Oracle® Essbase

Migrating Essbase Instances from Oracle Analytics Cloud to Essbase on Oracle Cloud Infrastructure via Marketplace

Release 19.3
F24346-06
September 2020

Oracle Essbase Migrating Essbase Instances from Oracle Analytics Cloud to Essbase on Oracle Cloud Infrastructure via Marketplace, Release 19.3

F24346-06

Primary Author: Essbase Information Development Team

Contents

1 Learn About Migration to Oracle Cloud Infrastructure

About the Migration Scope 1-1
About the Migration Task Flow 1-2
About the Migration Tools 1-4

2 Prepare to Migrate Essbase Instances to Oracle Cloud Infrastructure

Before You Begin with Oracle Essbase 2-1
- Create Dynamic Groups 2-6
- Set Up Policies 2-7
- Set Up Essbase Access in Identity Cloud Service 2-9
- Create a Confidential Identity Cloud Service Application 2-9
- Supported Compute Shapes 2-11
- Create Vault and Encrypt Values 2-11
- Access the WebLogic Console 2-13
- Administrator Access Requirements 2-14

Deploy Oracle Essbase 2-15
- Deploy for Version 19.3.0.2.3 2-15
- Deploy for Version 19.3.0.3.4 2-19

Complete Post-Deployment Tasks 2-22
- Modify the Confidential Identity Cloud Service Application 2-22
- Set Up the SSL Certificate 2-23
- Secure Your Network 2-25
- Migrate Users and Groups from Oracle Analytics Cloud 2-26
  - Migrate Users And Groups from Oracle Identity Cloud Service 2-26
  - Migrate Users and Groups from Embedded WebLogic LDAP Server 2-26
- Complete System Hardening and Cleanup Tasks 2-27
- Troubleshoot Deployment Errors 2-27

3 Migrate Your Essbase Instances to Oracle Cloud Infrastructure

Prepare to Migrate Cloud Service Applications and Users 3-1

Migrate Cloud Service Applications 3-2
Migrated Cloud Service Artifacts 3-2
Migrate Cloud Service Applications Using CLI Tool 3-4
Download and Use the Command-Line Interface 3-5
Selective and Ordered Import of Artifacts 3-6
LcmExport: Back Up Cube Files 3-8
LcmImport: Restore Cube Files 3-9
Migrate Cloud Service Applications Using Migration Utility 3-10

4 Complete the Post-Migration Tasks

Test the Migrated Essbase Instance 4-1
Clean Up Infrastructure and Platform Resources in Oracle Analytics Cloud - Essbase Classic (Customer Managed) 4-1
Clean Up Infrastructure and Platform Resources in Oracle Analytics Cloud - Essbase (Oracle Managed) 4-2

5 Manage Users and Roles

About Users and Roles 5-1
User Roles and Application Permissions 5-1
Provision Application Permissions 5-2

6 Monitor Essbase Operations

Monitor Operations and Resources Using Oracle Cloud Infrastructure Monitoring Service 6-1
Get Event Notifications Using Oracle Cloud Infrastructure Notifications Service 6-2

Preface

Learn how to migrate Oracle Analytics Cloud – Essbase.

Topics:

- Audience
- Documentation Accessibility
- Conventions

Audience

This document is intended for administrators within an organization who use Oracle Analytics Cloud – Essbase and plan to migrate Essbase instances from Oracle Analytics Cloud – Essbase to Essbase 19c on Oracle Cloud Infrastructure via Marketplace.

Documentation Accessibility

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

Access to Oracle Support

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

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Videos and Images

Your company can use skins and styles to customize the look of the application, dashboards, reports, and other objects. It is possible that the videos and images included in the product documentation look different than the skins and styles your company uses.

Even if your skins and styles are different than those shown in the videos and images, the product behavior and techniques shown and demonstrated are the same.

1

Learn About Migration to Oracle Cloud Infrastructure

Learn about how to migrate your existing Oracle Analytics Cloud – Essbase instance (on Oracle Cloud Infrastructure or on Oracle Cloud Infrastructure-Classic) to Essbase 19c on Oracle Cloud Infrastructure.

About the Migration Scope

About the Migration Task Flow

About the Migration Tools

About the Migration Scope

Before migrating Essbase instances from Oracle Analytics Cloud to Oracle Cloud Infrastructure, consider the scope and constraints of this migration path.

Summary

- Migration scenarios covered in this Guide
  - Source EssbaseOracle Analytics Cloud instance: , 105.2 or later

    Source Oracle Analytics Cloud - Classic instance: Essbase, 105.2 or later
  - Source Oracle Analytics Cloud Oracle Managed instance: Essbase, 105.2 or later (Oracle Identity Cloud Service instances only, not embedded LDAP)
  - Source identity management: Oracle Identity Cloud Service (Cloud accounts) or embedded LDAP server (traditional accounts)
  - Target Essbase 19c instance on Oracle Cloud Infrastructure
- Not covered in the Guide
  - Source Oracle Analytics Cloud - Classic instance: Data Visualization, Business Intelligence
  - Database migration

Migration scenarios covered in this Guide

With Oracle Analytics Cloud, you can deploy services with several different feature sets: Business Intelligence, Data Visualization, and Essbase.

