Extensibility**. Click the **Extended Job Definitions** tab. Then click **Extend Job Definition**.

   If you are editing an existing extended job definition, then in the Extended Job Definitions page, click the **Actions** icon next to that extended job definition, and then select **Edit**.

2. Enter the following basic properties:

   - **Name**: Enter a name for the extended job definition. Note that you cannot change the name of an existing extended job definition.

   - **Description**: Enter an optional description for the extended job definition.

   - **Base Job Definition**: Select the base definition for the job you want to extend, either **EBS Provisioning**, **EBS Clone**, **EBS Promote Standby**, or **EBS Refresh**. Note that you cannot change the base job definition for an existing extended job definition.

   Then click **Next**.

3. Specify the details for the extended job definition. The Job Definition Details page initially displays the default phases that are part of the base job definition. You can optionally add a phase to the extended job definition with additional tasks to meet your own requirements.

   - Click the **Actions** icon next to the last phase in the base job definition, and then select **Insert After** to insert an additional phase at the end of the extended job definition.

   - 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 extended job definition 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 extended job definition, click **Next**.

4. In the Review Extended Job Definition page, review the extended job definition's basic properties and the phase and task details. To save the extended job definition, click **Submit**.

Use an Extended Job Definition in Oracle E-Business Suite Cloud Manager Processing:

After an Oracle E-Business Suite Cloud Manager administrator has created an extended job definition for Advanced Provisioning, cloning, promoting a standby environment, or refreshing an environment, Oracle E-Business Suite administrators can select that extended job definition when submitting that type of job. 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 job according to the extended job definition, including any tasks specified in the additional phase. See Advanced Provisioning, page 9-7, Clone an Oracle E-Business Suite Instance, page 12-5, Promote a Standby Environment, page 12-56, and Refresh an Oracle E-Business Suite Environment, page 12-52.

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 Environment, page 12-36.

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 8-18

- Create a Scheduling Policy, page 8-19

- Assign a Scheduling Policy to an Environment, page 8-20

- Delete a Scheduling Policy, page 8-20

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, within the compartment that is selected in the **EBS Compartment** field in the Oracle E-Business Suite Cloud Manager header. 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 8-19.

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 8-19.

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 8-20.
4. To edit a schedule, click the **Actions** icon next to that schedule, and then select **Edit**. See Define a Schedule, page 8-20.
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.

See Schedule Backups, page 12-42 and Review Environment Details, page 11-7.

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 8-18 or Manage Policy Details, page 8-19.

9

Provision an Oracle E-Business Suite Instance

This chapter covers the following topics:

- Requirements for Provisioning a New Environment
- One-Click Provisioning
- Advanced Provisioning
- Provision a New Environment without Public Internet Access (Government Cloud Regions Only)
- 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.

For information on options for new environments, see Section 4.2.1, Provisioning Oracle E-Business Suite 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].

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 9-1 Cloud Services Minimum Resource Recommendations

Description	Machine Type	Number of Machines	OCPUs	Memory	Storage	External IPs
Oracle E-Business Suite Cloud Manager	VM	1	1	7 GB	55 GB (block)	1
A load balancer (You can use your own load balancer or Load Balancer as a Service [LBaaS])	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	1
Application tier	VM	n (where 'n' is the number of application tier nodes in the target environment)	n*m (where 'm' is the number of OCPUs in the shape selected for the application tier; the minimum for 'm' is 1)	Release 12.2 = 14 GB per VM Release 12.1 = 7 GB per VM	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)	n

Description	Machine Type	Number of Machines	OCPUs	Memory	Storage	External IPs
Database tier on Oracle Cloud Infrastructure Compute	VM	1	2	14 GB	Vision demo: 300 GB Fresh install: 200 GB	1
Database tier on Base Database Service 1-Node DB System (Single Instance)	VM	1	2	14 GB	Vision demo: 256 GB Fresh install: 256 GB Total storage: 712 GB [1]	1
Database tier on Base Database Service 2-Node DB System (Oracle RAC)	VM	2	2 per VM	30 GB per VM	Vision demo: 256 GB Fresh install: 256 GB Total storage: 912 GB [1]	2
Database tier on Exadata Database Service Dedicated (Oracle RAC) [2]	See footnote [2]	See footnote [2]	See footnote [2]	See footnote [2]	See footnote [2]	See footnote [2]

Footnotes on Table 9-1:

1. The Available Storage Size and Total Storage Size are different. For more information, see About Oracle Base Database Service [https://docs.oracle.com/en-us/iaas/dbcs/doc/bare-metal-and-virtual-machine-db-systems.html#virtualmachine]

.

2. For a database tier on Exadata Database Service Dedicated, the minimum requirement is an Exadata X10M, X9M, X8M, X7, or X6 base model with a 2-node Oracle RAC.

One-Click Provisioning

One-Click Provisioning streamlines the process of provisioning a new environment by using preset topology options.

In Oracle E-Business Suite Cloud Manager 24.1.1 and later, you have the option to provision your environment using a fresh install image, in addition to the demo install image available in previous versions. Use the demo install image to conduct demonstrations with example data and explore new features. Use the fresh install image to tailor the resulting environment and data to your specific business needs.

The One-Click 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 the application tier and database tier on a single Compute instance using default configuration options. With the demo install image, the Enterprise Command Center Framework tier is included. Your environment has the following characteristics:

- Oracle E-Business Suite Release: 12.2.x
- Oracle Database Release: 19.x
- Enterprise Command Center Framework (for environments provisioned with the demo install image only)
- Operating system: Oracle Linux 8 (Cloud Manager 23.3.1 and later)
- Availability domain: AD-1
- Shape: VM.Standard.E4.Flex
- Storage: Block volume
- Middleware licensing model: "Bring Your Own License (BYOL)"

- Web entry type: Application Tier Node
- Security: Transport Layer Security (TLS) enabled for inbound HTTP traffic

Note the following:

- "Table 5 - New Environment Options for One-Click Provisioning" 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] lists Oracle E-Business Suite, Oracle Database, and Enterprise Command Center release versions available with the latest Cloud Manager release.
- 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.
- In Oracle E-Business Suite Cloud Manager Release 24.1.1 and later, you can create a backup of an environment provisioned using One-Click Provisioning.
- The Oracle Assets Command Center dashboard is pre-configured in your environment. You can configure other dashboards as needed.

To create a more advanced deployment, instead of using One-Click Provisioning you can follow the steps in the section Advanced Provisioning, page 9-7.

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.

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`

- **Database**: **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. See Section 4.2.1, Provisioning Oracle E-Business Suite 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].

For information on options for new environments, see.

3. Enter a new password for the APPS account. This password will also be used for the APPLSYS and APPS_NE accounts.

4. Enter a new EBS_SYSTEM password. This password must contain alphanumeric characters only. For more information on the Oracle E-Business Suite System Schema and the EBS_SYSTEM password, see My Oracle Support Knowledge Document 2755875.1, *Oracle E-Business Suite Release 12.2 System Schema Migration* [https://support.oracle.com/rs?type=doc&id=2755875.1].

5. Enter a new WebLogic Server password. The password must be at least eight characters, and it must contain at least one alphabetic character plus at least one special character from `! " # $ % & ( ) * + , - . / : ; = < > ? @ ][ ^ _ ` { | }` ~ or at least one numeric character.

6. 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.

7. Click **Submit**.

8. You can check the status of the job to provision the environment in the Jobs page.

   After the environment is successfully provisioned, perform any necessary post-provisioning steps listed below.

Post-Provisioning Steps for One-Click Provisioning:

After the One-Click environment is successfully provisioned, you must follow instructions in Perform Post-Provisioning and Post-Cloning Tasks, page 9-27 to enable user access. Specifically, you must follow the instructions in these steps:

1. Manually Configure Firewall When Using Oracle HTTP Server or an On-Premises Load Balancer as the Web Entry Point (Conditionally Required), page 9-41

2. Update Web Entry Host and Domain Name (Conditionally Required), page 9-29

3. In addition, if you chose the Vision Demo Install and plan to use Enterprise Command Centers in this environment, follow these instructions:

   - Configure Enterprise Command Centers after One-Click Provisioning, page 9-47

Advanced Provisioning

With Advanced Provisioning you can configure your own topology for a new environment, instead of using the basic preset topology options in One-Click Provisioning. Environments are created using the following sources:

- Customer backups

  These customer backups are located in private object storage buckets and must be created by Cloud Manager from environments that it manages, or from on-premises environments using Oracle E-Business Suite Cloud Backup Module.

- Pre-seeded backups

  Pre-seeded backups can be used to provision new Vision demo or fresh installation environments. In order to access these, your Virtual Cloud Network (VCN) must be configured for public internet access, as is the case with commercial cloud regions (either with public subnets, or private subnets using a NAT Gateway).

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. The section Perform Post-Provisioning and Post-Cloning Tasks, page 9-27 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 3-44

  You can also create additional network profiles. Refer to Create a Network Profile, page 8-6

- 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 3-26 lists the ports that must be open between subnets for your system to function properly.

- When provisioning a shared application tier file system utilizing the File Storage service (a change introduced in Oracle E-Business Suite Cloud Manager 22.2.1), you must ensure that the APPLLDM variable is set to 'product' so that concurrent manager log files are placed in a corresponding product directory under $APPLCSF. This is necessary to avoid performance issues.

- If you choose **Virtual Machine DB System** (Base Database Service 1-Node or 2-Node DB System) for the Cloud database service, then you can choose the shape that determines the resources allocated to the database system. The following standard shapes are supported:

  - VM.Standard.E4.Flex (AMD) - Available for Oracle Database versions 19c and 12.1.0.2

  - VM.Standard.E3.Flex (AMD) - Available for Oracle Database versions 19c and 12.1.0.2

  - VM.Standard3.Flex (Intel) - Available for Oracle Database versions 19c and 12.1.0.2

  - VM.Standard2.x where x is 1, 2, 4, 8, 16 or 24

  Note: Not all shapes are available in all regions.

- If you choose **Virtual Machine DB System** (Base Database Service 1-Node or 2-Node DB System) or **Exadata Infrastructure** (Exadata Database Service Dedicated) 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.

- In Oracle E-Business Suite Cloud Manager 23.2.1 and later, TDE is done using multiple encryption processes that are run in parallel to reduce the provisioning time.

- 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/en-us/iaas/Content/Tagging/Tasks/managingtagsandtagnamespaces.htm] for more information.

- 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.

- For Oracle E-Business Suite Cloud Manager 23.3.1 and later, Oracle Linux 7 and Oracle Linux 8 are available in the following scenarios:

  - You can choose either Oracle Linux 7 or Oracle Linux 8 when provisioning your application tier, or when provisioning your database tier on Compute.

  - The database tier and the application tier can be on different operating systems.

  - When you provision an environment from a backup, for either tier you can "upgrade" the operating system from Oracle Linux 7 to Oracle Linux 8; note that you cannot downgrade the operating system from Oracle Linux 8 to Oracle Linux 7.

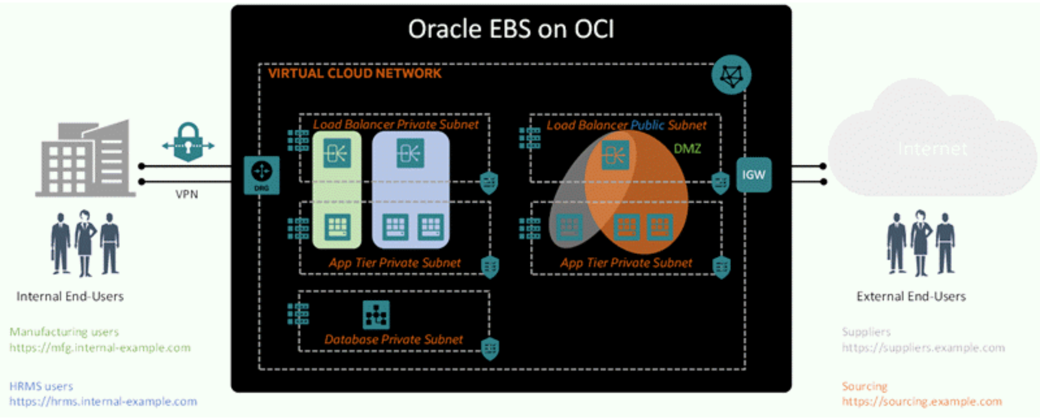
  - When provisioning your database on a Base Database Service, the operating system version is predetermined by the service and tied to the database release update level. For example, when you choose Oracle Database 19c with a patch update level of 19.21 or later, the operating system will be Oracle Linux 8.

  - For Exadata Database Service Dedicated, the operating system version is predetermined by the service upon creation of the Exadata VM Cluster.

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].

In the example in the following illustration, internal zones and external zones are configured. Internal users can access the private zones in the virtual cloud network over VPN through the Dynamic Routing Gateway (DRG). Each of the two internal zones includes a load balancer that directs the traffic to a set of application tier nodes. Likewise, external users can access the external zones using different URLs. This example shows that you can share a single load balancer between multiple zones. This load balancer is in a public subnet, allowing external users' requests to be passed into the DMZ by the Internet Gateway (IGW). The database is deployed in a private subnet in this configuration.

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. If you intend to use the File Storage service, you must use a network profile that has that service enabled. 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 Environments, page 3-9
- Create Network Profiles, page 3-44

❒ 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 Database Service Dedicated:

If you plan to use Oracle E-Business Suite Cloud Manager Advanced Provisioning to provision your database to a pre-existing Exadata Database Service Dedicated 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 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. Sign in to the Oracle Cloud Infrastructure Console.

4. Using the menu, navigate to **Oracle Database**, then **Oracle Exadata Database Service on Dedicated Infrastructure**.

5. Choose the compartment where your infrastructure is located.

6. Under **Oracle Exadata Database Service on Dedicated Infrastructure**, 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 9-12 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 9-12 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 available in the list. The default is your root compartment.

   - **Network Profile**: Select the network profile that contains the network resources you want to use to provision your environment. For example:

`DEFAULT_PROFILE_ADVANCED`.

> **Note:** If you plan to provision an environment which contains a multinode application tier with a shared file system, your network profile must support FSS and therefore you cannot use the default profile.

Click the information icon to view the Network Profile Details. You may wish to capture this information for use later in the interview.

- **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. Enter a new password for the APPS account. This password will also be used for the APPLSYS and APPS_NE accounts.

4. If Oracle E-Business Suite System Schema Migration has been completed on the source environment, then enter a new EBS_SYSTEM password. This password must contain alphanumeric characters only. For more information on the Oracle E-Business Suite System Schema and the EBS_SYSTEM password, see My Oracle Support Knowledge Document 2755875.1, *Oracle E-Business Suite Release 12.2 System Schema Migration* [https://support.oracle.com/rs?type=doc&id=2755875.1].

5. Enter a new WebLogic Server password. The password must be at least eight characters, and contain at least one alphabetic character plus at least one special character from `! " # $ % & ( ) * + , - . / : ; < = > ? @ ][ ^ _ ` { | }` ~ or at least one numeric character.

6. 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 Database Service Dedicated 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.

7. 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.

8. Click **Next**. Now continue to the section Enter Database Information, page 9-16 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`

     Click the information icon to view the Network Profile Details. You may wish to capture this information for use later in the interview.

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.

- **Source Wallet Password**: (Conditionally Required) If you selected a backup created from a TDE-enabled source environment, enter the source wallet password.

- **New EBS_SYSTEM Password**: If Oracle E-Business Suite System Schema Migration has been completed on the source environment, then enter a new EBS_SYSTEM password. This password must contain alphanumeric characters only. For more information on the Oracle E-Business Suite System Schema and the EBS_SYSTEM password, see My Oracle Support Knowledge Document 2755875.1, *Oracle E-Business Suite Release 12.2 System Schema Migration* [https://support.oracle.com/rs?type=doc&id=2755875.1].

- **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.

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** (Base Database Service 1-Node or 2-Node DB System), or **Oracle Exadata Database Service** (Exadata Database Service Dedicated).

2. If you chose Compute for the Cloud database service, enter the following:

   - **DB SID**: Enter the database SID. For example: `demodb`

   - **PDB Name**: If the database version is 19c, enter the pluggable database (PDB) name.

   - **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.

   - **Operating System**: Choose whether to deploy the new environment on Oracle Linux 7 or Oracle Linux 8.

     If the backup was taken on an instance that is on Oracle Linux 8, then in restoring the backup you can choose only Oracle Linux 8.

   - **Shape**: Select a shape. You can choose VM.Standard.E4.Flex or VM.Standard3.Flex shape based on the availability in the OCI region. Ensure that you have checked your quota in advance. When choosing a flexible shape option, use the slider to choose the number of OCPUs. Choose a number between 1 and 64.

     The amount of memory is determined by the number of OCPUs, and is currently set to 16 GB for each OCPU.

- **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 also used for the users SYS, SYSTEM, and EBS_SYSTEM. This password 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)**

     You can choose VM.Standard.E4.Flex or VM.Standard3.Flex based on the availability in the OCI region. With these choices, you can choose the number of OCPUs and the amount of memory. For VM.Standard.E4.Flex, the default number of OCPUs is 4 and the default amount of memory is 64 GB.

   - **Node Count**: Select **1** for a Base Database Service 1-Node DB System (Single

Instance), or select **2** for a Base Database Service 2-Node 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 shape.

4. If you selected **Oracle Exadata Database Service** for the Cloud database service, enter the following:

   - **Exadata VM 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: Overview of X8M and X9M Scalable Exadata Infrastructure [https://docs.oracle.com/en-us/iaas/exadatacloud/exacs/ecs-ovr-x8m-scable-infra.html#exaflexsystem_topic-resource_model].

Once you have selected the VM cluster, its corresponding Exadata infrastructure resource is displayed in the Exadata Infrastructure read-only field below.

> **Note:** This field displays only Exadata VM Clusters with a status of ACTIVE. If an action currently being performed on an Exadata VM Cluster causes the cluster to have the status UPDATING, then that cluster will temporarily be omitted from the list of values in this field. For example, if a user is adding SSH keys to an Exadata VM cluster, then it will have a status of UPDATING for a few minutes. Consequently, if you do not see the cluster you want to use, wait for the action being performed on the cluster to complete and then return to this page to select the cluster.

- **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:

1. Define your zones. For more information on zones, refer to 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].

   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.

You must define your internal (primary) zone first, before optionally defining additional zones.

Enter values for the following properties:

- **Name**
- **Type**

  > **Note:** For the first zone that you define, which is your primary zone, the Type is Internal and is not selectable.

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)**, **Use OCI Load Balancer** to select an existing OCI load balancer, **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 chose New Load Balancer as the web entry type, a new flexible shape load balancer will be created. Select the maximum bandwidth for your new load balancer. For example: **100 Mbps**. The minimum bandwidth will default to 10 Mbps.
   - **OCI Load Balancer**: If you chose OCI Load Balancer for the web entry type, select an existing OCI Load Balancer from the dropdown list.

     > **Note:** If an existing load balancer is used, then load balancer resources, such as "listener", "backend set", "backend", and "certificate," are created anew during provisioning. Preexisting load balancer resources are not used.

   - **Protocol**: Select the protocol for access to the environment, either **http** or **https**.
   - **Hostname**: Enter the host name for your web entry point. The web entry host name must be in lowercase. For example: `myhost`

- **Domain**: Enter the domain for your web entry point. The web entry domain name must be in lowercase. 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 you are prompted for the File Storage Mount Target. If the File Storage Mount Target for the network profile specified earlier matches any of the Mount Targets in the network compartment created on the Oracle Cloud Infrastructure, then that Mount Target appears in the list.

   For a Shared File System Type, you can also specify Mount Options. Default parameters are shown. You can edit these options, but specifying a mount option or parameter that is not supported or recommended for a shared storage file system deployment may result in a provisioning failure. Exercise extreme caution when editing these parameters, as options are not validated in this page.

   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.

   > **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.

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, click **Add Node** to enter properties for your primary application tier node, and then for each additional application tier node in

your environment.

In the **Add Node** dialog window, the following properties appear. Enter the value for each property, except in the case where it has been generated for you.

Note that you can define a specific shape for each application tier node.

- **Logical Hostname**
- **Logical FQDN**
- **Shape**: Select a shape that is available in the OCI region. Ensure that you have checked your quota in advance. When choosing a flexible shape, for example, VM.Standard.E4.Flex, use the sliders to choose the number of OCPUs and the amount of memory (GB).
- **Block Volume Storage**

  > **Note:** If you chose a shared File System Type earlier, the Block Volume Storage value is 0.

- **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.

Click **Add Node** again to save your choices.

6. Click **Save Zone** to save your zone definition.

7. After you have saved the definition for your primary zone, choose a middleware licensing model, either BYOL or UCM. If you choose BYOL, you are indicating that you have purchased or transferred the perpetual licenses required for customized Oracle E-Business Suite Applications. If you choose UCM, you are adopting the Universal Credits subscription-based model, and paying for usage as you go. Make sure you understand the cost associated with this choice.

   Select either Oracle Linux 7 or Oracle Linux 8 for the operating system. Note that if you have multiple application tier nodes, this selection applies to all nodes (all nodes must be on the same operating system). Also, in restoring from a backup, if the backup is taken from an Oracle E-Business Suite instance where all application nodes are on Oracle Linux 8, then Oracle Linux 8 is the only option here.

8. Define additional zones using the **Add Zone** button.

   For the additional internal zones, if **New Load Balancer (LBaaS)** is selected as the Web Entry Type for the first zone, then an extra option **Reuse Internal Zone1 Load Balancer** is displayed in the Web Entry Type list along with the options **New Load Balancer (LBaaS)**, **Use OCI Load Balancer**, and **Manually Configured Load**

Balancer.

9. When you are finished adding application tier nodes, scroll to the top of the window and click **Save Zone** to save your zone definition.

10. When you have completed adding your zones, click **Next**.

Specify Your Extensibility Options:

You can optionally extend the provisioning job to meet your own requirements. By default, Oracle E-Business Suite Cloud Manager follows a standard job definition for provisioning. However, Oracle E-Business Suite Cloud Manager administrators can also create extended job definitions that include additional tasks as part of the provisioning job. In this case you can select the appropriate extended job definition for Oracle E-Business Suite Cloud Manager to follow when provisioning your environment. If you select an extended job definition, 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 job definitions, see Set Up the Extensibility Framework, page 8-10.

Additionally, whether you are using the standard provisioning job definition or an extended job definition, you can choose to have Oracle E-Business Suite Cloud Manager pause at specified points during the provisioning job. 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 job when you are ready to proceed. See Monitor Job Status, page 13-1.

Specify Your Job Definition

1. Optionally select an extended job definition for provisioning your environment in the **Job Definition** field.

2. In the Task Parameters tab, specify any parameter values required for the additional tasks in the job definition. Some parameters may include default values, which you can override as needed.

Specify Your Job Definition Details

3. Click the **Job Definition Details** tab. This tab displays a list of the phases in the job definition 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 Infrastructure** 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 Database Service Dedicated instances, the cluster name is included. If the database service type is Compute, then the operating system is also listed.

   - Application tier details, including

     - Middleware licensing model

     - Operating system

     - Storage information. For the shared file system type, the mount target and mount options are shown.

  - Web entry details
  - Information on zones

- Job definition details.
- SSH Key information.

2. To provision your environment, click **Submit**.

3. You can check the status of the job to provision the environment in the Jobs 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 9-27.

Provision a New Environment without Public Internet Access (Government Cloud Regions Only)

To provision a new environment which uses an advanced topology when your VCN is not configured for public internet access, follow these high-level steps:

1. Provision the environment of your choice (either a Vision Demo or a Fresh Install) using One-Click Provisioning. See One-Click Provisioning, page 9-4.

2. Back up the environment to object storage. See Create a Backup of a Cloud-Based Oracle E-Business Suite Environment, page 12-37.

3. Provision from that backup using Advanced Provisioning. See Advanced Provisioning, page 9-7.

This capability is provided with Oracle E-Business Suite Cloud Manager 24.1.1 and later.

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 cloning job definitions. See Set Up the Extensibility Framework, page 8-10.

- Implement Workaround for Oracle Databases on Exadata Database Service Dedicated (Conditionally Required), page 9-28
- Update Profile Options (Conditionally Required), page 9-28
- Update Web Entry Host and Domain Name (Conditionally Required), page 9-29
- Upload TLS Certificate (Conditionally Required) , page 9-31
- Manually Enable TLS When Using Load Balancer as a Service (LBaaS) as an Alternate Termination Point (Conditionally Required) , page 9-36
- Enable TLS for Manually Configured Load Balancer (Conditionally Required), page 9-39
- Manually Enable TLS When Using Oracle HTTP Server on the Application Tier Node as the Web Entry Point (Conditionally Required), page 9-40
- Manually Configure Firewall When Using Oracle HTTP Server or an On-Premises Load Balancer as the Web Entry Point (Conditionally Required), page 9-41
- Configure Security and Firewall Rules for Secure Access to the Fusion Middleware Control and WebLogic Server Administration Console (Conditionally Required), page 9-42
- Set EBS_SYSTEM Password (Conditionally Required), page 9-43
- Enable and Set Oracle E-Business Account Passwords (Conditionally Required), page 9-44
- Apply Oracle E-Business Suite and Database Patches (Conditionally Required),

page 9-46

- Configure Enterprise Command Centers after One-Click Provisioning (Conditionally Required), page 9-47

- Review Secure Configuration Recommendations for Oracle E-Business Suite (Conditionally Required), page 9-47

Implement Workaround for Oracle Databases on Exadata Database Service Dedicated (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 Database Service Dedicated instance with Oracle Database Release 12.1.0.2.

1. Identify the private IP address of each secondary Exadata Database Service Dedicated node from the Exadata Database Service Dedicated Console.

2. Perform steps 3-8 for all secondary Exadata Database Service Dedicated 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 Database Service Dedicated 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
   ```

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:

     ```
     [http|https]://<web_entry_host>.<web_entry_domain>:
     <listener_port>
     ```

   - `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:

     ```
     [http|https]://<web_entry_host>.<web_entry_domain>:
     <listener_port>/OA_HTML/AppsLogin
     ```

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 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 next task, Upload TLS Certificate, page 9-31.

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)**, **Use OCI Load Balancer**, 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)**, **Use OCI Load Balancer**, 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) or Use OCI Load Balancer

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 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].

  Note: If your environment was created from a backup, and the backup included an existing wallet in the `$ORACLE_HOME/appsutil` directory, then that wallet is preserved in the newly deployed environment. In this case, perform the following steps to import your self-signed certificate manually in the database tier node. These steps replace Section 5.3.2: Database Tier Setup 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], or Section 5.3.2: Database Truststore Configuration 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].

  1. Copy the required zone certificate from `/var/www/files/<env_name>/CACertificate_<env>_<zone>.crt` to the `scripts_dir` directory in the database node.

  2. Source the database environment file.

  3. Navigate to the `$ORACLE_HOME/appsutil/wallet` directory:

     ```
     cd $ORACLE_HOME/appsutil/wallet
     ```

  4. If you know the password for the existing wallet and you want to add your self-signed certificate to that wallet, use the following command to add the certificate:

     ```
      $ORACLE_HOME/bin/orapki wallet add -wallet . -
     trusted_cert -cert
     <CERTIFICATE_FILE_FULL_PATH> -pwd <PASSWORD>
     ```

  5. If you do not want to use the existing wallet, you can create a new wallet and add the certificate to that wallet instead, using the following steps:

     - Take a backup of the existing wallet.

- Create a new wallet using the following command:

  ```
   $ORACLE_HOME/bin/orapki wallet create -wallet .
  -auto_login_only;
  ```

- Add your self-signed certificate to the new wallet using the following command:

  ```
  $ORACLE_HOME/bin/orapki wallet add -wallet . -
  trusted_cert -cert
  <CERTIFICATE_FILE_FULL_PATH> -auto_login_only;
  ```

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 9-40.

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.

   - 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].

   > **Note:** If your environment was created from a backup, and the backup included an existing wallet in the `$ORACLE_HOME/appsutil` directory, then that wallet is preserved in the newly deployed environment. In this case, perform the

following steps to import your self-signed certificate manually in the database tier node. These steps replace Section 5.3.2: Database Tier Setup 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], or Section 5.3.2: Database Truststore Configuration 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].

1. Copy the required zone certificate from `/var/www/files/<env_name>/CACertificate_<env>_<zone>.crt` to the `scripts_dir` directory in the database node.

2. Source the database environment file.

3. Navigate to the `$ORACLE_HOME/appsutil/wallet` directory:

   ```
   cd $ORACLE_HOME/appsutil/wallet
   ```

4. If you know the password for the existing wallet and you want to add your self-signed certificate to that wallet, use the following command to add the certificate:

   ```
    $ORACLE_HOME/bin/orapki wallet add -wallet . -
   trusted_cert -cert
   <CERTIFICATE_FILE_FULL_PATH> -pwd <PASSWORD>
   ```

5. If you do not want to use the existing wallet, you can create a new wallet and add the certificate to that wallet instead, using the following steps:

   - Take a backup of the existing wallet.

   - Create a new wallet using the following command:

     ```
      $ORACLE_HOME/bin/orapki wallet create -wallet .
     -auto_login_only;
     ```

   - Add your self-signed certificate to the new wallet using the following command:

     ```
     $ORACLE_HOME/bin/orapki wallet add -wallet . -
     trusted_cert -cert
     <CERTIFICATE_FILE_FULL_PATH> -auto_login_only;
     ```

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)** or **Use OCI Load Balancer** 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 9-31.

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:

     ```
     https ://<web_entry_host>.<web_entry_domain>
     /OA_HTML/AppsLogin
     ```

   For more information, see *Using Load-Balancers with Oracle E-Business Suite Release 12.2* [https://support.oracle.com/rs?type=doc&id=1375686.1], My Oracle Support

Knowledge Document 1375686.1 or *Using Load-Balancers with Oracle E-Business Suite Release 12.0 and 12.1* [https://support.oracle.com/rs?type=doc&id=380489.1], My Oracle Support Knowledge Document 380489.1.

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*.

6. 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*.

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.

- 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 > End-to-End TLS.

- 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 > End-to-End TLS.

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 9-41.

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.

   - 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 5.1: Apply Required Updates and Patches.

   - 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 5.1: Apply Required Updates and Patches.

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.

   - 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 5.2: Configure Inbound Connections.

- 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 5.2: Configure Inbound Connections.

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 9-41.

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].

   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`

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 11-4.

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:

   ```
   # 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';
   # 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 systemctl restart firewalld
   ```

   Run the following command to verify the current firewall settings:

   ```
   # firewall-cmd --list-all
   ```

Set EBS_SYSTEM Password (Conditionally Required):

The steps in this section are required only for an environment created from a backup if the backup was created prior to the Oracle E-Business Suite Cloud Manager 23.3.1 release, and the following patches were present in the source system used to create the backup:

- R12.AD.C.Delta.13 and R12.TXK.C.Delta.13, or a later version of the AD and TXK release update packs
- The EBS System Schema Migration Completion Patch, Patch 32573930

Among other changes, the R12.AD.C.Delta.13 and R12.TXK.C.Delta.13 release update packs introduce a new schema named EBS_SYSTEM. By default, Oracle Advanced Provisioning sets the password for the EBS_SYSTEM schema to the same value as the password for the SYSTEM schema. After Advanced Provisioning is complete, you should set the password for the EBS_SYSTEM schema to a new value.

To reset the password for the EBS_SYSTEM schema, perform the following steps on the database node.

1. Source the database environment file.
   - For a multitenant 12c or 19c database, use the following commands to source the environment file:

     ```
     $ source <ORACLE_HOME>/<CDB SID>_<hostname>.env
     $ export ORACLE_PDB_SID=<PDB NAME>
     ```

   - For a non-multitenant 11g or 12c database, use the following commands to source the environment file:

     ```
     $ source <CONTEXT_NAME>.env
     ```

2. Run the following commands:

   ```
   $ sqlplus '/ as sysdba'
   SQL>alter user EBS_SYSTEM identified by "<new password>";
   ```

Enable and Set Oracle E-Business Account Passwords (Conditionally Required):

In Oracle E-Business Suite Cloud Manager Release 22.2.1 and later, the One-Click Provisioning and Advanced Provisioning pages prompt you to specify a new APPS user password, and, in the case of Oracle E-Business Suite Release 12.2, a new WebLogic Server password.

The additional 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:

- Oracle E-Business Suite Release 12.2: Default passwords for application user accounts [https://docs.oracle.com/cd/E26401_01/doc.122/e22950/T422699g54568.htm#ig_default_pwds], Standard Installation, *Oracle E-Business Suite Installation Guide: Using Rapid Install Release 12.2 (12.2.0)*

- Oracle E-Business Suite Release 12.1: Change Default Passwords [https://docs.

oracle.com/cd/E18727_01/doc.121/e12842/T422699i4783.htm#T422735], *Oracle E-Business Suite Installation Guide: Using Rapid Install Release 12.1 (12.1.1)*

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 Base Database Service 1-Node or 2-Node DB System or Exadata Database Service Dedicated. 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 Base Database Service 1-Node or 2-Node DB System or Exadata Database Service Dedicated 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 Base Database Service 1-Node or 2-Node DB

System or Exadata Database Service Dedicated 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 11-2.
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 11-2.
   - 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.

Review Secure Configuration Recommendations for Oracle E-Business Suite (Conditionally Required):

When you provision an environment or promote a standby environment, if the environment is at one of the following code levels, then Oracle E-Business Suite Cloud Manager initially places your Oracle E-Business Suite system in lockdown mode to prompt you to review and respond to the secure configuration recommendations.

- Release 12.2.6 or the R12.ATG_PF.C.Delta.6 Release Update Pack or later
- Release 12.1.3

In this case, a system administrator must resolve or acknowledge the recommended security configurations in the Secure Configuration Console to unlock the system for normal usage. To access this console, a user must have a responsibility that includes the Applications System (OAM_APP_SYSTEM) function privilege, such as the seeded System Administration or System Administrator responsibilities, and must be registered as a local user with Oracle E-Business Suite. The administrator must log in to Oracle E-Business Suite using the local login page (`http(s)://[host]:[port]/OA_HTML/AppsLocalLogin.jsp`) to navigate to the console and unlock the system. If a user with local system administrator privileges is not available, you can access the Secure Configuration Console through a command line utility. For more information, see Secure Configuration Console [https://docs.oracle.com/cd/E26401_01/doc.122/e22952/T156458T663583.htm], *Oracle E-Business Suite Security Guide* or Secure Configuration Console, Secure Configuration for Oracle E-Business Suite Release 12.1 [https://support.oracle.com/rs?type=doc&id=403537.1], My Oracle Support Knowledge Document 403537.1.

> **Additional Information:** For more information on connecting to the Oracle E-Business Suite login page, see User Access, page 11-2.

If your environment is at a Release 12.2 code level earlier than Release 12.2.6 or the R12.ATG_PF.C.Delta.6 Release Update Pack, then the system will not be automatically placed into lockdown mode. However, it is highly recommended that you do the following:

1. Review and comply with the secure configuration recommendations in the Secure Configuration Console. See Secure Configuration Console [https://docs.oracle.com/cd/E26401_01/doc.122/e22952/T156458T663583.htm], *Oracle E-Business Suite Security Guide*.

2. Update to the latest ATG_PF Release Update Pack as soon as possible.

10

Discover an Oracle E-Business Suite Instance

This chapter covers the following topics:

- Overview
- Prerequisites
- Review Discovery Requests
- Prepare for Discovery
- Submit a Discovery Request
- Review the Discovery Report
- Resubmit a Discovery Request
- Register a Compliant Environment
- Unregister an Environment
- Rediscover an Updated Environment

Overview

You can use the Discovery feature in Oracle E-Business Suite Cloud Manager to register Oracle E-Business Suite environments that follow our documented standards. The types of environments you can discover include the following:

- Environments manually migrated from on-premises to Oracle Cloud Infrastructure, including those where the source environment was non-Linux.
- Environments initially deployed by Oracle E-Business Suite Cloud Manager, after performing a major modification such as:
  - An Oracle E-Business Suite, Oracle Database, or Oracle Linux upgrade.

- A configuration change, such as the addition of a load balancer or addition or deletion of a node.

  Environments must be unregistered prior to rediscovery; refer to Rediscover an Updated Environment, page 10-9 for complete instructions.

The process for discovering your Oracle E-Business Suite instance is as follows:

1. Ensure all prerequisites are met.

2. Perform steps to prepare for discovering your environment.

3. Submit the Discovery request.

4. Review the resulting report and make any necessary changes to bring the environment into compliance.

5. Register the environment once it passes all compliance checks.

Once your environment is registered, you can use Oracle E-Business Suite Cloud Manager to perform lifecycle management activities, such as backing up or restoring your instance. For a full list of Oracle E-Business Suite Cloud Manager features, see Features, page 1-2.

Note the following Discovery implementation details:

- Environments with a single application tier node will be registered as having a shared file system.

- The zone names for environments with multiple zones will be set to `InternalZone<`*`seqno`*`>` and `ExternalZone<`*`seqno`*`>` upon registration. For example, the zones would be `InternalZone1`, `InternalZone2`, and `ExternalZone3` for an environment with two internal zones and one external zone.

If your environment has any of the following characteristics, you cannot use the Discovery feature at this time:

- The application tier and database tier are on a single virtual machine (VM), such as an instance provisioned by the One-Click Provisioning feature.

- Your Compute instance is deployed on a dedicated virtual machine host.

- Your environment contains bare metal shapes.

For details on performing the discovery process, see the following sections:

- Prerequisites, page 10-3

- Review Discovery Requests, page 10-3

Prerequisites

You must have the following prerequisites in place in order to discover an Oracle E-Business Suite environment in Oracle Cloud Infrastructure:

- 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 candidate Oracle E-Business Suite environment on Oracle Cloud Infrastructure with optional database services that meets the following requirements:
    - The environment must be certified according to the information contained 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].
    - The environment must meet the standards described in My Oracle Support Knowledge Document 2656874.1, *Standards Used by the Oracle E-Business Suite Cloud Manager for Provisioning Oracle E-Business Suite on Oracle Cloud Infrastructure* [https://support.oracle.com/rs?type=doc&id=2656874.1].

Review Discovery Requests

1. To review the discovery requests that have been submitted in Oracle E-Business Suite Cloud Manager, click the **Navigator** icon, select **Administration**, and then select **Discovery**.

2. The Discovery Requests page displays the discovery requests that have been submitted in your Oracle E-Business Suite Cloud Manager instance, within the compartment that is selected in the **EBS Compartment** field in the Oracle E-Business Suite Cloud Manager header. You can optionally enter a full or partial value in the search field to display only requests whose properties contain that

value. You can search by the following properties shown in this page:

- Request name
- Environment name

The page also displays the status of the discovery job and the date and time the request was submitted.

3. To submit a discovery request, first perform the tasks required to prepare your environment for discovery, and then click **Submit Discovery Request**. See Prepare for Discovery, page 10-4 and Submit a Discovery Request, page 10-5.

4. To review the job details for a discovery job, click the job status link for that request. See Review Job Status, page 13-3.

5. To review the Discovery Report for a discovery request, click the **View Discovery Report** icon in the **Compliance** column. See Review the Discovery Report, page 10-7.

6. To register an environment that meets all the standards for discovery, click the **Actions** icon next to that request and then select **Register Environment**. See Register a Compliant Environment, page 10-8.

7. To remove a discovery request for an environment that has not yet been registered, click the **Actions** icon next to that request and then select **Remove Discovery Request**. For example, you can remove a request if you no longer want to register that environment.

   > **Note:** If you submit multiple discovery requests for an environment as you prepare it for discovery, any superseded requests are automatically removed when the environment is successfully registered. However, the final successful discovery request for the environment remains displayed in the Discovery Requests page after the environment is registered, as a record of the environment's history. You cannot remove that request unless you later unregister the environment.

8. To review the environment details for a successfully registered environment, click the environment name link. See Review Environment Details (Standard), page 11-7.

Prepare for Discovery

Perform the following tasks to prepare to discover an environment.

Enable SSH Connectivity:

SSH connectivity must be enabled from the Oracle E-Business Suite Cloud Manager instance to all application tier and database tier nodes. To enable this connectivity, log in to the Oracle E-Business Suite Cloud Manager VM as the `oracle` user and copy the contents of `~/.ssh/id_rsa.pub` into `~/.ssh/authorized_keys` for the `opc` user on all nodes that are part of the environment to be discovered.

Create a Network Profile:

As an Oracle E-Business Suite Cloud Manager administrator, use Oracle E-Business Suite Cloud Manager to create a network profile describing the network on which the candidate Oracle E-Business Suite instance is deployed. This network profile includes key network characteristics such as compartment, region, VCN, availability domain and subnets. For detailed instructions, see Create a Network Profile, page 8-6.

Create a Stage Directory:

Create a directory on the database server to use as the database node stage directory. The stage directory is a temporary storage directory used by the discovery process, and must be writable by the oracle user. For example, `/u01/install/APPS/stage`.

Submit a Discovery Request

You can now submit a discovery request in Oracle E-Business Suite Cloud Manager. The discovery request process identifies the candidate environment to Oracle E-Business Suite Cloud Manager. The Prevalidation phase ensures that prerequisites are met, then the discovery check itself runs and generates a report which will validate whether the environment meets predefined standards.

1. In Oracle E-Business Suite Cloud Manager, click the **Navigator** icon, select **Administration**, and then select **Discovery**.

2. In the Discovery Requests page, click **Submit Discovery Request**.

3. In the Submit Discovery Request window, enter the following details:

   1. **Name** - Enter a unique name for your discovery request. The name must meet the following requirements:

      - The name must contain no more than 50 characters.

      - The first character cannot be a numeral.

      - Special characters and spaces are not allowed.

   2. **EBS Compartment** - Select the Oracle E-Business Suite compartment associated

with the Oracle Cloud Infrastructure resources for the environment.

3. **Network Profile** - Select the network profile that contains the network resources for the environment.

4. **DB Node IP Address** - Enter the private IP address of the database node for the environment being discovered.

   Note: For an Oracle RAC database, you can enter the private IP address of any of the database nodes in this field.

5. **DB Context File** - Enter the full path for the database context file.

   Note: For an Oracle RAC database, enter the context file corresponding to the database node IP specified in **DB Node IP Address**.

6. **DB Node Stage Directory** - Provide the stage directory location previously created to store metadata gathered during the discovery job.

   Note: For an Oracle RAC database, the stage directory should be located on the database node IP specified in **DB Node IP Address**.

7. **Environment Name** - Enter the environment name.

8. **APPS Password** - Enter the APPS user password for the Oracle E-Business Suite source environment.

9. Optionally, if the candidate Oracle E-Business Suite environment for discovery is already configured with an Oracle Cloud Infrastructure load balancer, click the **Discover OCI Load Balancers** toggle switch. Then, click **Add** to specify the details of the load balancer and listener. An environment can have multiple load balancers and zones associated with it.

   If the candidate Oracle E-Business Suite Environment has an Oracle Cloud Infrastructure load balancer associated with it but you do not specify the load balancer details when you submit the discovery request, or if the specified load balancer and listener mappings do not match the environment's configuration, then the web entry point identified by the discovery process is registered with a default web entry type as follows:

   - If the environment includes only one application tier node, then its web entry type is set to `Application Tier Node`.

- If the environment includes multiple application tier nodes, then its web entry type is set to `Manually Configured Load Balancer`.

  You can unregister the environment and submit a new discovery request to supply the corrected load balancer information.

4. Click **Submit** when you are ready to submit the request. Ensure that the **EBS Compartment** field in the Oracle E-Business Suite Cloud Manager header is set to the compartment associated with the request. Oracle E-Business Suite Cloud Manager then displays the request in the Discovery Requests page.

In the Discovery Requests page, your newly submitted request with an automatically populated environment name appears. The request then goes through the Prevalidation phase, which ensures that Oracle E-Business Suite Cloud Manager can locate the environment and prerequisites are met. Refresh the page to view an updated job status.

You can click the status link to view the Job Details page. The Job Details page provides an option to auto-refresh every 20 seconds as the various compliance checks are performed and completed. Click the **Auto Refresh** toggle switch to enable and disable this feature. See Review Job Status, page 13-3.

Once Prevalidation succeeds, the request status will change to `Waiting for User to Register Environment`. At this point, you can review the Discovery Report and ensure that all artifacts identified by this process are consistent with your environment.

Review the Discovery Report

To review the Discovery Report, navigate to the Discovery Requests page. Click the **View Discovery Report** icon in the Compliance column associated with your environment.

In the report, each row corresponds to a standard listed in My Oracle Support Knowledge Document 2656874.1, *Standards Used by the Oracle E-Business Suite Cloud Manager for Provisioning Oracle E-Business Suite on Oracle Cloud Infrastructure* [https://support.oracle.com/rs?type=doc&id=2656874.1]. Each row containing a standard includes the following information:

- Expected Result
- Actual Result
- Status - Either a green check mark to indicate compliance or a red 'X' to indicate non-compliance.
- Explanation - For cases of non-compliance, a description of the standard that the environment must meet.

Resubmit a Discovery Request

If the Discovery Report indicates that your environment does not meet the standards for discovery, you can make the necessary changes and resubmit the discovery request. To do so, click **Submit Discovery Request** in the Discovery Requests page. See Submit a Discovery Request, page 10-5.

After you submit another request for the same environment, your initial request appears in the Discovery Requests page with a status of `Superseded by discover request <`*`environment name`*`>`.

Register a Compliant Environment

If the Discovery Report indicates that your environment meets the standards for discovery, you can proceed to register your environment. An environment that is compliant and ready to be registered appears with the status `Waiting for User to Register Environment`.

Click the **Actions** icon and select **Register Environment**. In the Register Environment window, enter the APPS user password and click **Register**.

The message `Successfully submitted registration request` appears on the Discovery Requests page. The status then changes to `Discovery Input Validation in Progress`.

After the registration completes, the status of the request changes to `Discovery Successful`.

Unregister an Environment

Prior to making a major change to your environment, you must unregister it. After the change is complete, you can rediscover the environment in order to record the updates within Oracle E-Business Suite Cloud Manager.

When you unregister an environment, the metadata for the environment is removed from Oracle E-Business Suite Cloud Manager. This process does not delete the environment itself.

> **Note:** Single VM instances, such as instances provisioned by the One-Click Provisioning feature, cannot be registered or unregistered.

To Unregister an Environment:

1. Click the **Navigator** icon and select **Environments**.

2. Navigate to the Environment Details page for the environment that you want to

unregister by clicking the environment name link.

3. Click **Unregister**.

4. The Confirm Unregister window appears. Enter the environment name to confirm your choice. Then click **Yes**.

> **Note:** After you complete the unregister action, you can no longer view or manage the environment in Oracle E-Business Suite Cloud Manager. If you would like to continue using Cloud Manager, review Rediscover an Updated Environment, page 10-9 for guidance prior to making your desired change.

Rediscover an Updated Environment

If your environment is managed by the Oracle E-Business Suite Cloud Manager, you must unregister the environment prior to making a major change, then rediscover it after the change is complete in order to record the updates within Oracle E-Business Suite Cloud Manager. Here are common scenarios where this applies:

- When performing an Oracle E-Business Suite, Oracle Database, or Oracle Linux upgrade.

- When changing the environment configuration. Examples include adding a load balancer, increasing the size of the block volume attached to an application or database tier node, or adding or deleting a node.

Complete the following steps to update your environment:

1. Unregister your environment (see Unregister an Environment, page 10-8).

2. Perform the update.

3. Submit a new discovery request (see Submit a Discovery Request, page 10-5).

4. Register the updated environment (see Register a Compliant Environment, page 10-8).

Important Notes:

- Check the Oracle E-Business Suite Cloud Manager registration settings.

  Before you proceed with rediscovering an updated environment, ensure that the Resource Owner option is selected under the 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 2-41.

- Configure the load balancer (conditional).

  If you plan to upgrade 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 and prior to submitting the discovery request. 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 Infrastructure* [https://support.oracle.com/rs?type=doc&id=2517025.1].

  If you plan to perform 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.

- Make note of the database node IP address and context file location (conditional).

  If you plan to perform an in-place Oracle E-Business Suite or Oracle Database upgrade where your application tier or database tier will not change, make note of the database node IP address and context file location prior to proceeding with the unregister process. You will use these settings when you submit a new discovery request prior to registering your updated environment.

11

Oracle E-Business Suite System Administration

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

This chapter describes system administration features for Oracle E-Business Suite environments deployed on Oracle Cloud Infrastructure. For more information on general Oracle E-Business Suite system administration, see *Oracle E-Business Suite Setup Guide* [https://docs.oracle.com/cd/E26401_01/doc.122/e22953/toc.htm], *Oracle E-Business Suite Security Guide* [https://docs.oracle.com/cd/E26401_01/doc.122/e22952/toc.htm], and *Oracle E-Business Suite Maintenance Guide* [https://docs.oracle.com/cd/E26401_01/doc.122/e22954/toc.htm].

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 through One-Click Provisioning, the protocol is `https` and the port is `4443`. For environments created through Advanced Provisioning, the protocol and the port depend on the options selected in the Topology page.

Conditional Action: Additionally, if your environment was created through Advanced Provisioning or One-Click Provisioning or by promoting a standby environment, and the environment is at one of the following code levels, then Oracle E-Business Suite Cloud Manager initially places your Oracle E-Business Suite system in lockdown mode to prompt you to review and respond to the secure configuration recommendations.

- Release 12.2.6 or the R12.ATG_PF.C.Delta.6 Release Update Pack or later

- Release 12.1.3

  In this case, a system administrator must resolve or acknowledge the recommended security configurations in the Secure Configuration Console to unlock the system for normal usage. See Review Secure Configuration Recommendations for Oracle E-Business Suite (Conditionally Required), page 9-47.

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 2-32. 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 Base Database Service 1-Node or 2-Node DB System or Exadata Database Service Dedicated, 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 Base Database Service 1-Node or 2-Node DB System or Exadata Database Service Dedicated.

- 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 9-27.

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 -L localhost:<WLS_admin_port>:
<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** panel. 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.
- Any snapshots created from the environment.
- Jobs related to the environment.

You can rediscover an environment to refresh its metadata in Oracle E-Business Suite Cloud Manager after an upgrade, including database upgrades from Oracle Database 12.1.0.2 or 11.2.0.4 to Oracle Database 19c, or Oracle E-Business Suite upgrades from Release 12.1 to Release 12.2. After the environment has been rediscovered, you can resume managing the environment through the Oracle E-Business Suite Cloud Manager UI. See Rediscover an Updated Environment, page 10-9.

For reviewing standby environments, refer to the section Review Standby Environment, page 11-13.

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 9-4, Advanced Provisioning, page 9-7, or Clone an Oracle E-Business Suite Environment, page 12-5.

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. You can use buttons provided in the Environment details page to clone (if applicable), create a snapshot (if applicable), back up, refresh, unregister, or delete an environment.

   For more information on these capabilities, see:

   - Clone an Oracle E-Business Suite Environment, page 12-5
   - Back Up an Oracle E-Business Suite Environment, page 12-36
   - Refresh an Oracle E-Business Suite Environment, page 12-52
   - Unregister an Environment, page 10-8
   - Delete an Oracle E-Business Suite Environment, page 12-62

Review General Information:

1. The General Information region on the Overview page displays the following details:

   - Oracle E-Business Suite version
   - Number of application tier nodes
   - Number or database tier nodes
   - Oracle E-Business Suite Compartment, with the associated network profile name.
   - Version of the Oracle E-Business Suite Cloud automation tools with which the environment was provisioned
   - Last job, with a Status link for details

     For more information, see: Monitor Job Status, page 13-1
   - Creation date and time
   - If applicable, the backup from which this environment was refreshed, with the backup type
   - If applicable, the refresh 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. 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`.

4. 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 12-42.

   See Set Up Scheduling Policies, page 8-17 for more information on scheduling policies for backups.

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
- Middleware Licensing model
- Storage Type
- File System Type
- Operating System

For a shared file system type, the following details are shown:

- File System Name
- File System OCID
- File Storage Mount Target
- Storage Type

2. For each zone defined for the application tier, the following details are shown:
   - Zone type
   - Web entry IP
   - Web entry type

     If **New Load Balancer (LBaaS)**, **Use OCI Load Balancer**, or **Reuse InternalZone1 Load Balancer** (for a secondary zone) was chosen when the Oracle E-Business Suite instance was provisioned, then the corresponding web entry type is shown as **Load Balancer as a service**.
   - 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 12-1.

Review Database Tier Information

1. The Database Tier region displays the following:
   - Cloud Service Type
   - Creation Date and Time
   - Database Name
   - SQL*Net Port
   - Database Version
   - Pluggable database (PDB) Name
   - Oracle Home
   - Operating System
   - Shape
   - VM Cluster Name (for Exadata Database Service Dedicated only)
   - Database patch level
   - Update date for the database patch level
   - Database edition
   - Cluster name
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. See Review Backups, page 12-46.

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 9-7 for more information.

2. To refresh this environment from one of its backups, click **Action** for that backup and select **Refresh**. See Refresh an Oracle E-Business Suite Environment, page 12-52.

3. You can also select **Delete** from the **Action** menu for a backup to delete it.

   See Delete a Backup, page 12-49 for more information.

Review Snapshots:

If applicable, the Snapshots tab lists snapshots created from this environment.

1. For each snapshot, the following is shown:
   - Name
   - Last Job
   - Creation date and time

2. You can click on a snapshot name to navigate to the Snapshot Details page. From the Snapshot Details page, you can create a clone of that snapshot. See Review Snapshot Details, page 12-27 for more information.

Review Jobs:

The Jobs tab lists jobs associated with the environment.

1. You can use the **Search** box to search for a specific job.

2. For each job, the following fields are shown:

   - Job
   - Status
   - Action
   - Submitted by
   - Started
   - Finished

3. Click on a job name to navigate to the Job Details page.

   See: Monitor Job Status, page 13-1 for more information.

Review Standby Environment Details

You can review details of a standby environment you created in Oracle Applications Manager.

After a standby environment is created, the Last Job field has the value "setup-standby (Successful)" with a link to the job details. See Review Job Status, page 13-3 for more information.

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.
- Jobs 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 6-12.

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
   - Last job, with a Status link for details

     For more information, see: Monitor Job Status, page 13-1
   - 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 12-1.

1. The Application Tier region lists the Oracle E-Business Suite base directory with the following details:

   - File System OCID
   - Middleware Licensing Model
   - Operating System

   If the File System Type is Shared, the following information is given:

   - File Storage Mount Target
   - File System Name
   - Storage Type

   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 Jobs:

The Jobs tab lists jobs associated with the standby environment.

If a job has been restarted from a parent job, a link is provided for details for the parent.

1. You can use the **Search** box to search for a specific job.
2. For each job, the following fields are shown:
   - Job

- Status
- Action
- Submitted by
- Started
- Finished

3. Click on a job name to navigate to the Job Details page.

   See: Monitor Job Status, page 13-1 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

What's Next

Use the **Promote** button to promote the standby environment. See: Promote a Standby Environment, page 12-56 for more information.

You can also delete a standby environment using the **Delete** button. See: Delete a Standby Environment, page 12-63 for more information.

12

Oracle E-Business Suite Lifecycle Management

This chapter covers the following topics:

- Add and Delete Nodes
- Clone an Oracle E-Business Suite Environment
- Clone an Oracle E-Business Suite Environment with the Database on Oracle Cloud Infrastructure Compute
- Clone an Oracle E-Business Suite Environment with the Database on a Base Database Service DB System
- Clone an Oracle E-Business Suite Environment with the Database on Exadata Database Service Dedicated
- Back Up an Oracle E-Business Suite Environment
- Refresh an Oracle E-Business Suite Environment
- Promote a Standby Environment (Commercial Cloud Regions Only)
- 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 environment 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 9-7 or Clone an Oracle E-Business Suite Environment, page 12-5.

❒ 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
  - Validates that the WLS domain configuration lock is enabled
- 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 backend set to accommodate the new application tier node.

Note that if **Manually 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.

   - Block Volume Storage

   - Fault Domain

   - Logical Hostname

   - Middleware Licensing Model

   - 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 backend 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
$ 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
```