This Guide only describes how to migrate services deployed with Essbase.

Before you start, Oracle recommends that you patch your source service with the latest available version. The migration tools you need aren't available in earlier versions. For Oracle Managed instances, you must be on the latest version; if not, work with Oracle Support to ensure that you are.

You can verify the current version of your source and target environments in Oracle Cloud Infrastructure Console. If you're not sure, check with your administrator.

Not covered in this Guide

This Guide doesn't describe how to migrate Oracle Analytics Cloud instances deployed with the Business Intelligence or Data Visualization, or non-Oracle Analytics Cloud artifacts, such as associated databases, security configuration, and so on. You must migrate non-Oracle Analytics Cloud artifacts separately or re-create them on the target instance.

About the Migration Task Flow

You use migration tools to migrate Essbase instances to Oracle Cloud Infrastructure. Before you start the migration, here's what you need to do.

- Deploy an Instance
- Migrate Your Service
- Complete Post-Migration Tasks

Deploy an Instance

Task	Description	More Information
Plan your new deployment	Plan your Essbase deployment on Oracle Cloud Infrastructure. Determine the details of how the stack components on Oracle Cloud Infrastructure will be deployed and the size of the Essbase VM.	Before You Begin with Oracle Essbase
Migrate users and groups	Choose one of the following options: • You can use the CLI tool to migrate one application at a time. This is applicable to the following source scenarios: Oracle Analytics Cloud - Classic that uses Embedded Weblogic LDAP or Oracle Identity Cloud Service, or Oracle Analytics Cloud that uses Oracle Identity Cloud Service. For migrating users and groups from your Oracle Analytics Cloud – Essbase account (Embedded Weblogic LDAP) to Oracle Identity Cloud Service, see the LDAP topic link, in the right column, for more information. • You can use the Migration Utility to migrate applications, users, and groups, at the same time.	• Migrate Users and Groups from Embedded WebLogic LDAP Server • Migrate Cloud Service Applications Using CLI Tool

Task	Description	More Information
Reconfigure single sign-on	(Optional) If SAML Single Sign-on (SSO) is configured in your source environment using samlssodocker, set up SSO in your target environment between your identity provider and Oracle Identity Cloud Service.	• Add an Identity Provider • Integrating Oracle Identity Cloud Service with Microsoft Active Directory Federation Services
Integrate Oracle Identity Cloud Service with other identity providers	(Optional) Use Oracle Identity Cloud Service in your target environment to integrate with your identity provider. For example: • Reconcile Microsoft Active Directory with Oracle Identity Cloud Service • Configure Oracle Identity Manager and synchronize users with Oracle Identity Cloud Service • Configure Office 365 users with Oracle Identity Cloud Service	• Manage Bridges for Oracle Identity Cloud Service • Integrate Oracle Identity Manager with Oracle Identity Cloud Service • Configure Oracle Identity Cloud Service to Provide Single Sign-On (SSO) for Office 365 • REST API for Oracle Identity Cloud Service
Deploy Essbase instance	-	Deploy Oracle Essbase
Complete post-deployment tasks	-	Complete Post-Deployment Tasks

Migrate Your Service

Task	Description	More Information
Understand migration options	Understand tool options for migrating Essbase applications.	Migrate Cloud Service Applications
Prepare for migration	Review considerations and requirements for migrating Essbase applications.	Prepare to Migrate Cloud Service Applications and Users
Understand supported artifacts	Review which global, application-level, and cube-level Essbase artifacts you can migrate.	Migrated Cloud Service Artifacts

Complete Post-Migration Tasks

Task	Description	More Information
Test the migrated instance	Check the content you migrated is available on Oracle Cloud Infrastructure and everything works as you expect.	Test the Migrated Essbase Instance
Clean up services on Oracle Cloud Infrastructure	Remove any resources that you don't need.	Clean Up Infrastructure and Platform Resources in Oracle Analytics Cloud - Essbase Classic (Customer Managed)

About the Migration Tools

The tools that you use to migrate instances to Oracle Cloud Infrastructure are shown here, and explained in this Guide.

Tools to Migrate Essbase Services

You can choose one of this methods:

- Migration Utility - migrates multiple applications, artifacts, and users at one time. Users employ the Migration Utility from the target Essbase instance.
  or
- Command Line Interface Tool - migrates source applications and artifacts across Essbase deployments and releases. This is used to migrate applications one-at-a-time. When using CLI tool, users and groups must be migrated before migrating Essbase artifacts.

2

Prepare to Migrate Essbase Instances to Oracle Cloud Infrastructure

Before you migrate instances, plan and perform the various required plan and deploy tasks.

Before You Begin with Oracle Essbase

Deploy Oracle Essbase

Complete Post-Deployment Tasks

Before You Begin with Oracle Essbase

Before you begin to set up Oracle Essbase deployment, here are pre-requisite lists of metadata you must gather and tasks that you must complete.

The quick-start process, which deploys Essbase on Oracle Cloud Infrastructure using Marketplace, uses default settings on Marketplace. The process assumes, and at times provides, less prohibitive access to infrastructure components. You're recommended to use the information here, as well as the default settings, only as a guide, and to determine the appropriate security and access requirements for your organization. You can also use Oracle Cloud Infrastructure documentation as a reference.