Clone an Oracle E-Business Suite Environment

Oracle E-Business Suite Cloud Manager includes cloning capabilities that utilize cloud-native cloning features.

Refer to the following sections:

1. Clone an Oracle E-Business Suite Environment with the Database on Oracle Cloud Infrastructure Compute, page 12-8

2. Clone an Oracle E-Business Suite Environment with the Database on a Base Database Service DB System, page 12-15

3. Clone an Oracle E-Business Suite Environment with the Database on Exadata Database Service Dedicated, page 12-23

Overall Prerequisites

The following requirements apply for all Oracle E-Business Suite Cloud Manager cloning operations.

- You must have a source Oracle E-Business Suite environment on Oracle Cloud Infrastructure deployed through Oracle E-Business Suite Cloud Manager, such as through a lift and shift, provisioning, or discovery process.

- You must have access to the network profile used by the source environment and to the network profile that you will specify for the target 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 environment defines network profiles and assigns you the profiles that you can use to provision Oracle E-Business Suite environments. For more information, see:

  - Create Network Resources For Deploying Oracle E-Business Suite Environments, page 3-9
  - Create Network Profiles, page 3-44

- If you choose to use tags, you can create defined tags before you begin cloning. Any tag namespace that you select for the clone must be defined for the compartment in which you are cloning, as specified in the network profile. For more information, see: Managing Tags and Tag Namespaces [https://docs.cloud.oracle.com/en-us/iaas/Content/Tagging/Tasks/managingtagsandtagnamespaces.htm].

File Storage service (FSS) Prerequisites

- A network profile for the cloned environment must be defined. The network profile must have a File Storage mount target subnet defined.
- The user performing the cloning task must be part of a group which has permissions to create a File Storage File system on the EBS compartment defined in the network profile. These permissions are allocated by the policies below:
  - Allow group `ebscm-proddba-grp` to manage file-systems in compartment `ebsprod-compartment`
  - Allow group `ebscm-proddba-grp` to manage export-sets in compartment `ebsprod-compartment`

Overall Attributes

- You can specify a different network profile for the target (cloned) environment from the source environment. Within this profile, you can specify a different compartment and a different network if you choose. If the network profile for the source environment contains both internal and external zones, then the network profile for the target must also contain both types of zones.
- If the network profile of the source environment is FSS-enabled, then the network profile of the target environment must be FSS-enabled.
- You can deploy the load balancer for the clone as either a public or private Load Balancer as a Service (LBaaS), depending on the load balancer type defined in the network profile.
- The clone resides in the same availability domain as the source environment.

- The application tier topology 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.
- If the source environment is configured with a shared file system, cloning is performed as follows:
  - If the environment was provisioned with Oracle E-Business Suite Cloud Manager Release 22.2.1 or later, the File Storage service volume mounted from the application tier nodes is cloned, and then mounted to the application tier nodes of the target system.

    For more information on File Storage service cloning, see Cloning File Systems [https://docs.oracle.com/en-us/iaas/Content/File/Tasks/cloningFS.htm].

    Note that Oracle E-Business Suite Cloud Manager supports the deletion of a source environment even if it is associated with the root file system. The root file system will be preserved, however, as long as a descendant clone exists. See Cloning File Systems [https://docs.oracle.com/en-us/iaas/Content/File/Tasks/cloningFS.htm] for more information.
  - If the environment was provisioned with a release prior to Oracle E-Business Suite Cloud Manager Release 22.2.1, the block volume attached to the primary application tier node is cloned, and then attached to the primary application tier node of the target system.
- If the source environment is configured with a non-shared file system, all block volumes attached to application tier nodes are cloned and subsequently attached to the target application tier nodes.
- If you have added additional (custom) block volumes to your application tier nodes, the cloning process will clone these as well.
- You can optionally change the shape of the application tiers for the clone.
- The Cloud Manager automation configures the application tier services to use port pools 0 and 1. These port pool values cannot be changed. Ensure that the necessary ports are open between subnets in order for your system to function properly, as listed in Create Security Rules, page 3-26.
- 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 predefined tag or specifying a new (free-form) tag. You can use a tag to identify all resources associated with an environment or a 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.

- The clone uses the same fault domain as the source environment.

Clone an Oracle E-Business Suite Environment with the Database on Oracle Cloud Infrastructure Compute

This cloud-native cloning feature, applicable for Oracle E-Business Suite environments in which the database runs on Oracle Cloud Infrastructure Compute, has the following key attributes:

- You can run the cloning procedure on Compute either when the Oracle E-Business Suite services (application tier and database tier) are running, or when they are shut down.

- When cloning on Compute, you can assign the clone a different database tier shape than the source environment.

- 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.

- On Compute, the clone inherits the middleware technology licensing model of the source environment, either Bring Your Own License (BYOL) or Universal Credit Management (UCM).

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 **Clone** button.

Enter Environment Details:

On this page the details for the source environment are shown:

- Environment name

- EBS Compartment

- Network Profile

- Availability Domain

- File System Type

1. Enter values for the clone details:
   - **Environment Name**: Enter a name for your environment. For example: `usdev3`
   - **EBS Compartment**: The compartment for the cloned environment. You can select an EBS compartment that is different than that for the source environment.
   - **Network Profile**: Select a network profile for the cloned environment. The list of available network profiles is dependent on the EBS compartment that you selected above. From this list of network profiles, select a network profile that includes the same Availability Domain as that of the source.

     Note that if you are cloning a File Storage service-enabled environment, you can choose a different network profile than that of the source environment, but it also must have File Storage service enabled.

     > **Note:** The source environment and the cloned environment can also have different mount targets.

   - **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 Database Tier Information for Oracle Cloud Infrastructure Compute (Compute VM):

If your cloned environment is on Oracle Cloud Infrastructure Compute (Compute VM), then follow these steps to enter the database tier information as required.

1. Enter a Database Name.

2. Enter the admin password for the database of your cloned environment. This password is used for the SYS user as well and it 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.

3. Enter a new APPS password for your cloned environment. The password must contain only alphanumeric characters.

4. If Oracle E-Business Suite System Schema Migration has been completed on the source environment, then enter a new EBS_SYSTEM password. This password must contain alphanumeric characters only. For more information on the Oracle E-Business Suite System Schema and the EBS_SYSTEM password, see My Oracle Support Knowledge Document 2755875.1, *Oracle E-Business Suite Release 12.2 System Schema Migration* [https://support.oracle.com/rs?type=doc&id=2755875.1].

5. For a Release 12.2 environment, enter a new WebLogic Server password for your cloned environment.

6. The following information is provided as read-only:

   - Database Service Type

   - Logical FQDN

7. You can optionally update the following:

   - VM Shape

   - Number of OCPUs

   - Amount of memory (GB)

8. 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)**, **Use OCI Load Balancer** to select an existing OCI load balancer, **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.

5. If you chose New Load Balancer as the web entry type, a new flexible shape load balancer will be created. Select the maximum bandwidth for your new load balancer. For example: **100 Mbps**. The minimum bandwidth will default to 10 Mbps.

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 host name. The web entry host name must be in lowercase. For example: `myhost`

   - **Domain**: Enter a domain name. The web entry domain name must be in lowercase. 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.

   If your source environment is using File Storage service, then you are prompted for the File Storage Mount Target. If the File Storage Mount Target for the network profile specified earlier matches any of the Mount Targets in the network compartment created on the Oracle Cloud Infrastructure, then that Mount Target appears in the list.

   For a Shared File System Type, you can also specify Mount Options. Default parameters are shown. You can edit these options, but specifying a mount option or parameter that is not supported or recommended for a shared storage file system deployment may result in a provisioning failure. Exercise extreme caution when editing these parameters, as options are not validated in this page.

8. Review the properties for each node in the Application Tier Nodes information.

- **Logical FQDN**
- **Shape**: You can change the shape of the node. When choosing a flexible shape, for example, VM.Standard.E3.Flex, use the sliders to choose the number of OCPUs and the amount of memory (GB).
- **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 job to meet your own requirements. By default, Oracle E-Business Suite Cloud Manager follows a standard job definition for cloning. However, Oracle E-Business Suite Cloud Manager administrators can also create extended job definitions that include additional tasks as part of the cloning job. In this case you can select the appropriate extended job definition for Oracle E-Business Suite Cloud Manager to follow when cloning your source environment. If you select an extended job definition, you may need to enter values for input parameters required by the additional tasks in that job definition.

> **Additional Information:** For more information on using the Extensibility Framework to extend job definitions, see Set Up the Extensibility Framework, page 8-10.

Additionally, whether you are using the standard cloning job definition or an extended job definition, you can choose to have Oracle E-Business Suite Cloud Manager pause at specified points during the cloning job. 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 job when you are ready to proceed. See Monitor Job Status, page 13-1.

Specify Your Job Definition

1. Optionally select an extended job definition for cloning your environment in the **Job Definition** field.

2. In the Task Parameters tab, specify any parameter values required for the additional tasks in the job definition. Some parameters may include default values, which you can override as needed.

Specify Your Job Definition Details

3. Click the **Job Definition Details** tab. This tab displays a list of the phases in the job definition 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:

Review the details for the cloned environment on this page.

1. Review the following:
   - Clone Details:
     - Environment Name
     - Installation Type
     - EBS Version
     - DB Version

        - Network Profile

    - Database Details:
        - Database Service Type
        - Shape
        - Enable TDE
        - Database Name
        - PDB Name
        - Node Count
        - DB Software Edition
        - License Type

    - Application Tier Details:
        - Middleware Licensing Model
        - Start Application Services (Yes/No)
        - Zone information, including
            - Web entry details
            - Storage information. For a shared file system, the File Storage service mount target and mount options are shown
            - Information on nodes

    - Details for Custom Tasks or Paused Tasks, if any

    - SSH Keys information, if any

2. To create the cloned environment, click **Submit**.

3. You can check the status of the job to clone the source environment in the Jobs page.

Perform Post-Cloning Tasks:

After the environment is successfully cloned, perform any necessary post-cloning steps and access the cloned environment following the instructions provided in Perform Post-Provisioning and Post-Cloning Tasks, page 9-27.

Clone an Oracle E-Business Suite Environment with the Database on a Base Database Service DB System

Cloning is available for Oracle E-Business Suite environments that use a Base Database Service 1-Node or 2-Node DB System (VM DB System) as the cloud service for the database tier, with the following attributes:

- When cloning a Base Database Service DB System, you cannot change the database tier shape.
- When cloning a Base Database Service DB System, you can specify whether the clone should use an included license for the middleware technology or use Bring Your Own License (BYOL).

Base Database Service DB System Cloning Prerequisites:

The following requirements apply to the source environment when cloning with Oracle E-Business Suite Cloud Manager on a Base Database Service DB System:

- Base Database Service DB System cloning is available for environments with Oracle Database 12c Release 1 and Oracle Database 19c only.
- For Oracle Database 19c-based clones, the Oracle Grid Infrastructure software on the source environment must be 19.9 or later.
- The PDB datafile directory structure must comply with OMF standards. That is, the files must be in the following directory structure: `+DATA/`*`<DB_UNIQUE_NAME>/ <PDB_GUID>`*`/DATAFILE`

  If your files are not currently in this directory structure, then you must move the files before beginning the cloning procedure. For example, you can use the following steps to perform an online move.

  As SYSDBA, run the following commands:

  ```
  alter session set container="<PDB>";
  set line 140
  set pagesize 2000
  set heading off
  spool dbfmove.sql
  select 'ALTER DATABASE MOVE DATAFILE ' || FILE_ID ||';' from
  dba_data_files;
  spool off
  vi @dbfmove.sql (Remove unwanted lines)
  SQL> @dbfmove.sql
  ```

  Add new temp file(s) to the existing TEMP tablespace; for example:

  ```
  ALTER TABLESPACE <TEMP tablespace_name> ADD TEMPFILE SIZE <size>M;
  ```

  By default, these will be created in the OMF location `+DATA/<CDB_DB_UNIQUE_NAME>/<PDB GUID>/TEMPFILE/`.

Then run the DROP TEMPFILE commands to remove the temp files in the older location, for example:

```
ALTER TABLESPACE <TEMP tablespace_name> DROP TEMPFILE <file id>;
```

- The source Base Database Service DB System nodes must be running when you perform the cloning procedure, and the database must also be running.

- The value of db_recovery_file_dest_size must be greater than db_recovery_file_dest_size + sum(online_redo_log_size of thread#1). To be precise, the required size for db_Recovery_file_Dest_size is:

```
(select 'RECOVERYFILEDEST='||(floor(space_limit/1024/1024)) from
v\$recovery_file_dest)
+
(select 'REDOLOGSIZE='||sum(bytes/1024/1024) from v\$log where
thread#=1)
```

- The initialization parameter pre_page_sga must be set to FALSE. To set this parameter value, run the following command:

```
SQL> alter system set pre_page_sga=FALSE scope=spfile;
```

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 **Clone** button.

Enter Environment Details:

On this page the details for the source environment are shown:

- Environment name

- EBS Compartment

- Network Profile

- Availability Domain

- File System Type

1. Enter values for the clone details:

   - **Environment Name**: Enter a name for your environment. For example: usdev3

   - **EBS Compartment**: The compartment for the cloned environment. You can select an EBS compartment that is different than that for the source environment.

- **Network Profile**: Select a network profile for the cloned environment. The list of available network profiles is dependent on the EBS compartment that you selected above. From this list of network profiles, select a network profile that includes the same Availability Domain as that of the source.

  Note that if you are cloning a File Storage service-enabled environment, you can choose a different network profile than that of the source environment, but it also must have File Storage service enabled.

  > **Note:** The source environment and the cloned environment can also have different mount targets.

- **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 Database Tier Information for Base Database Service 1-Node or 2-Node DB System (VM DB System):

If your cloned environment is on Base Database Service 1-Node or 2-Node DB System (VM DB System) then follow these steps to enter the database tier information as required.

1. Enter a Database Name.

2. Enter a PDB Name.

3. If you are cloning an environment that uses Base Database Service 1-Node or 2-Node DB System as the cloud service for the database tier, then the following information is provided as read-only.

- Database Service Type
- DB Patch Level
- Shape

  Note: If you are cloning an environment that has a flexible shape, then this shape is also read-only.

- Node Count
- DB Software Edition
- Cluster Name

4. Select a license type.

   For a Base Database Service DB System, you can 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.

5. Enter the admin password for the database of your cloned environment. 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.

6. Enter a new APPS password for your cloned environment. The password must contain only alphanumeric characters.

7. If Oracle E-Business Suite System Schema Migration has been completed on the source environment, then enter a new EBS_SYSTEM password. This password must contain alphanumeric characters only. For more information on the Oracle E-Business Suite System Schema and the EBS_SYSTEM password, see My Oracle Support Knowledge Document 2755875.1, *Oracle E-Business Suite Release 12.2 System Schema Migration* [https://support.oracle.com/rs?type=doc&id=2755875.1].

8. For a Release 12.2 environment, enter a new WebLogic Server password for your cloned environment.

9. 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)**, **Use OCI Load Balancer** to select an existing OCI load balancer, **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.

5. If you chose New Load Balancer as the web entry type, a new flexible shape load balancer will be created. Select the maximum bandwidth for your new load balancer. For example: **100 Mbps**. The minimum bandwidth will default to 10 Mbps.

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 host name. The web entry host name must be in lowercase. For example: `myhost`

   - **Domain**: Enter a domain name. The web entry domain name must be in lowercase. 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.

   If your source environment is using File Storage service, then you are prompted for the File Storage Mount Target. If the File Storage Mount Target for the network profile specified earlier matches any of the Mount Targets in the network compartment created on the Oracle Cloud Infrastructure, then that Mount Target appears in the list.

   For a Shared File System Type, you can also specify Mount Options. Default parameters are shown. You can edit these options, but specifying a mount option or parameter that is not supported or recommended for a shared storage file system deployment may result in a provisioning failure. Exercise extreme caution when editing these parameters, as options are not validated in this page.

8. Review the properties for each node in the Application Tier Nodes information.

   - **Logical FQDN**
   - **Shape**: You can change the shape of the node. When choosing a flexible shape, for example, VM.Standard.E3.Flex, use the sliders to choose the number of OCPUs and the amount of memory (GB).
   - **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 job to meet your own requirements. By default, Oracle E-Business Suite Cloud Manager follows a standard job definition for cloning. However, Oracle E-Business Suite Cloud Manager administrators can also create extended job definitions that include additional tasks as part of the cloning job. In this case you can select the appropriate extended job definition for Oracle E-Business Suite Cloud Manager to follow when cloning your source environment. If you select an extended job definition, you may need to enter values for input parameters required by the additional tasks in that job definition.

> **Additional Information:** For more information on using the Extensibility Framework to extend job definitions, see Set Up the Extensibility Framework, page 8-10.

Additionally, whether you are using the standard cloning job definition or an extended job definition, you can choose to have Oracle E-Business Suite Cloud Manager pause at specified points during the cloning job. 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 job when you are ready to proceed. See Monitor Job Status, page 13-1.

Specify Your Job Definition

1. Optionally select an extended job definition for cloning your environment in the

Job Definition field.

2. In the Task Parameters tab, specify any parameter values required for the additional tasks in the job definition. Some parameters may include default values, which you can override as needed.

Specify Your Job Definition Details

3. Click the **Job Definition Details** tab. This tab displays a list of the phases in the job definition 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:

Review the details for the cloned environment on this page.

1. Review the following:

   - Clone Details:

     - Environment Name

    - Installation Type
    - EBS Version
    - DB Version
    - Network Profile
  - Database Details:
    - Database Service Type
    - Shape
    - Database Name
    - PDB Name
    - Node Count
    - DB Software Edition
    - License Type
  - Application Tier Details:
    - Middleware Licensing Model
    - Start Application Services (Yes/No)
    - Zone information, including
      - Web entry details
      - Storage information. For a shared file system, the File Storage service mount target and mount options are shown
      - Information on nodes
  - Details for Custom Tasks or Paused Tasks, if any
  - SSH Keys information, if any

2. To create the cloned environment, click **Submit**.

3. You can check the status of the job to clone the source environment in the Jobs page.

Perform Post-Cloning Tasks:

After the environment is successfully cloned, perform any necessary post-cloning steps and access the cloned environment following the instructions provided in Perform Post-Provisioning and Post-Cloning Tasks, page 9-27.

Clone an Oracle E-Business Suite Environment with the Database on Exadata Database Service Dedicated

This feature provides a method to clone an Oracle E-Business Suite environment that includes an Oracle database running on Oracle Exadata Database Service on Dedicated Infrastructure. The database cloning operation utilizes Exadata snapshots.

This procedure is supported on Oracle E-Business Suite Release 12.2 environments with Oracle Database 19c only.

> **Note:** Snapshots and clone databases are brought down when the Exadata VM Cluster nodes are restarted. Therefore, when the Exadata VM Cluster is restarted, wait five minutes and then start the snapshot and clone databases manually after the restart.

Cloning using Exadata Snapshots is a two-step process:

First, you must create a snapshot of the source environment. This process performs the following actions:

1. Creates a snapshot of the source environment's database. A snapshot is a point-in-time, read-only backup of an Exadata database system. Any changes to the source environment after the snapshot is taken are not propagated to the snapshot. To obtain a snapshot with updated data, you must create a new snapshot.

2. Creates a snapshot of the source environment's primary application tier node. Regardless of the number of application tier nodes on the source environment, only the primary application tier node is cloned. Note: After the snapshot creation is complete, this cloned Compute VM is stopped because its only purpose is in creating clones and not for any transactions.

Then, you will create a clone from the snapshot to create a new environment. This process performs the following actions:

1. Clones the snapshot database to create a new, cloned database. The cloned database is a sparse or thin clone, meaning only the data that is different from the parent (snapshot) is stored on the disk.

2. Clones the application tier node from snapshot. You have the option to specify more nodes and/or zones as required.

The following are characteristics of cloning using Exadata Snapshots:

- The source and cloned environments need not have the same number of application tier nodes. When specifying the cloning details in the Application Tier page, you have the option to add more zones and nodes.
- The application tier file system type of the cloned environment will be the same as that of the source. This cannot be changed.
- You can create multiple snapshots from a single source environment. Note that you cannot create a snapshot of an Exadata environment that is itself a clone.
- You can create multiple clones from a single snapshot. Note that the snapshot cannot be deleted if any clones exist. Therefore, you must delete any clones before you can delete the snapshot.
- Because snapshot creation clones only the primary application tier node, any customizations done to secondary nodes will be lost during snapshot creation. For example, only custom block volumes attached to the primary node are cloned.
- If you add any custom database services to the source database before creating the snapshot, these services are moved to the snapshot database as well. But, these custom services will retain their original definitions and might not be valid in the cloned environment. Therefore, you should recreate any custom database services after the snapshot and clone creation.
- The cloned environment has a cloned database, called the Sparse Clone database, that is a read/write-enabled database. Initially, the Sparse Clone database refers to data from the snapshot database. Any changes made on the Sparse Clone database are stored on the cloned database only.
- Currently the Oracle Home of the cloned database is separate from that of the snapshot database. Oracle E-Business Suite Cloud Manager does not support a shared Oracle Home between the snapshot and the cloned database.

> **Note:** The Oracle E-Business Suite Cloud Manager Cloning Using Exadata Snapshots feature cannot currently be used if you are also using OCI Data Guard automation.

Prerequisites

❒ Ensure that you have configured your Exadata VM Cluster properly according to Create Exadata Infrastructure and Associated VM Cluster for Exadata Database Service on Dedicated Infrastructure (Conditionally Required)., page 3-44

❒ Ensure that Patch 31033380 [https://updates.oracle.com/download/31033380.html] has been applied to your source database.

❒ Perform the following steps on your source database tier if your database was upgraded from 12c to 19c:

1. Update the `sqlnet.ora` file under the `$ORACLE_HOME/network/admin/<CDB name>` directory on all the database nodes by removing the extra `/` (slash) at the end of the file system path specified for the `DIRECTORY` parameter in the `ENCRYPTION_WALLET_LOCATION` parameter.

   That is, change

   ```
   ENCRYPTION_WALLET_LOCATION = (SOURCE=(METHOD=FILE)(METHOD_DATA=
   (DIRECTORY=/var/opt/oracle/dbaas_acfs/amp12c/tde_wallet/)))
   ```

   to

   ```
   ENCRYPTION_WALLET_LOCATION = (SOURCE=(METHOD=FILE)(METHOD_DATA=
   (DIRECTORY=/var/opt/oracle/dbaas_acfs/amp12c/tde_wallet)))
   ```

   Note that the `/` after `tde_wallet` is removed.

2. Run the following command on one of the database nodes as the root user:

   ```
   dbaascli tde enableWalletRoot -dbname <CDB name> --dbRestart
   rolling
   ```

Create a Snapshot:

Follow this procedure to create a snapshot.

1. Select the source environment. From the Environments page, select an environment created with Exadata as its DB Service Type.

2. From the Environment Details page, click the **Create Snapshot** button.

3. Enter a name for the snapshot. This name can be up to 20 alphanumeric characters long, and must begin with an alphabetical character.

4. Enter the Database Name for the snapshot. This name can be up to 20 alphanumeric characters long, and must begin with an alphabetical character.

5. Enter values for the snapshot details:

   - Enter a Snapshot Password, and confirm it. This password must be nine to thirty characters long and contain at least two uppercase, two lowercase, two numeric, and two special characters. Special characters may be an underscore (_) or a hash (#) only. Note: This password will be used for the APPS, WebLogic Server and Database Admin user passwords on the snapshot.

   - Enter the APPS password for the source environment. This entry is validated after you select the Create Snapshot button.

- Select the Snapshot Application Tier Node VM Shape for the primary node from the list provided. Only the primary application tier node will be cloned in the snapshot creation.

  If you have selected a flexible shape (for example, VM.Standard.E4.Flex), also select the number of OCPUs and the amount of memory in GB.

- The File System Type of the source environment is displayed and cannot be changed for the snapshot.

  If the File System Type is Shared, select the File System Service Mount Target from the list provided.

  If the File System Type is Shared, you can select Show Advanced Options to enter in additional information.

- If applicable, you can change the mount options in the Advanced Options window. Use caution in updating mount options.

  > **Important:** Specifying an incorrect mount option or unsupported parameter for shared file storage may result in provisioning failure. These options and parameters should only be edited by advanced users to meet specific needs.

- 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.

6. Click **Create Snapshot**.

7. Once you have created a snapshot, you can create a clone of it. Follow one of the procedures described below to access your snapshot for cloning.

Access a Snapshot from the Global Menu:

1. Navigate to the global menu and select Snapshots.

2. The Snapshots page displays a list of snapshots with the following information:

   - Name

- Last Job
- Source Environment
- Created [Date]
- Actions

3. Select a snapshot to view details of the snapshot.

4. Alternatively, you can delete a snapshot using the Actions menu. See: Delete a Snapshot, page 12-35.

Review Snapshot Details:

1. The Snapshot Details page displays the following:
   - Source Environment
   - EBS Compartment and Network Profile
   - Last Job
   - Creation date and time

2. In the Resources tab, under Application Tier, the following is shown:
   - Snapshot Node information
   - Block Storage information
   - File System Service Storage information, if the environment uses the File Storage service (FSS)

3. The Database Tier region of the Resources tab lists details on the database tier and a list of nodes.

4. The Clones tab includes a list of all clones created from the snapshot. Note that you cannot delete a snapshot if it has any associated clones created from it. You must delete its clones before you can delete the snapshot itself.

   You can delete a snapshot using the **Delete** button. See: Delete a Snapshot, page 12-35.

5. From the Snapshot Details page, select **Create Clone** to begin the cloning process.

Access a Snapshot from the Environment Details Page:

Another way to access a snapshot is from the Details page for the source environment.

1. Navigate to the Environments page and select the source environment.

2. From its Environment Details page, select the Snapshots tab.

3. Select the desired snapshot from the list.

4. From the Snapshot Details page, click the **Create Clone** button to begin the cloning process.

Enter Clone Details:

The details for the given snapshot are shown on the Clone Snapshot <snapshot name> page.

- Snapshot name

- EBS Compartment

- Network Profile

- Availability Domain

- File System Type

1. Enter values for the clone details:

   - **Environment Name**: Enter a name for your environment. For example: `usdev3`

   - **EBS Compartment**: This field is read-only. The EBS compartment for the cloned environment is the same as that of the source environment.

   - **Network Profile**: Select a network profile for the cloned environment. The list of available network profiles is dependent on the EBS compartment listed above. From this list of network profiles, select a network profile that includes the same Availability Domain as that of the source.

     Note that if you are cloning a File Storage service-enabled environment, you can choose a different network profile than that of the snapshot, but it also must have File Storage service enabled.

     > **Note:** The source environment snapshot and the cloned environment can also have different mount targets.

   - **Snapshot Password**: Enter the password for the snapshot. This password is validated after you select Next to go to the next page.

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 Database Tier Information:

Enter details for your cloned environment.

The following database details are read-only:

- Infrastructure Name

- Cluster Name

- Snapshot Database Name

- Database Compartment

1. Enter a Database Name. This name must contain uppercase alphabetic characters and numeric characters only. It must not begin with a numeral. Special characters and spaces are not allowed.

2. Enter a PDB Name. This name must contain uppercase alphabetic characters and numeric characters only. It must not begin with a numeral. Special characters and spaces are not allowed.

3. The Database Service Type (Exadata Infrastructure), is display-only.

4. Enter the admin password for the database of your cloned environment. This password is used for the SYSTEM and EBS_SYSTEM users as well. 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.