When Essbase is deployed on Oracle Cloud Infrastructure, you receive access to the required services based on your defined role and policies, including Oracle Cloud Infrastructure Compute Service and Oracle Identity Cloud Service.

A text worklist is provided at the end of this page, which you can copy to a text file and use for storing names, IDs, and other values needed during setup.

Table 2-1 Pre-deployment metadata

Prerequisite Metadata	Links to overviews and tasks / examples	Record values needed for deployment	Verify completion
Account and environment for Oracle Cloud Infrastructure (OCI)	-	Account	
Command Line Interface (CLI) tool installed from OCI	CLI Quickstart	-	
User name for OCI administrator	Administrator Access Requirements	Admin user name and password	
Identity Cloud Service (IDCS) system administrator user ID (or create it later with REST API for IDCS)	Administrator Access Requirements	IDCS system admin user ID	

Table 2-1 (Cont.) Pre-deployment metadata

Prerequisite Metadata	Links to overviews and tasks / examples	Record values needed for deployment	Verify completion
IDCS Essbase administrator user name, as defined during stack creation	Administrator Access Requirements	Initial Essbase administrator name	
Sufficient quota in target region and target availability domain	Regions and Availability Domains	Region Availability domain	
Encryption key to encrypt your Essbase administrator password, DB system administrator password and IDCS application client secret, using Oracle Cloud Infrastructure Vault provisioning encryption (prior to version 19.3.0.3.4 this was known as Key Management and KMS)	Create Vault and Encrypt Values	(Note: Prior to version 19.3.0.3.4, these values were: KMS key OCID and KMS service endpoint) Vault encryption key OCID Vault cypto endpoint See Overview of Vault and Using Keys in Oracle Cloud Infrastructure documentation.	
[Optional] **Load balancer** to specify shape and subnets	Overview of Load Balancing	Load balancer shape and subnets	
Compute shape for Essbase compute instance	Supported Compute Shapes	Compute shape	
[Optional] **Use existing network** setup option - if used, you must configure network infrastructure with security lists, or ask Oracle Support to create an instance	Creating a Virtual Cloud Network	Existing virtual cloud network Name	
Essbase administrator user name, as defined during stack creation. User can be same as IDCS admin name.	Administrator Access Requirements	Also known asEssbase 911 user name (administrator who manages the WebLogic server on which Essbase runs)	
Essbase Node Public IP	-	If creating a private Essbase subnet, and deploying a Bastion host, record Bastion node public IP, and Essbase node private IP. Otherwise record Essbase node public IP.	
Essbase URL for Essbase web interface and confidential application use	-	Essbase URL	
[Optional] **Enable Monitoring service** (Added for version 19.3.0.3.4)	Monitor Operations and Resources Using Oracle Cloud Infrastructure Monitoring Service		

Table 2-1 (Cont.) Pre-deployment metadata

Prerequisite Metadata	Links to overviews and tasks / examples	Record values needed for deployment	Verify completion
[Optional] **Enable and set up Notifications service** (Added for version 19.3.0.3.4)	Get Event Notifications Using Oracle Cloud Infrastructure Notifications Service	Notifications topic OCID	

Table 2-2 Pre-deployment tasks to be completed

Prerequisite Tasks	Links to overviews and tasks / examples	Record values needed for deployment	Verify completion
1. Select one of these database options: • Oracle Autonomous Database deployed by Oracle • Existing Oracle Autonomous Database (shared (ADB-S) or dedicated (ADB-D)) that you deployed from Oracle Cloud Infrastructure Console • Existing Database System that you deployed from Oracle Cloud Infrastructure	• Creating an Autonomous Database • Creating a Database System – How to Use Network Components – Set Up Rules for Database Connectivity	• For Oracle-created database: admin name and password • For existing Autonomous database: admin name and password, and compartment • For existing Database System: admin name and password, database name and home, and compartment	
2. As shown in the table above, if you haven't already done so, use Oracle Cloud Infrastructure Vault provisioning encryption for: • Essbase administrator password • Database system administrator password • Identity Cloud Service application client secret	Create Vault and Encrypt Values	(Note: Prior to version 19.3.0.3.4, these values were: KMS key OCID and KMS service endpoint) Vault encryption key OCID Vault crypto endpoint	

Table 2-2 (Cont.) Pre-deployment tasks to be completed

Prerequisite Tasks	Links to overviews and tasks / examples	Record values needed for deployment	Verify completion
4. **Log in to OCI tenancy as Administrator** - In OCI console, log in to your tenancy as the admin subscribed to that tenancy. [Optional]: Create OCI admin user - Add user to admin group (Identity>Groups>Administrator>Create User), close browser, change password using email you receive, and log in as new admin.	Administrator Access Requirements	-	
3. **Create an SSH key pair** - In Oracle Cloud Infrastructure (OCI) console, create SSH public key and corresponding private key to access Essbase compute instances.	Creating a Key Pair	SSH public key Path to private key	
5. **Create compartment(s)** - In OCI console, choose or create a compartment (Identity>Compartments>Create Compartment) where you want to deploy Essbase.	Choosing a Compartment	Compartment ID (OCID) and name	
6. **Create dynamic group** - In OCI console, create a dynamic group to allow resources to allow OCI resources to be created and networked together dynamically without explicit approvals. You can associate groups with policies.	Create Dynamic Groups	Dynamic group name	

Table 2-2 (Cont.) Pre-deployment tasks to be completed

Prerequisite Tasks	Links to overviews and tasks / examples	Record values needed for deployment	Verify completion
7. **Set up policies** - In OCI console, set up policies to enable you to manage or create resources in OCI.	Set Up Policies See also Common Policies and How Policies Work.	Policy statements (enter in text worklist doc for entry convenience)	
8. **Set up Essbase access** - In Oracle Identity Cloud Service (IDCS), set up Essbase access.	Set Up Essbase Access in Identity Cloud Service	-	
9. **Set up confidential application to register Essbase** - In Oracle Identity Cloud Service, for each compartment in which you plan to deploy Essbase, create a confidential Oracle Identity Cloud Service application, and activate the confidential application.	Create a Confidential Identity Cloud Service Application	Confidential application name IDCS Instance GUID IDCS Application Client ID IDCS Application Client Secret	

Storing Recorded Metadata for Deployment

Copy and paste the following to a text file, for your convenience, and enter the relevant values, to be used during deployment. If you fail to record any needed deployment metadata, an Oracle Cloud Infrastructure administrator can collect them from the Variables page or Application Information page of the Oracle Resource Manager. Make sure to protect and dispose of the metadata text file appropriately. (Note changes listed above for Vault metadata names before version 19.3.0.3.4.)

```
Region:
Target availability domain:
Oracle Cloud Infrastructure administrator user:
OCI administrator group name:
IDCS system administrator:
DB system admin password:
Vault encryption key OCID:
Vault crypto endpoint:
Existing virtual cloud network name (optional):
Compute node shape:
Essbase node OCID (OCI ID of the compute node):
Bastion host instance OCID (OCID ID of bastion compute node if created):
Load balancer shape and subnets (optional):
SSH-2 RMA key pair, stored locally:
Path to private key:
```

```
Compartment ID:
Compartment name:
Dynamic group name:
Policy statements:
Confidential application details
 Name:
 IDCS instance GUID (IDCS host):
 IDCS application client ID:
 IDCS application client secret:
IDCS Essbase admin user and password (Initial Essbase admin):
Essbase admin user (also known as WebLogic user--defined during stack
creation):
SSH access details:
  Bastion node public IP (optional):
  Essbase node private IP (when creating private subnet):
  Essbase node public IP (when not creating private subnet):
  Essbase URL (for web interface):
  Essbase IP (for confidential application):
Notification topic OCID (optional):
```

Create Dynamic Groups

You create dynamic groups of Oracle Cloud Infrastructure compute instances, and associate them with policies. You must provide a unique, unchangeable name for the dynamic group. Oracle assigns a unique Oracle Cloud ID (OCID).

1. On the Oracle Cloud Infrastructure console, navigate to the left icon under the Governance and Administration section, click **Identity**, and then click **Dynamic Groups**.
2. Click **Create Dynamic Group**.
3. Enter a name for the dynamic group. Record the name for future use.
4. Enter a description (optional).
5. In the **Matching Rules** section, click **Launch Rule Builder** to define the rule.
6. In **Add instances that match the following rules. Rules to consider for match**, select the option **Any of the following rules**, allows the dynamic group broad access if you have multiple rules. The other option, **All of the following rules**, enables the dynamic group to service specific compartment/instance combinations when multiple rules are specified.
7. In the Create Matching Rule dialog, select a resource. In **ATTRIBUTE** field, select the option **Match Instances in Compartment ID**. For the **VALUE** field, paste the compartment ID you noted for the compartment in which you're creating the Essbase stack. With this option, any instances in the compartment will work using this dynanic group. The other option, **Match instances with ID**, specifies matching just one instance ID.
8. Click **Add Rule**.
9. You can enter tags (optional) to organize and track resources in your tenancy.
10. Click **Create Dynamic Group**.

For more information on dynamic groups, see Managing Dynamic Groups.

Set Up Policies

A policy is a document that specifies who can access which Oracle Cloud Infrastructure resources that your company has, and how.

Before deploying the Essbase stack on a compartment in Oracle Cloud Infrastructure, the tenant administrator must set up policies to access or create the following resources in the selected compartment:

- Marketplace applications
- Resource Manager stacks and jobs
- Compute instances, networks, and load balancers
- Database for storing Essbase metadata
- Managing and using virtual keys for Oracle Cloud Infrastructure Vault

To create policies:

1. On the Oracle Cloud Infrastructure console, navigate to the left icon under the Governance and Administration section, click **Identity**, select **Policies**, select the root compartment, and then click **Create Policy**.
2. Provide a name and description for the policy.
3. Add a policy statement (Allow) for each instance in the compartment. Copy them from your text worklist file. Specify the group_name in the policy statement.
4. When done, click **Create**.

Create a policy each, for both groups and dynamic groups, as necessary.