5. Enter a new APPS password for your cloned environment. The password must contain only alphanumeric characters.

6. If Oracle E-Business Suite System Schema Migration has been completed on the

source environment, then enter a new EBS_SYSTEM password. This password must contain alphanumeric characters only. For more information on the Oracle E-Business Suite System Schema and the EBS_SYSTEM password, see My Oracle Support Knowledge Document 2755875.1, *Oracle E-Business Suite Release 12.2 System Schema Migration* [https://support.oracle.com/rs?type=doc&id=2755875.1].

7. For a Release 12.2 environment, enter a new WebLogic Server password for your cloned environment.

8. Click **Next**.

Enter Application Tier Information:

1. Define your zones. Zone information from the source environment will appear by default.

   For more information on zones, refer to 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].

   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.

   You must define your internal (primary) zone first, before optionally defining additional zones.

   Enter values for the following properties:

   - **Name**

   - **Type**

     Note: For the first zone that you define, which is your primary zone, the Type is Internal and is not selectable.

2. You can also add internal or external zones.

3. In the **Web Entry Point** region, choose one of the following web entry types: **New Load Balancer (LBaaS)**, **Use OCI Load Balancer** to select an existing OCI load balancer, **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.

4. If you chose New Load Balancer as the web entry type, a new flexible shape load balancer will be created. Select the maximum bandwidth for your new load balancer. For example: **100 Mbps**. The minimum bandwidth will default to 10 Mbps.

5. Enter values for the following web entry properties.

   - **Protocol**: Select the protocol for access to the environment, either **http** or **https**.

   - **Hostname**: Enter a host name. The web entry host name must be in lowercase. For example: `myhost`

   - **Domain**: Enter a domain name. The web entry domain name must be in lowercase. 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.

6. Under Storage, the **File System Type** is the same as that for the source environment.

   If the File System Type is Shared then the field **File System Service Mount Target** appears along with a **Show Advanced Options** link.

7. Review the properties for each node in the Application Tier Nodes information. The following properties may be shown:

   - **Logical Hostname**

   - **Logical FQDN**

   - **Shape**

   - **Block Volume Storage (GB)**

   - **Fault Domain**

8. For a listed node, click **Edit** under the Actions column to edit the node.

9. Click **Add Node** to add a new node.

   In the **Add Node** dialog window, the following properties appear. Enter the value for each property, except in the case where it has been generated for you.

   Note that you can define a specific shape for each application tier node.

   - **Logical Hostname**
   - **Logical FQDN**
   - **Shape**: Select a shape that is available in the OCI region. Ensure that you have checked your quota in advance. When choosing a flexible shape, for example, VM.Standard.E4.Flex, use the sliders to choose the number of OCPUs and the amount of memory (GB).
   - **Block Volume Storage**

     Note: If you chose a shared File System Type earlier, the Block Volume Storage value is 0.

   - **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.

   Click **Add Node** again to save your choices.

10. Click Save Zone to save your zone definition.

11. The middleware licensing model of the source environment is inherited and cannot be changed.

12. You can choose to start the application tier services at then end of the clone creation by toggling the **Start Application Tier Services** option.

13. Define additional zones using the **Add Zone** button.

    For the additional internal zones, if **New Load Balancer (LBaaS)** is selected as the Web Entry Type for the first zone, then an extra option **Reuse Internal Zone1 Load Balancer** is displayed in the Web Entry Type list along with the options **New Load Balancer (LBaaS)**, **Use OCI Load Balancer**, and **Manually Configured Load Balancer**.

14. When you are finished adding application tier nodes, scroll to the top of the window and click **Save Zone** to save your zone definition.

15. When you are finished editing your zones, click **Next**.

Specify Your Extensibility Options:

You can optionally extend the cloning job to meet your own requirements. By default, Oracle E-Business Suite Cloud Manager follows a standard job definition for cloning. However, Oracle E-Business Suite Cloud Manager administrators can also create extended job definitions that include additional tasks as part of the cloning job. In this case you can select the appropriate extended job definition for Oracle E-Business Suite Cloud Manager to follow when cloning your source environment. If you select an extended job definition, you may need to enter values for input parameters required by the additional tasks in that job definition.

> **Additional Information:** For more information on using the Extensibility Framework to extend job definitions, see Set Up the Extensibility Framework, page 8-10.

Additionally, whether you are using the standard cloning job definition or an extended job definition, you can choose to have Oracle E-Business Suite Cloud Manager pause at specified points during the cloning job. 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 job when you are ready to proceed. See Monitor Job Status, page 13-1.

Specify Your Job Definition

1. Optionally select an extended job definition for cloning your environment in the **Job Definition** field.

2. In the Task Parameters tab, specify any parameter values required for the additional tasks in the job definition. Some parameters may include default values, which you can override as needed.

Specify Your Job Definition Details

3. Click the **Job Definition Details** tab. This tab displays a list of the phases in the job definition 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. The tier value must be Application 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:

Review the details for the cloned environment on this page.

1. Review the following:
   - Clone Details:
     - Environment Name
     - Installation Type
     - EBS Version
     - DB Version
     - Network Profile
   - Database Details:
     - Database Service Type
     - Infrastructure Name
     - Cluster Name
     - Database Name
     - PDB Name
   - Application Tier Details:

    - Middleware Licensing Model
    - Start Application Services (Yes/No)
    - Zone information, including
        - Web entry details
        - Storage information. For a shared file system, the File Storage service mount target and mount options are shown
        - Information on nodes
- Details for Custom Tasks or Paused Tasks, if any
- SSH Keys information, if any

2. To create the cloned environment, click **Submit**.

3. You can check the status of the job to clone the source environment in the Jobs page.

Perform Post-Cloning Tasks:

After the environment is successfully cloned, perform any necessary post-cloning steps and access the cloned environment following the instructions provided in Perform Post-Provisioning and Post-Cloning Tasks, page 9-27.

Delete a Snapshot:

> **Note:** For more information on zones, refer to My Oracle Support Knowledge Document 2942998.1, *DBAASAPI - Sparse cloning ACFS not reclaiming space* [https://support.oracle.com/rs?type=doc&id=2942998.1].

If you wish to delete a snapshot, you can do so from the Snapshots or Snapshot Details page.

1. If you are using the Snapshots page, select **Delete** from the Actions menu for the snapshot you wish to delete.

   Alternatively, if you are on the Snapshot Details page for the pertinent snapshot, select **Delete**.

2. At the prompt, type in the snapshot name to confirm that you want to delete it.

3. Select **Yes** to proceed with deleting the snapshot.

Back Up an Oracle E-Business Suite Environment

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 One-Click Provisioning and 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].

❒ If you are creating a backup of an Oracle E-Business Suite instance created using One-Click Provisioning, you must manually enable the archive log on the database.

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 review backup details and take actions including provisioning another environment based on a backup, refreshing an environment from a backup, or deleting a backup when you no longer need it.

For more information about how to create backups that you can manage through Oracle E-Business Suite Cloud Manager, see the following sections:

- Create a Backup of a Cloud-Based Oracle E-Business Suite Environment, page 12-37

- Schedule Backups, page 12-42

- Create a Backup of an On-Premises Oracle E-Business Suite Environment on Oracle Cloud Infrastructure, page 5-2

For more information about managing your backups using Oracle E-Business Suite Cloud Manager, see the following sections:

- Review Backups, page 12-46
- Delete a Backup, page 12-49
- Refresh an Oracle E-Business Suite Environment, page 12-52

Create a Backup of a Cloud-Based Oracle E-Business Suite Environment:

Perform the following steps when creating a backup:

1. Place the database in archive log mode (One-Click environments only), page 12-37.
2. Create a backup, page 12-37.
3. Review Oracle WebLogic Server validation warnings (conditionally required), page 12-41.
4. Take the database out of archive log mode (One-Click environments only), page 12-42.

Place the Database in Archive Log Mode (One-Click Environments only)

Prior to taking a backup of an environment created with One-Click provisioning, you must log on to the virtual machine as the oracle user and place the database in archive log mode. Here are the steps:

```
$ source orcl.env
$ sqlplus / as sysdba
SQL> shutdown immediate;
SQL> startup mount;
SQL> alter database archivelog;
SQL> alter database open;
SQL> exit;
```

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**.

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. Select `Application Tier and Database (RMAN)` as the backup type.

5. 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.

6. Enter the password for the Oracle E-Business Suite `APPS` schema for the source environment.

7. For an Oracle E-Business Suite Release 12.2 environment only, enter the Oracle WebLogic Server administration password for the source environment.

8. If Transparent Data Encryption (TDE) is enabled in the source database, enter the password for the TDE wallet.

9. If Oracle E-Business Suite System Schema Migration has been completed on the source environment, then enter the EBS_SYSTEM password. For more information, see My Oracle Support Knowledge Document 2755875.1, *Oracle E-Business Suite Release 12.2 System Schema Migration* [https://support.oracle.com/rs?type=doc&id=2755875.1].

10. You can optionally define lifecycle policy rules to specify how to manage the backup in Object Storage after it is created. Using lifecycle policy rules can help you reduce your storage costs and the amount of time you spend manually managing data. See Using Object Lifecycle Management [https://docs.oracle.com/en-us/iaas/Content/Object/Tasks/usinglifecyclepolicies.htm#Using_Object_Lifecycle_Management], *Oracle Cloud Infrastructure Documentation*.

    In order to create lifecycle policy rules, you must have a policy defined to allow the Object Storage service in your region to manage objects on your behalf, at either your tenancy or compartment level. See Assign Policies, page 3-5.

    - The objects in a backup are initially created in the Standard tier within Object Storage. If you want to move objects in the backup to the Infrequent Access tier, select one of the following lifecycle policy rules:

  - **Enable Auto-Tiering** - This rule automatically moves objects from the Standard tier to the Infrequent Access tier when the objects have not been accessed for 31 days.

  - **Move to Infrequent Access** - This rule automatically moves objects from the Standard tier to the Infrequent Access tier after the number of days you specify, regardless of whether the objects have been accessed. The lowest value you can specify for this rule is 1 day and the highest value is 1,000,000 days. The default value is 30 days.

    > **Note:** You can select only one of the tiering rules for objects in your backup, either **Enable Auto-Tiering** or **Move to Infrequent Access**. You cannot define both of these rules for the same backup.

- If you want to automatically delete objects in the backup after a certain number of days, select the **Delete** rule. Deleting objects that you no longer need can save space and reduce your storage costs. However, note that objects deleted by a lifecycle policy cannot be restored.

  The lowest value you can specify for the **Delete** rule is 1 day and the highest value is 1,000,000 days. The default value is 30 days.

  > **Note:** You can optionally choose to define a **Delete** rule in combination with either the **Enable Auto-Tiering** or the **Move to Infrequent Access**. For example, you could specify that the objects should be moved to the Infrequent Access tier after 30 days and deleted after 60 days.
  >
  > If you define both a tiering rule and a **Delete** rule, note that the tiering rule will not take effect if the objects have already been deleted. For example, if you define an **Enable Auto-Tiering** rule and also a **Delete** rule with a value of 30 days, the objects will be deleted after 30 days, so they will no longer be available to be moved to the Infrequent Access tier. Similarly, if you define a **Move to Infrequent Access** rule with a value of 45 days and also a **Delete** rule with a value of 30 days, the objects will be deleted after 30 days, so they will no longer be available to be moved to the Infrequent Access tier.

11. 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 17.

12. 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.

13. 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 Database Service Dedicated subscriptions, and in Base Database Service subscriptions with Enterprise Edition High Performance and Extreme Performance options.

14. 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.

15. Specify the section size for multisection backups. The default value is `4G`. Valid values are `2G`, `4G`, `8G`, `16G`, `32G`, `64G`, `128G`, or `256G`.

16. 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>, ...`

17. 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 9-7.

18. You can check the status of the job to create the backup in the Jobs page. Locate the `create-ossbackup` job that you want to troubleshoot, and click the job name link to go to the Job Details page. See Monitor Job Status, page 13-1.

    The Job 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 job does not succeed, you can review the related log files for the specific task that failed to troubleshoot the issue.

19. After a backup is successfully created, you can review the backup details in the Backups page or in the Backups 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 9-7.

20. From the environment details page for an environment, you can refresh the environment from a backup. See Refresh an Oracle E-Business Suite Environment, page 12-52.

21. If you no longer need a backup, to begin deleting it manually, navigate to that backup in the Backups page or the Backups tab of the environment details page for the source environment, then click the action icon, and select **Delete**. If you have defined a Delete lifecycle policy rule for a backup, it will be deleted automatically after the specified number of days. You can also use a command-line API to delete a failed backup. See Delete a Backup, page 12-49.

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 job with a warning if the default threshold values are exceeded. If the job 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 job.

- `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 job.

For more information about retrying a backup creation job, see Monitor Job Status, page 13-1.

Take the Database out of Archive Log Mode (One-Click Environments only)

If you do not plan to clean up the archive logs on a regular basis, then we recommend that you turn off archivelog mode after the backup completes. To do so, log on to the virtual machine as the oracle user and complete these steps:

```
$ source orcl.env
$ sqlplus / as sysdba
SQL> shutdown immediate;
SQL> startup mount;
SQL> alter database noarchivelog;
SQL> alter database open;
SQL> exit;
```

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 8-17 and Review Environment Details, page 11-7.

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 job 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 job at that time. The status for the other scheduled backup job is marked as **Missed**.
>
> - If a backup is scheduled to be created at a certain time but another job 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 job is set to **Missed**.

You cannot retry a missed job directly. However, you can schedule another backup or manually create another backup for the environment if necessary.

If you assign a scheduling policy to create backups automatically, you may find it useful to define lifecycle policy rules as part of the assignment in order to manage objects in those backups and reduce storage costs. With lifecycle policy rules, you can automatically move objects in the backups to the Infrequent Access tier when you are not actively using them, or automatically delete the objects when you no longer need them.

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. Select `Application Tier and Database (RMAN)` as the backup type.

7. 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.

8. Enter the password for the Oracle E-Business Suite APPS schema for the source environment.

9. For an Oracle E-Business Suite Release 12.2 environment only, enter the Oracle WebLogic Server administration password for the source environment.

10. If Transparent Data Encryption (TDE) is enabled in the source database, enter the password for the TDE wallet.

11. If Oracle E-Business Suite System Schema Migration has been completed on the source environment, then enter the EBS_SYSTEM password. For more information, see My Oracle Support Knowledge Document 2755875.1, *Oracle E-Business Suite Release 12.2 System Schema Migration* [https://support.oracle.com/rs?type=doc&id=2755875.1].

12. You can optionally define lifecycle policy rules to specify how to manage the backups in Object Storage after they are created. Using lifecycle policy rules can help you reduce your storage costs and the amount of time you spend manually managing data. See Using Object Lifecycle Management [https://docs.oracle.com/en-us/iaas/Content/Object/Tasks/usinglifecyclepolicies.htm#Using_Object_Lifecycle_Management], *Oracle Cloud Infrastructure Documentation*.

    In order to create lifecycle policy rules, you must have a policy defined to allow the Object Storage service in your region to manage objects on your behalf, at either your tenancy or compartment level. See Assign Policies, page 3-5.

    - Objects in a backup are initially created in the Standard tier within Object Storage. If you want to move objects in the backups to the Infrequent Access tier, select one of the following lifecycle policy rules:

        - **Enable Auto-Tiering** - This rule automatically moves objects from the Standard tier to the Infrequent Access tier when the objects have not been accessed for 31 days.

        - **Move to Infrequent Access** - This rule automatically moves objects from the Standard tier to the Infrequent Access tier after the number of days you specify, regardless of whether the objects have been accessed. The lowest value you can specify for this rule is 1 day and the highest value is 1,000,000 days. The default value is 30 days.

            Note: You can select only one of the tiering rules for objects in your backups, either **Enable Auto-Tiering** or **Move to Infrequent Access**. You cannot define both of these rules for the same backups.

- If you want to automatically delete objects in the backups after a certain number of days, select the **Delete** rule. Deleting objects that you no longer need can save space and reduce your storage costs. However, note that objects deleted by a lifecycle policy cannot be restored.

  The lowest value you can specify for the **Delete** rule is 1 day and the highest value is 1,000,000 days. The default value is 30 days.

  > **Note:** You can optionally choose to define a **Delete** rule in combination with either the **Enable Auto-Tiering** or the **Move to Infrequent Access**. For example, you could specify that the objects should be moved to the Infrequent Access tier after 30 days and deleted after 60 days.
  >
  > If you define both a tiering rule and a **Delete** rule, note that the tiering rule will not take effect if the objects have already been deleted. For example, if you define an **Enable Auto-Tiering** rule and also a **Delete** rule with a value of 30 days, the objects in each backup will be deleted after 30 days, so they will no longer be available to be moved to the Infrequent Access tier. Similarly, if you define a **Move to Infrequent Access** rule with a value of 45 days and also a **Delete** rule with a value of 30 days, the objects will be deleted after 30 days, so they will no longer be available to be moved to the Infrequent Access tier.