Set up policies that are appropriate for your organization's security setup. The following is an example of a policy template, with each row being a policy statement.

```
Allow group group_name to manage orm-stacks in compartment
compartment_name
Allow group group_name to manage orm-jobs in compartment
compartment_name
Allow group group_name to manage virtual-network-family in compartment
compartment_name
Allow group group_name to manage instances in compartment
compartment_name
Allow group group_name to manage volume-family in compartment
compartment_name
Allow group group_name to manage load-balancers in compartment
compartment_name
Allow group group_name to manage buckets in compartment compartment_name
Allow group group_name to manage objects in compartment compartment_name
Allow group group_name to manage autonomous-database-family in
compartment compartment_name
Allow group group_name to use instance-family in compartment
compartment_name
Allow group group_name to manage autonomous-backups in compartment
compartment_name
Allow group group_name to manage buckets in compartment compartment_name
Allow group group_name to manage vaults in compartment compartment_name
```

```
Allow group group_name to manage keys in compartment compartment_name
Allow group group_name to manage app-catalog-listing in compartment
compartment_name
```

Some policies may be optional, depending on expected use. For example, if you're not using a load balancer, you don't need a policy that allows management of load balancers.

To allow instances within the compartment to invoke functionality without requiring further authentication, you must have group policies for the instances in the compartment. To do this, create a dynamic group, and set the policies for that dynamic group, such as shown in the following example:

```
Allow dynamic-group group_name to use autonomous-database in
compartment compartment_name
Allow dynamic-group group_name to use keys in compartment
compartment_name
Allow dynamic-group group_name to read buckets in compartment
compartment_name
Allow dynamic-group group_name to manage objects in compartment
compartment_name
Allow dynamic-group group_name to inspect volume-groups in compartment
compartment_name
Allow dynamic-group group_name to manage volumes in compartment
compartment_name
Allow dynamic-group group_name to manage volume-group-backups in
compartment compartment_name
Allow dynamic-group group_name to manage volume-backups in compartment
compartment_name
Allow dynamic-group group_name to manage autonomous-backups in
compartment compartment_name
Allow dynamic-group group_name to manage database-family in compartment
compartment_name
```

The following policies are optional, but necessary for the following integrations:

> **Note:**
>
> Added for version 19.3.0.3.4.

- Oracle Notification Service integration:

  ```
  allow dynamic-group group_name to use ons-topic in compartment dev
  where request.permission='ONS_TOPIC_PUBLISH'
  ```

- Oracle Cloud Infrastructure Monitoring integration:

  ```
  allow dynamic-group group_name to use metrics in compartment dev
  where target.metrics.namespace='oracle_essbase'
  ```

Set Up Essbase Access in Identity Cloud Service

To set up security and access, you integrate Essbase with Oracle Identity Cloud Service. You provision Essbase users using Essbase roles, rather than Oracle Identity Cloud Service roles.

To prepare security access for Essbase, you must log in to Oracle Identity Cloud Service as the identity domain administrator and complete a few tasks.

Before you can provision users and groups in Essbase, you need, during creation of the Essbase stack, to provide the name of a user in Oracle Identity Cloud Service who will be the initial Service Administrator for Essbase.

This Service Administrator can then log in to the Essbase web interface to provision other users.

You also need to provide access to the signing certificate.

Complete the following tasks in Identity Cloud Service before deploying the Essbase stack.

1. Log in to Identity Cloud Service as the identity domain administrator. To get to the Identity Cloud Service console from Oracle Cloud Infrastructure, click **Identity**, then **Federation**, and click on the URL link next to Oracle Identity Cloud Service Console.
2. In the Identity Cloud Service console, expand the navigation drawer icon, click **Settings**, and then click **Default Settings**.
3. Turn on the switch under **Access Signing Certificate** to enable clients to access the tenant signing certificate without logging in to Identity Cloud Service.
4. Scrill up and click **Save** to store your changes.
5. If not already created, create a user in Identity Cloud Service who will be the initial Essbase Service Administrator.

About Single Sign-On (SSO)

If you use single sign-on (SSO) with Identity Cloud Service, your Essbase login screen routes to Identity Cloud Service.

If you use SSO that is external to Identity Cloud Service, you configure Identity Cloud Service to point to the external security provider. The Essbase login screen routes to Identity Cloud Service, which routes to the external login screen. After logging in, you're directed back to the Essbase web interface.

Create a Confidential Identity Cloud Service Application

Before deploying the Essbase stack, create a confidential application in Oracle Identity Cloud Service and register Essbase with it.

1. Open the Oracle Identity Cloud Service Console. From Oracle Cloud Infrastructure, select **Identity, Federation, Identity Provider Details**. In the Identity Provider Information tab, click the **Oracle Identity Cloud Service Console** link.
2. In the Identity Cloud Service console, expand the Navigation Drawer icon, and then select **Applications**.

3. Select **+Add**.
4. Select **Confidential Application,** as described in Add a Confidential Application.
5. In the **App Details** step, enter a name only, and then select **Next**. Tip: you may use the same name as the compartment, as you need one confidential application per compartment. Record the name for your information.
6. In the **Client** step, select the option **Configure this application as a client now**.
7. In the **Authorization** section,
   - Select the following allowed grant types: **Client Credentials** and **Authorization Code**.
   - If you don't plan to provision a load balancer, select **Allow non-HTTPS URLs**.
     a. For the **Essbase Redirect URL**, enter a temporary/mock redirection URL (it ends with _uri):

        ```
        http://temp/essbase/redirect_uri
        ```

     b. For the **Essbase Post Logout Redirect URL**, enter a temporary/mock URL:

        ```
        http://temp/essbase/jet/logout.html
        ```

   - Otherwise, if you're provisioning a load balancer, enter the following: above URL, but using **https:**, as shown.
     a. For the **Essbase Redirect URL**, enter a temporary/mock redirection URL:

        ```
        https://temp/essbase/redirect_uri
        ```

     b. For the **Essbase Post Logout Redirect URL**, enter a temporary/mock URL:

        ```
        https://temp/essbase/jet/logout.html
        ```

8. Under **Token Issuance Policy**, in the section **Grant the client access to Identity Cloud Service Admin APIs**, click **Add**, find and select the **Identity Domain Administrator** role, and select **Add**.
9. Scroll to the top of the page and click **Next** until you reach the Authorization section.
10. Click **Finish**.
11. From the Application Added popup window, record the following Identity Cloud Service details: IDCS Application Client ID and IDCS Application Client Secret. Record these values to use during your Essbase deployment.
12. Record the IDCS Instance GUID from the following location: in the Identity Cloud Service Console, select your ID icon in the top right corner (the icon contains your initials), select **About**, and record the **IDCS Instance GUID** value. If you don't have access, ask your administrator to provide it. Example: `idcs-123456789a123b123c12345678d123e1`. Alternatively, the **IDCS Instance GUID** is at the front of the IDCS url in the browser - take the host portion of the url.
13. Select **Activate** in the title bar, next to your application's name.

Oracle Cloud Services accounts provides Oracle Identity Foundation, which enables basic identity services functionality. This includes user management, group management, basic reporting, and authentication for Oracle applications. See: Oracle PaaS and IaaS Universal Credits Service Descriptions. For information regarding features available in various Oracle Identity Cloud Service versions, see: About Oracle Identity Cloud Service Pricing Models.

Supported Compute Shapes

Oracle Essbase offers compute sizes (OCPUs) to suit different scenarios. The larger the compute size, the greater the processing power. If you're not sure which size to use, contact your sales team to discuss sizing guidelines.

Essbase can be Oracle Compute Unit (OCPU)-intensive depending on your application. The minimum number of OCPUs recommended for production deployments is 4 OCPUs. To help you decide which compute size best suits your deployment, consider how many active users you expect to perform concurrent activities such as:

- Users running queries in hybrid mode
- Users running calculations in block storage mode
- Users running reports or queries in aggregate storage cubes

You can configure storage size when you deploy Essbase. Determine the storage size needed, or consult with your sales team to determine that your storage needs are met, based on the number of applications that you plan to deploy.

Essbase currently supports the following shapes:

- VM.Standard.2.*
- VM.Standard.E2.*
- BM.Standard.2.52
- BM.Standard.E2.64
- BM.Standard.E3.128

For a description of the difference between VM and BM shapes, and a discussion on how to decide which to use, see https://cloud.oracle.com/compute/faq.

Create Vault and Encrypt Values

Oracle Cloud Infrastructure Vault enables you to manage sensitive information when creating a server domain.

> **Note:**
>
> Prior to version 19.3.0.3.4, Vault encryption was known as Key Management, and Vault metadata was named KMS.

When you use Vault to encrypt credentials during provisioning, you need to create a key. Passwords chosen for Essbase administrator and Database must meet the Resource Manager password requirements.

Keys need to be encrypted for the following fields:

- Essbase Administrator Password
- IDCS application client secret
- Database system administrator password

To create a vault and a key:

> **Note:**
>
> Creating a vault and key is required. These steps explain how to create a Virtual Vault, which is a lower-cost option than virtual private vaults.

1. Sign in to the Oracle Cloud Infrastructure console.
2. In the navigation menu, select **Security**, and click **Vault**.
3. Select your **Compartment**, if not already selected.
4. Click **Create Vault**.
5. For **Name**, enter `OracleEssbaseVault`.
6. For the lower-cost option, leave unchecked option to make it a virtual private vault.
7. Click **Create**.
8. Click the new vault and record the **Vault Crypto Endpoint** for later use.
9. Go back to vaults page and then click **Create Key**.
10. For **Name**, enter `OracleEssbaseKey` and create a key.
11. Click the new key and record the **OCID** value for the key, for later use.
    Note that Essbase uses the same key to decrypt all passwords for a single domain.

To encrypt your Oracle Essbase Administrator password:

1. Convert the administrator password that you want to use for the Essbase domain to a base64 encoding.
   For example, from a Linux terminal, use this command:

   ```
   echo -n 'OracleEssbase_Password' | base64
   ```

2. Run the `encrypt oci` command using Oracle Cloud Infrastructure command line interface. Provide the following parameters:
   - Vault Encryption Key OCID
   - Vault Crypto Endpoint
   - base64-encoded password

   ```
   oci kms crypto encrypt --key-id Key_OCID --endpoint
   Cryptographic_Endpoint_URL --plaintext Base64_OracleEssbase_Password
   ```

3. From the output, copy the encrypted password value for use in the deploy process, as shown here:

   ```
   "ciphertext": "Encrypted_Password"
   ```

You also use vault encryption to encrypt your Database Password and your Client Secret.