13. 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 17.

14. 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.

15. 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 Database Service Dedicated subscriptions, and in Base Database Service subscriptions with Enterprise Edition High Performance and Extreme Performance options.

16. 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.

17. Specify the section size for multisection backups. The default value is `4G`. Valid values are `2G`, `4G`, `8G`, `16G`, `32G`, `64G`, `128G`, or `256G`.

18. 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>, ...`

19. Click **Assign**.

20. 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 11-7.

2. The Backups page displays the available backups within the compartment that is selected in the **EBS Compartment** field in the Oracle E-Business Suite Cloud Manager header. The list can include 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
   - EBS Version: Oracle E-Business Suite version
   - DB Version: Database version
   - ADB Compatible: Whether the backup is created to be compatible with Autonomous Database for use in a migration to Autonomous Database
   - Database Name: Database name
   - TDE Enabled: Whether TDE is enabled for the environment
   - Backup Type: Whether the backup contains the full environment, including both the application tier and the database, or only the application tier
   - Restored DB Size: The size of the database after it is restored
   - Created On: Creation date and time
   - Method: The method used to create the backup, either Recovery Manager (RMAN) or Oracle Data Pump Export and Import

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 9-7.

4. To delete a backup, click the **Actions** icon next to that network profile, and then select **Delete**. See Delete a Backup, page 12-49.

5. To review additional details for a backup, click the backup name link.

6. In the backup details page, review the following properties:

   - Backup name

- EBS Version: Oracle E-Business Suite version

- Database Name: Database name

- Restored DB Size: The size of the database after it is restored

- DB Version: Database version

- TDE Enabled: Whether TDE is enabled for the environment

- Created On: Creation date and time

- ADB Compatible: Whether the backup is created to be compatible with Autonomous Database for use in a migration to Autonomous Database

- Backup Type: Whether the backup contains the full environment, including both the application tier and the database, or only the application tier

- Method: The method used to create the backup, either Recovery Manager (RMAN) or Oracle Data Pump Export and Import

7. In the Resources region, review the following properties for the backups of the application tier and of the database tier:

   - Bucket Name: Bucket name where the backup is stored in Oracle Cloud Infrastructure Object Storage

   - Auto Tiering Enabled: Whether auto-tiering is enabled to move objects in the backup to the Infrequent Access tier automatically when they have not been accessed for 31 days

   - A list of lifecycle policy rules defined for the backup, including the rule name, whether the rule is active, the target, the action (either deleting objects in the backup or moving the objects to the Infrequent Access tier), and the number of days after which the rule's action is performed

     > **Note:** Lifecycle policy rules must match for all objects in the same bucket, including an application tier and database tier stored in the same bucket.
     >
     > You must ensure that the content of the buckets is present and that the lifecycle policy rules for the application tier and database tier match before conducting any lifecycle operation.

8. Click a bucket name link to review the bucket and lifecycle policy rule details in the Oracle Cloud Infrastructure console. If you are not already logged in to the console,

then you must log in before you can view the console. See Using Object Lifecycle Management [https://docs.oracle.com/en-us/iaas/Content/Object/Tasks/usinglifecyclepolicies.htm#Using_Object_Lifecycle_Management], *Oracle Cloud Infrastructure Documentation*.

> **Caution:** Although you can review details for your backups and the objects within them using the Oracle Cloud Infrastructure console, do not use the console to make any changes to the lifecycle policy rules for backups created through Oracle E-Business Suite Cloud Manager. Use only Oracle E-Business Suite Cloud Manager to manage lifecycle policy rules for these backups.

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 Environment on Oracle Cloud Infrastructure, page 5-2 or Create a Backup of a Cloud-Based Oracle E-Business Suite Environment, page 12-37.

> **Note:** In addition to deleting backups manually, you can also optionally define lifecycle policy rules to delete backups automatically when you no longer need them. You can specify a Delete rule either while creating an individual backup or while assigning a scheduling policy to create backups automatically for an environment. See: Create a Backup of a Cloud-Based Oracle E-Business Suite Environment, page 12-37 or Schedule Backups, page 12-42.

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 job to delete the backup in the Jobs page. See: Monitor Job Status, page 13-1.

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 job logs for the failed job. See the section Monitor Job Status, page 13-1 for more information. The session ID should be in the format `<STAGE_DIRECTORY>/session/<SESSION_ID>`. An example is `/u01/db1/session/xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx`.

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:

   ```
   $ ps -ef|grep remoteclone|grep xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
   ```

   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:

      ```
      $ cd /u01/install/APPS/apps-unlimited-ebs/RemoteClone
      ```

   2. Run the following command with the required details to delete the bucket.

      Note: You must provide the proxy details if the connection to ObjectStorage is going through a proxy server.

```
$ 3pt/jre/bin/java -cp lib/cln_utils.jar:3pt/ext-jars/*
oracle.apps.liftNshift.commandline.client.bmcs.
EBSLiftBMCSDeleteBucketClient
-bucketName <bucketName> [-proxyPort <proxyPort>] [-proxyProtocol
<proxyProtocol>] -bmcsTenantName <bmcsTenantName> -compartmentID
<compartmentID>
[-proxyUsername <proxyUsername>] -bmcsConfigFilePath
<bmcsConfigFilePath>
[-proxyHost<proxyHost>] [-h]
```

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..
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  -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..
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  -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

Backing Up a Database to Object Storage Using RMAN [https://docs.cloud.oracle.com/en-us/iaas/Content/Database/Tasks/backingupOSrman.htm]

Oracle Database Backup and Recovery User's Guide 19c [https://docs.oracle.com/en/database/oracle/oracle-database/19/bradv/toc.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]

Refresh an Oracle E-Business Suite Environment

You can use the Refresh feature in Oracle E-Business Suite Cloud Manager to replace, or refresh, both the database contents and the applications code in the target environment from a backup, while preserving the target environment's infrastructure and topology. For example, you can refresh an environment using one of its own backups if you want to return the environment to an earlier saved state, or you can refresh an environment using a backup from a different compatible environment, such as refreshing a test environment from a production environment.

The Refresh feature is available for environments with a source and target of Oracle E-Business Suite Release 12.2 with Oracle Database Release 19c.

Attributes:

The following restrictions apply for refreshing environments:

- The backup must be at the same Oracle E-Business Suite release level as the target environment. For example, Release 12.2.8.
- The backup must be at the same Oracle Applications DBA (AD) and Oracle E-Business Suite Technology Stack (TXK) codelevel as the target environment. For example, AD and TXK Delta 13.

The refresh operation copies the following objects from the backup to the target environment:

- The database contents, including the data model, data, and applications code

- The applications code (binaries), including the APPL_TOP and COMMON_TOP directories

The refresh operation preserves the following objects in the target environment:

- The operating system
- The technology stack, including the following:
  - The 10.1.2 ORACLE_HOME, FMW_HOME, and related configuration
  - The Oracle WebLogic Server domain
- The INST_TOP directory, including context files and configuration files
- The database ORACLE_HOME
- The contents of the FND_NODES and AD_NODES_CONFIG_STATUS tables

> **Additional Information:** See Architecture [https://docs.oracle.com/cd/E26401_01/doc.122/e22949/T120505T120508.htm], *Oracle E-Business Suite Concepts* and File System Structure [https://docs.oracle.com/cd/E26401_01/doc.122/e22949/T120505T120509.htm], *Oracle E-Business Suite Concepts*.

Refresh an Oracle E-Business Suite Environment from a Backup:

Access the Refresh Environment Page

1. Click the **Navigator** icon and select Environments.
2. For a successfully created environment, click the environment name link.
3. In the environment details page, click the **Refresh** button.
4. Alternatively, if you want to refresh the environment from one of its own backups, select the Backups tab in the environment details page. Then click the **Action** icon and select **Refresh**.

Enter Refresh Environment Details

On this page the details for the target environment are shown:

- Environment Name
- EBS Compartment
- Network Profile

- Database Name
- Pluggable Database Name
- Availability Domain
- File System Type

1. Enter the credentials for the target environment to be refreshed:

   - **Database ADMIN Password**: Enter the admin password for the database.
   - **WebLogic Server Password**: For an Oracle E-Business Suite Release 12.2 environment only, enter the Oracle WebLogic Server administration password.
   - **Apps Password**: Enter the password for the Oracle E-Business Suite APPS schema for the environment.
   - **SYSADMIN Password**: Enter the password for the SYSADMIN user for the environment.
   - **EBS_SYSTEM Password**: If Oracle E-Business Suite System Schema Migration has been completed on the source environment, then enter the EBS_SYSTEM password. For more information, see My Oracle Support Knowledge Document 2755875.1, *Oracle E-Business Suite Release 12.2 System Schema Migration* [https://support.oracle.com/rs?type=doc&id=2755875.1].

2. Enter the details for the backup that you want to use to refresh the target environment. If you started the refresh operation by selecting one of that environment's own backups within the Backups tab in the environment details page, then the details for that backup are automatically displayed in these fields.

   - **Backup Compartment**: Select the compartment where the backup is stored.
   - **Backup Type**: The page displays the type of the available backups.
   - **Backup**: Select the backup that you want to use to refresh the target environment.

3. Enter the credentials for the backup:

   - **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.
   - **Source Wallet Password**: (Conditionally Required) If you selected a backup

created from a TDE-enabled source environment, enter the source wallet password.

4. You can optionally specify advanced Recovery Manager (RMAN) details. To do so, click **Show Advanced Options**. If you do not need to change the RMAN details, skip to step 6.

5. Specify the number of RMAN staging channels to allocate for refreshing the environment. 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.

6. Click **Next**.

Specify Your Extensibility Options

You can optionally extend the refresh job to meet your own requirements. By default, Oracle E-Business Suite Cloud Manager follows a standard job definition for refreshing an environment. However, Oracle E-Business Suite Cloud Manager administrators can also create extended job definitions that include additional tasks as part of the refresh job. In this case you can select the appropriate extended job definition for Oracle E-Business Suite Cloud Manager to follow when refreshing your target environment. If you select an extended job definition, you may need to enter values for input parameters required by the additional tasks in that job definition.

> **Additional Information:** For more information on using the Extensibility Framework to extend job definitions, see Set Up the Extensibility Framework, page 8-10.

Additionally, whether you are using the standard refresh job definition or an extended job definition, you can choose to have Oracle E-Business Suite Cloud Manager pause at specified points during the cloning job. 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 refresh job when you are ready to proceed. See Monitor Job Status, page 13-1.

Specify Your Job Definition

1. Optionally select an extended job definition for refreshing your environment in the **Job Definition** field.

2. In the Task Parameters tab, specify any parameter values required for the additional tasks in the job definition. Some parameters may include default values, which you can override as needed.

Specify Your Job Definition Details

3. Click the **Job Definition Details** tab. This tab displays a list of the phases in the job definition 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**.

Review Your Refresh Environment Flow Details

Review the details for the refresh flow on this page.

1. Review the following:
   - Backup Details:
     - Backup Compartment
     - Backup Type
     - Backup
   - Details for Custom Tasks or Paused Tasks, if any

2. To refresh the target environment, click **Submit**.

3. You can check the status of the job to refresh the target environment in the Jobs page.

Promote a Standby Environment (Commercial Cloud Regions Only)

You can 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. The Database Name and PDB Name are shown but can be updated. The Database Service Type field is read-only.

   Enter the following:

   - **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**: 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.

   - **New APPS Password**: Enter a password for the APPS user.

   - **New EBS_SYSTEM Password**: If Oracle E-Business Suite System Schema Migration has been completed on the source environment, then enter a new

EBS_SYSTEM password. This password must contain alphanumeric characters only. For more information on the Oracle E-Business Suite System Schema and the EBS_SYSTEM password, see My Oracle Support Knowledge Document 2755875.1, *Oracle E-Business Suite Release 12.2 System Schema Migration* [https://support.oracle.com/rs?type=doc&id=2755875.1].

- **New WebLogic Server Password**: Enter a password for the Oracle WebLogic Server administration user on the environment.

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.

   For more information on zones, refer to 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].

   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:

   - **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 chose New Load Balancer as the web entry type, a new flexible shape load balancer will be created. Select the maximum bandwidth for your new load balancer. For example: **100 Mbps**. The minimum bandwidth will default to 10 Mbps.

- **Protocol**: Select the protocol for access to the environment, either **http** or **https**.

- **Hostname**: Enter the host name for your web entry point. The web entry host name must be in lowercase. For example: `myhost`

- **Domain**: Enter the domain for your web entry point. The web entry domain name must be in lowercase. 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 Environments, page 3-9.

3. When promoting an environment that uses File Storage service, the File System details are shown by default:

   - File System Type (Shared)

   - File System Name

   - File System OCID

   - File Storage Mount Target

   - Storage Type

     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**: You can change the shape of the node. When choosing a flexible shape, for example, VM.Standard.E3.Flex, use the sliders to choose the number of OCPUs and the amount of memory (GB).
   - **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 standby promotion job to meet your own requirements. By default, Oracle E-Business Suite Cloud Manager follows a standard job definition for promotion. However, Oracle E-Business Suite Cloud Manager administrators can also create extended job definitions that include additional tasks as part of the promotion job. In this case you can select the appropriate extended job definition for Oracle E-Business Suite Cloud Manager to follow when promoting your environment. If you select an extended job definition, you may need to enter values for input parameters required by the additional tasks in that job definition.

> **Additional Information:** For more information on using the Extensibility

> Framework to extend job definitions, see Set Up the Extensibility Framework, page 8-10.

Additionally, whether you are using the standard promotion job definition or an extended job definition, you can choose to have Oracle E-Business Suite Cloud Manager pause at specified points during the promotion job. 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 promotion job when you are ready to proceed. See Monitor Job Status, page 13-1.

Specify Your Job Definition

1. Optionally select an extended job definition for promoting your environment in the **Job Definition** field.

2. In the Task Parameters tab, specify any parameter values required for the additional tasks in the job definition. Some parameters may include default values, which you can override as needed.

Specify Your Job Definition Details

3. Click the **Job Definition Details** tab. This tab displays a list of the phases in the job definition 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; job definition details, and SSH key information.

2. To promote your environment, click **Submit**.

3. You can check the status of the job to promote the environment in the Jobs page.

   A standby environment that has just been promoted successfully has the value "promote-standby (Successful)" in the Environment Details page, with a link to the Job Details page. See Review Job Status, page 13-3 for more information.