Access the WebLogic Console

As an Essbase administrator, when you are managing your Oracle Essbase stack on Oracle Cloud Infrastructure, you may need access to the WebLogic console to perform some administrative tasks.

The Essbase stack on Oracle Cloud Infrastructure runs from a managed WebLogic server. When you start or stop the Essbase stack, it starts and stops the WebLogic server as well as the Essbase applications.

Caution: Essbase instances are configured by default with no access to the administrative T3 WebLogic port. Oracle highly recommends that all access to the T3 port remain disabled, and that you secure it immediately. If necessary for business purposes, access to the T3 port should only be allowed from a certain fixed set of IPs, using SecIPList or a restricted classless inter-domain routing block (CIDR); for example, xx.xx.0.0/16.

The WebLogic AdminServer runs on port 7002. To access it,

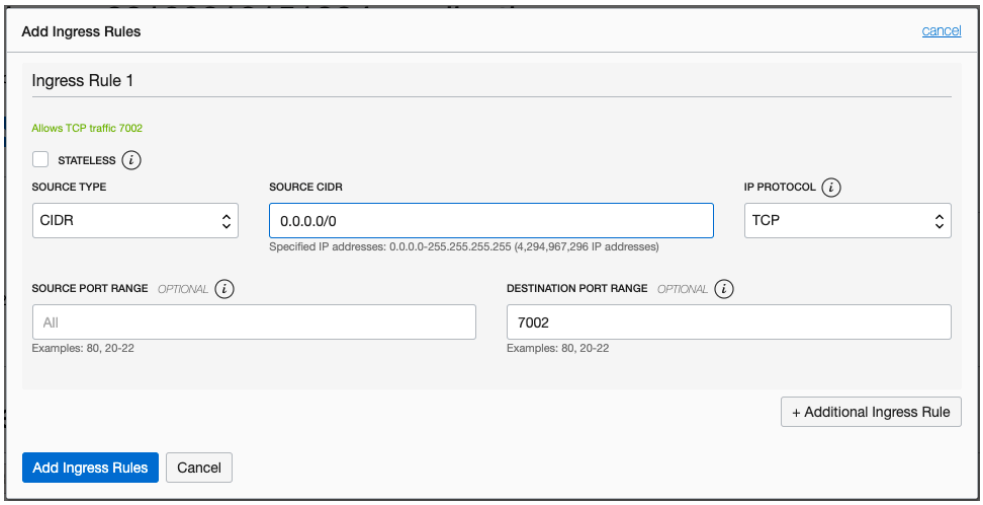
1. Expose the port on the target compute node. To do this, SSH into the target machine as the opc user and run the following commands:

   ```
   [opc@essbase-1 ~]$ sudo firewall-cmd --add-port=7002/tcp --
   zone=public

   # To make this survive restarts of the firewall service
   [opc@essbase-1 ~]$ sudo firewall-cmd --add-port=7002/tcp --
   zone=public --permanent
   [opc@essbase-1 ~]$ sudo systemctl restart firewalld
   [opc@essbase-1 ~]$ sudo firewall-cmd --list-all
   public
     target: default
     icmp-block-inversion: no
     interfaces:
     sources:
     services: sshdhcpv6-client http https
     ports: 7002/tcp
     protocols:
     masquerade: no
     forward-ports:
     source-ports:
     icmp-blocks:
     rich rules:
   ```

2. Enable the security list for the subnet to allow access to the port from a source network. This example enables access from the entire Internet. The quick start

creates a virtual cloud network (VCN) named `<prefix>-vcn`, and a security list named `<prefix>-app-security-list`. Add an ingress rule as follows:



3. Log in to the target machine using the Console URL `https://<Essbase IP address>:7002/console`, with the same Essbase administrator login that you used during configuration of the stack.

Administrator Access Requirements

Learn about different kinds of administrative access requirements for setting up Oracle Essbase on Oracle Cloud Infrastructure.

Administrator Type	Description
Oracle Cloud Infrastructure administrator	The administrator who is subscribed to the Oracle Cloud Infrastructure tenancy. This administrator sets up policies for access to resources in the compartment, and also designates the other administrators (listed below) during stack deployment.
IDCS system administrator	The Oracle Identity Cloud Service identity domain administrator. This administrator is responsible for setting up Essbase access in Identity Cloud Service, including creating and modifying a confidential IDCS application.
IDCS Essbase admin user	An Identity Cloud Service user selected to act as the initial Service Administrator for Essbase. During provisioning and deployment of the stack, the Oracle Cloud Infrastructure administrator provides the ID of this user. This user can log in to Essbase and provision other users.
Essbase admin user	This user is specified by the Oracle Cloud Infrastructure administrator during provisioning and deployment of the stack. This is a native Essbase administrator used during deployment. This user ID provides an alternate way to log in to Essbase for administration of the Essbase environment/deployment.

Deploy Oracle Essbase

To deploy Oracle Essbase on Oracle Cloud Infrastructure using Marketplace, by following the deployment procedure below for the appropriate version of your patch listing update.

- Deploy for Version 19.3.0.2.3
- Deploy for Version 19.3.0.3.4

Deploy for Version 19.3.0.2.3

Deploy Oracle Essbase from Oracle Cloud Marketplace for patch listing version 19.3.0.2.3.