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
   ```

2. Depending on the Oracle E-Business code level of your environment, Oracle E-Business Suite Cloud Manager may initially place the environment in lockdown mode to prompt you to review and respond to the secure configuration recommendations. In this case, a system administrator must resolve or acknowledge the recommended security configurations in the Secure Configuration Console to unlock the system for normal usage. See Review Secure Configuration Recommendations for Oracle E-Business Suite, page 9-47.

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 Job 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.

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 9-4, Advanced Provisioning, page 9-7, or Clone an Oracle E-Business Suite Environment, page 12-5.

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.

If you have existing cloned environments of a source environment with a shared file system, then deleting the source environment does not delete the source, or parent, file system, because the parent file system is still in use by the cloned environments. Therefore, it is recommended that you delete all cloned environments before deleting the source environment on which they are based, in order to remove the shared file system.

If you have cloned an Oracle E-Business Suite environment that includes an Oracle database running on Oracle Exadata Database Service on Dedicated Infrastructure, then you must delete all cloned environments before deleting their associated snapshot.

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 Job status shown as Successful, Aborted, or Failed, then select **Delete**. Alternatively, from the Environment Details page for a specific environment, select the **Delete** button.

2. In the confirmation window, enter the environment name to confirm your choice. Then click **Yes**.

3. You can check the status of the job to delete the environment in the Jobs page. See: Monitor Job Status, page 13-1.

   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.

   ```
   $ 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> --session-dir <session dir to create temporary files and
   log files>
   ```

13

Monitor Job Status

This chapter covers the following topics:

- Monitor Job Status

Monitor Job Status

You can monitor the status of a job performed within Oracle E-Business Suite Cloud Manager to check its progress, resume a paused job, and retry a failed job if necessary. Each job 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 jobs:

- `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.

- `clone-snapshot` - Cloning a previously provisioned 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 environment that was stored on Oracle Cloud Infrastructure.

- `refresh-ebs` - Refreshing an Oracle E-Business Suite environment from a backup.

- `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.

- `pre-discover-ebs` - Checking whether an Oracle E-Business Suite environment that is not currently registered in Oracle E-Business Suite Cloud Manager meets the requirements for discovery.

- `discover-ebs` - Discovering an Oracle E-Business Suite environment and registering its metadata in Oracle E-Business Suite Cloud Manager.

- `soft-cleanup` - Unregistering an Oracle E-Business Suite environment and removing its metadata from Oracle E-Business Suite Cloud Manager.

- `create-network-profile` - Creating a network profile. Jobs of this type are displayed only if you are logged in as an Oracle E-Business Suite Cloud Manager administrator.

  > **Note:** To have Oracle E-Business Suite Cloud Manager administrator privileges, a user must be a member of the Oracle E-Business Suite Cloud Manager administrator group that was specified during configuration of this Oracle E-Business Suite Cloud Manager instance. For more details, see Configure Oracle E-Business Suite Cloud Manager Compute Instance, page 2-37.

If you added pauses in the job definition for a job 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 a job 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 job when you are ready to proceed.

If a job fails, you can review the log for the specific task that failed to help you resolve the problem before you retry the job. When you retry a job, depending on the task that failed, Oracle E-Business Suite Cloud Manager may either continue the job from the point of failure or clean up the previous attempt and restart the job from the beginning.

> **Note:** You must have a minimum of 10 GB of free disk space in order to run Oracle E-Business Suite Cloud Manager jobs, including provisioning, discovery, configuration, and all lifecycle management activities.

- Review Job Status, page 13-3
- Resume a Paused Job, page 13-6
- Retry a Failed Job, page 13-6

Review Job Status:

1. To review job status, click the **Navigator** icon, and then select **Jobs**.

   > **Note:** Alternatively, you can review a list of the jobs performed for a particular environment in the environment details page for that environment. See Review Environment Details, page 11-7.
   >
   > You can also review the history of all jobs 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 job type you are interested in reviewing and the timestamp when the job was performed.

2. The Jobs page lists the most recent job of each type for each Oracle E-Business Suite environment and each backup within the compartment that is selected in the **EBS Compartment** field in the Oracle E-Business Suite Cloud Manager header. The list includes jobs for successfully deployed environments as well as jobs for any incomplete or failed attempts. If you are logged in as an Oracle E-Business Suite Cloud Manager administrator, then the page also lists the most recent job for each network profile. Jobs are listed in order by start time.

   > **Note:** To have Oracle E-Business Suite Cloud Manager administrator privileges, a user must be a member of the Oracle E-Business Suite Cloud Manager administrator group that was specified during configuration of this Oracle E-Business Suite Cloud Manager instance. For more details, see Configure Oracle E-Business Suite Cloud Manager Compute Instance, page 2-37.

You can optionally enter a full or partial value in the search field to display only jobs whose properties contain that value. You can search by the following properties shown in this page:

- Job name
- Status, either **Input Validation in Progress**, **Scheduled**, **In Progress**, **Paused**, **Successful**, **Failed**, **Aborted**, or **Missed**
- Action being performed
- User who submitted the job
- Start time, if applicable
- End time, if applicable

3. When you first submit a job, its status is set to **Input Validation in Progress**. After the validation is completed, if the processing engine is available to start performing the job, the job status changes to **In Progress**. If the processing engine is not immediately available, the job status is first set to **Scheduled** and then changes to **In Progress** later when the processing engine starts performing the job.

   If you added a pause before a particular phase of a provisioning or cloning job, then when the job reaches that point, the job status changes to **Paused**. After you have performed any necessary manual action, you can resume the job. The job then returns to the **In Progress** status. See Resume a Paused Job, page 13-6.

   When a job is in progress, continue monitoring it until the job 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 job that you submitted is completed successfully.

   Alternatively, you can intentionally abort in-progress jobs by stopping the Oracle E-Business Suite Cloud Manager VM services with the `stopall force` options. When you restart the services, jobs that were previously in progress are changed to the status **Aborted**. See Abort Running Jobs, page 4-9.

   > **Note:** A scheduled backup job can be run only when no other job 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 job at that time. The status for the other scheduled backup job is marked as **Missed**.

- If a backup is scheduled to be created at a certain time but another job 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 job is set to **Missed**.

You cannot retry a missed job directly. However, you can schedule another backup or manually create another backup for the environment if necessary. See Schedule Backups, page 12-42 and Create a Backup of a Cloud-Based Oracle E-Business Suite Environment, page 12-37.

4. For jobs with a status of **In Progress**, **Paused**, **Successful**, **Failed**, **Aborted**, or **Missed**, click the job name link to navigate to the Job Details page.

   Alternatively, you can navigate to the Job Details page for an environment-related job by clicking the job status link in the Environments page or the job name link in the environment details page.

5. In the Job Details page, you can review the following job properties:

   - Job name
   - Environment name or network profile name
   - User who initiated the job
   - Prevalidation status
   - Main run 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
   - Job definition that identifies the phases and tasks in the job

6. The Job Details page also displays a list of the phases and tasks that make up the job, 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 Job Details page automatically, click the Auto Refresh toggle switch. When Auto Refresh is on, the page refreshes every 20 seconds and displays the date and time of the last refresh.

8. If a job fails, click **Download Logs** to download the complete job logs. You can review the log details to help you resolve the problem before you retry the job. See Retry a Failed Job, page 13-6.

Resume a Paused Job:

1. If you added a pause before a particular phase of a job such as provisioning, cloning, or promoting a standby environment, then when the job reaches that phase, the job 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 job definition, navigate to the Job Details page for the job and click **Resume**.

   Note: You cannot resume jobs with any status other than **Paused**.

Retry a Failed Job:

1. To retry a failed job, navigate to the Job Details page for the job and click **Retry**.

   Note: You cannot retry jobs with any status other than **Failed**.

2. When you retry a job, Oracle E-Business Suite Cloud Manager marks the original failed job as the parent of the newly initiated child job. For a child job, the Jobs page and the Job Details page both display a **Parent Job** link along with the other job properties. Click the **Parent Job** link to navigate to the Job Details page for the parent job.

3. Similarly, for a parent job the Job Details page displays a **Child Job** link which you can click to navigate to the Job Details page for the child job.

   Note that you can only retry a particular failed job once, so after you have retried the job, the Retry action is disabled for that job. Instead, monitor the status of the child job to track its progress. If the child job 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 job. See Delete an Oracle E-Business Suite Environment, page 12-62 and Delete a Backup, page 12-49.

> **Note:** You can use the `ebscmadmin` utility to skip a task in order to enable resumption of a failed job after steps have been taken to correct the underlying issue. See Resume Job Execution After Manual Intervention, page 4-17.

A

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 job definitions in the Extensibility Framework.

Table A-1 Seeded Tasks

Task Name	Description
Run AutoConfig on R12.2 Application Tier nodes	Stops the application tier services, runs Autoconfig, and brings the application tier services back up.
Run AutoConfig on R12.1 Application Tier nodes	Stops all application tier services, runs Autoconfig, and brings the application tier services back up.
Change database archive mode on R12.2 environments	Changes the database archive mode on R12.2 environments. All application tier services are restarted.
Change database archive mode on R12.1 environments	Changes the database archive mode on R12.1 environments. All application tier services are restarted.

Task Name	Description
Change database administrator users passwords on R12.2 environments	Changes the following database users passwords SYS, SYSTEM, DBSNMP. All application tier services are restarted. **Note:** When you submit a job 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.
Change database administrator users passwords on R12.1 environments	Changes the following database users passwords SYS, SYSTEM, DBSNMP. All application tier services are restarted. **Note:** When you submit a job 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.
Change APPS password on R12.2 environments	Changes the APPS password on R12.2 environments. All application tier services are restarted.
Change APPS password on R12.1 environments	Changes the APPS password on R12.1 environments. All application tier services are restarted.
Change WebLogic administration user password	Changes the WebLogic administration user password and restarts all application tier services.

Task Name	Description
Change Oracle Forms mode from Servlet to Socket on R12.1 environments	Changes Oracle Forms mode from Servlet to Socket on R12.1 environments, it runs an implicit AutoConfig. All application tier services are restarted. **Note:** When you submit a job 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.
Configure Oracle OHS PID and LOCK directory paths on R12.1 environments	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 run and all application tier Services are restarted.
Start Application Tier services for R12.2 environments	Starts all application tier services in all nodes of a R12.2 environment.
Start Application Tier services for R12.1 environments	Starts all application tier services in all nodes of a R12.1 environment.
Stop Application Tier services for R12.2 environments	Stops all application tier services in all nodes of a R12.2 environment.
Stop Application Tier services for R12.1 environments	Stops all application tier services in all nodes of a R12.1 environment.
Install RPM from Oracle central yum repository	Installs the given RPM from Oracle central yum repository.
Create a new WebLogic Monitor user	Creates a new WebLogic Monitor user on EBS R12.2 environments.
Enable license for products	Enables licensing for products determined by the end-user.
Run Online Patching fs-clone phase on R12.2 environments	Runs Online Patching fs-clone phase on R12.2 environments.

Task Name	Description
Grant EM Monitoring role to a database user	Grants the role em_oam_monitor_role to DBSNMP and to a specified user.
Change sysadmin user password	Changes the sysadmin user password.
Install Oracle Support Analyzers	Installs Oracle Support Analyzers.
Change EBS_SYSTEM user password on R12.2 environments	Changes EBS_SYSTEM user password. All application tier services are restarted.

Custom Task Scripts in the Extensibility Framework

The Extensibility Framework lets you extend the jobs 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.

1. Create a wrapper script, page A-4.
   - Parse input parameters, page A-8.
   - Access environment variables, page A-9.
   - Invoke other programs, page A-9.
   - Source other scripts, page A-10.
   - Run dos2unix (Windows only), page A-20.
2. Test the script, page A-20.
3. Package the script in a zip file, page A-21.

For more information, see the following references.

Set Up the Extensibility Framework, page 8-10

Create a Task, page 8-13

Create a Wrapper Script

Each custom task that you want include in Oracle E-Business Suite Cloud Manager jobs 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.
>
> Additionally, note that this example is valid for Oracle E-Business Suite environments on R12.AD.C.Delta.12 and R12.TXK.C.Delta.12 or earlier AD-TXK release update packs. This example does not apply for R12. AD.C.Delta.13 and R12.TXK.C.Delta.13 or later.

```
#!/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>
#
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
#
========================================================================
===+
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
}

#
========================================================================
===+
#    Getting the CONTEXT_FILE Environment variable
#
========================================================================
===+
function getADTOPFromEnv(){
    echo $AD_TOP
}


#
========================================================================
===+
#                       Execution
#       Write Business logic to execute or invoke the scripts..
#
========================================================================
===+
getNonSensitiveParameters $@
getSensitiveParameters
adTop=$(getADTOPFromEnv)

sqlplus -S apps/$appsPwd  @$adTop/patch/115/sql/ADZDREG.sql $systemPwd
$appsUser $customSchemaName

if [ "$?" -ne "0" ]; then
    echo "Unable to register custom schema $customSchemaName"
    exitMain
fi

# any other business logic can be added here or calling any other
scripts or program.

# If the execution is successful, can exitSuccess or return 0
exitSuccess
```

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 a job 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 job.

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:

```
function getADTOPFromEnv(){
    echo $AD_TOP
}
```

The following example shows how to subsequently assign the value of the environment variable:

```
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.

```
{ 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 jobs. The following example shows sample code for calling a Perl file:

```
{ 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:

```
{ 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:

```
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)

    isNull $context_type
    if [ "$?" -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 credetials
# 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 "Not able to find adProvisionEBS.pl file in the PATH."
            echo "Please check if the environment is sourced."
        fi
    else
        echo "ERROR : Not able to find PERL executable."
    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
}
```

```
# Staring the Weblogic Admin Server
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 credentails are passed"
            fi
        else
            echo "Not able to find the adadminsrvctl.sh"
            echo "Please check if the environment is sourced"
        fi
    else
        echo "Not a Primary Node"
    fi

    return $retCode

}

# To check if the Domain is editable or not
function isDomainEditable()
{
    wls_pwd=$1

    retCode=$RETURN_FALSE

    s_wls_home=$(getCtxValue s_wls_home)
    s_wls_home=$(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)


    if [[ -z "$s_wls_home" || ! -f "${s_wls_home}/server/bin/setWLSEnv.
sh" ]]; then
        echo "Not able to source the WLS environment file."
        echo "Please check if environment is soured.."
    else
        . ${s_wls_home}/server/bin/setWLSEnv.sh

wls_admin_url="$s_wls_admin_host.$s_wls_admin_domain:$s_wls_adminport"

        if [[ -z "$s_wls_admin_user" || -z "$s_wls_admin_host" || -z
"$s_wls_admin_domain" || -z "$s_wls_adminport" ]]; then
            echo "Either one or more of the variables s_wls_admin_user
s_wls_admin_host  wls_admin_domain  s_wls_adminport  NULL"
            echo "Please check if environment is sourced "
        else
```

```
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 "$RETURN_TRUE" ]; then
                    echo "Domain is editiable"
                else
                    echo "Domain is in editable mode"
                    retCode=$RETURN_TRUE
                fi
            else
                echo "Not able to find file txkValidateDomainInRC.py"
                echo "Please check if environment is sourced"
            fi
        fi
    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
# Intially 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
```

```
if [ "$?" -eq "$RETURN_TRUE" ]; then
            # Platform Plugable RAC/Non RAC
            dataloc=$(echo $(getCtxValue s_dbhome1) | awk -F '/' '{print
$1}')
            dbname=$(getCtxValue s_cdb_name)
            orapw_file=$dataloc/$ORACLE_UNQNAME/orapw$dbname
        else
            # Non Pluggable database. For 11204 Flows
            isRACEnabled
            if [ "$?" -eq "$RETURN_TRUE" ]; then
                orapw_file="$ORACLE_HOME/dbs/orapw$ORACLE_SID"1
            else
                # Non RAC
                orapw_file=$ORACLE_HOME/dbs/orapw$ORACLE_SID
            fi
        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 environment 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:

```
{ 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:

   ```
   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 8-13.

B

Time Zone Support in Oracle E-Business Suite Cloud Manager

This appendix covers the following topics:

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 environment. 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 Oracle E-Business Suite 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

Backup Metadata	Default Value Shown in UI	User-Selected Value	Time Zone to be set on Compute	Time Zone to be set on Base Database Service DB Systems	Exadata Infrastructure Time Zone	Time Zone Variable (TZ) to be set on Exadata Database Service Dedicated
SRC_OS_TIMEZONE = NOVALUE Profile option SERVER_TIMEZONE_ID = NOVALUE	UTC	America/New_York	America/New_York	America/New_York	Europe/London	Time zone is America/New_York
SRC_OS_TIMEZONE = Asia/Kolkata Profile option SERVER_TIMEZONE_ID = NOVALUE	Asia/Kolkata	Asia/Kolkata	Asia/Kolkata	Asia/Kolkata	Europe/London	Time zone is Asia/Kolkata

Backup Metadata	Default Value Shown in UI	User-Selected Value	Time Zone to be set on Compute	Time Zone to be set on Base Database Service DB Systems	Exadata Infrastructure Time Zone	Time Zone Variable (TZ) to be set on Exadata Database Service Dedicated
SRC_OS_TIMEZONE = NOVALUE Profile option SERVER_TIMEZONE_ID = (GMT+05:30) India Time	IST	IST	IST	IST	Europe/London	Time zone is IST
SRC_OS_TIMEZONE = IST Profile option SERVER_TIMEZONE_ID = (GMT - 5) Eastern Time	America/New_York	America/New_York	America/New_York	America/New_York	Europe/London	Time zone is America/New_York

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 that use Exadata Database Service Dedicated, where there is one system with many databases on it, Oracle E-Business Suite Cloud Manager cannot use the operating system time zone for a given environment, but instead uses the time zone defined in the Exadata Database Service Dedicated 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

Backup Metadata	Default Value Shown in UI	User-Selected Value	Time Zone to be set on Compute	Time Zone to be set on Base Database Service DB Systems	Exadata Infrastructure Time Zone	Time Zone Variable (TZ) to be set on Exadata Database Service Dedicated
SRC_OS_TIMEZONE = Asia/Kolkata Profile option SERVER_TIMEZONE_ID = NOVALUE	Asia/Kolkata	America/Los_Angeles (Override)	America/Los_Angeles	America/Los_Angeles	Europe/London	Not Set
SRC_OS_TIMEZONE = NOVALUE Profile option SERVER_TIMEZONE_ID = (GMT+05:30) India Time	Asia/Kolkata	America/Los_Angeles (Override)	America/Los_Angeles	America/Los_Angeles	Europe/London	Not Set

Backup Metadata	Default Value Shown in UI	User-Selected Value	Time Zone to be set on Compute	Time Zone to be set on Base Database Service DB Systems	Exadata Infrastructure Time Zone	Time Zone Variable (TZ) to be set on Exadata Database Service Dedicated
SRC_OS_TIMEZONE = America/New_York Profile option SERVER_TIMEZONE_ID = (GMT+05:30) India Time	Asia/Kolkata	America/Los_Angeles (Override)	America/Los_Angeles	America/Los_Angeles	Europe/London	Not Set

In the case of environments that use Exadata Database Service Dedicated, where there is one system with many databases on it, Oracle E-Business Suite Cloud Manager cannot use the operating system time zone for a given environment, but instead uses the time zone defined in the Exadata Database Service Dedicated 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.