As the Oracle Cloud Infrastructure administrator, you use Oracle Cloud Infrastructure to set up Essbase. Oracle Cloud Marketplace uses Oracle Resource Manager to provision the network, compute instances, Autonomous Transaction Processing database for storing Essbase metadata, and Load Balancer.

During this process, you will need to provide other administrator user IDs. Review Administrator Access Requirements to understand what these administrator accounts can do.

1. Read prerequisites and requirements that you need to know or to do before deployment. See Before You Begin with Oracle Essbase.
2. Sign into Oracle Cloud Infrastructure console as the Oracle Cloud Infrastructure administrator.
3. From the navigation menu, select **Marketplace**.
4. On Oracle Marketplace page,
    a. In the title bar, select or accept the region from which to run the deployment.
    b. In the Category dropdown menu, select **Database Management**.
    c. Under All Applications, select Oracle Essbase.
    d. Select the stack version, or accept the default.
    e. From the dropdown menu, select the target **Compartment** that you created for Essbase, in which to create the stack instance.
    f. Select the check box to indicate you accept the Oracle Standard Terms and Restrictions.
    g. Click **Launch Stack**.
5. In **Stack Information**, on the Create Stack page.
    a. Enter a stack name, description, and any other stack information as necessary.
    b. Click **Next**.
6. In **General Settings**, on the Configure Variables page, you configure variables for the infrastructure resources that the stack creates.

a. [Optional] Enter **Resource Display Name Prefix** value to use to identify all generated resources, for example `essbase_<userid>`. If not entered, a prefix is assigned.

   The target compartment you previously selected is shown.

b. Enter values for **KMS Key OCID** and **KMS Service Crypto Endpoint** for encrypting credentials during provisioning.

c. [Optional] Select **Show Advanced Options** if you want to enable additional network configuration options under **Network Configuration**. Use this if you plan to create a new virtual cloud network (VCN) or subnets.

7. In **Essbase Instance**:

   a. Select an availability domain in which to create the Essbase compute instance. Enter the shape for the Essbase compute instance.

   b. Enter the data volume size or accept the default.

   c. Paste the value of the SSH public key that you created, to access the Essbase compute instance.

   d. In the **Essbase System Admin User Name** field, enter an Essbase administrator user name and password. It can be an Identity Cloud Service user, but it doesn't have to be. It provides an additional way (if necessary) to log in to Essbase, and is also the administrator used to Access the WebLogic Console on which Essbase runs. If you don't enter an Identity Cloud Service user in this field, then you must provide one in the **IDCS Essbase Admin User** field later in the stack definition, in the **Security Configuration** section. If you enter an Identity Cloud Service user in this field, then the Identity Cloud Service System Administrator User ID is optional in the **Security Configuration** section.

8. In **Security Configuration**:

   a. Select **IDCS** for use with your production instances. To set up security and access, you integrate Essbase with Identity Cloud Service as part of the stack deployment. The WebLogic Embedded LDAP option isn't recommended or supported for production instances.

   b. Enter the **IDCS Instance GUID**, **IDCS Application Client ID**, and **IDCS Application Client Secret** values, which you recorded as pre-deployment requirements, after you created a confidential Identity Cloud Service Application.

   c. Enter **IDCS Essbase Admin User** value. This can't be the same user ID as the Essbase administrator. Additionally, this user ID must already exist in the Identity Cloud Service tenancy. If you don't provide this user ID during stack creation, or if its mapping to the initial Essbase administrator doesn't happen correctly, you can later use the Identity Cloud Service REST API to create this user and link it to Essbase. See REST API for Oracle Identity Cloud Service.

9. In **Network Configuration**, if you did *NOT* select to show advanced options under **General Settings**:

   a. [Optional] Select a virtual cloud network strategy: If you choose **Use Existing Network**, select the name of the existing virtual cloud network (you can still create a new instance of the Autonomous Transaction Processing database).

   b. [Optional] Select the target network compartment, virtual network, and application subnet.

c. [Optional] Select a subnet strategy: use an existing public subnet or select **Create a Private Essbase Subnet** for the Essbase node and then select a bastion instance shape for the bastion compute instance for the created hosted.

d. [Optional] Unselect **Assign Public Key IP Address** if the subnet doesn't allow for a public IP address.

e. Leave **Assign Public IP Address** selected.

f. [Optional] Provision a load balancer if you want to add an extra layer of security. In Oracle Cloud Infrastructure, select **Provision Load Balancer**, and specify the load balancer shape and subnets.

10. In **Network Configuration**, if you DID select **Show Advanced Options** under **General Settings**:

    a. Select a virtual cloud network strategy: If you choose **Use Existing Network**, select the name of the existing virtual cloud network (you can still create a new instance of the Autonomous Transaction Processing database). If you want to create a new virtual cloud network, enter a **Virtual Network CIDR** value to assign the VCN. See Overview of Networking.

    b. Select the target network compartment, virtual network, and application subnet.

    c. If you want to create a private Essbase subnet, enter an **Application Network CIDR** to assign to the subnet for the target Essbase compute node.

    d. Select a subnet strategy: use an existing public subnet or select **Create a Private Essbase Subnet** for the Essbase node and then create the bastion subnet and select its shape.

    e. [Optional] Unselect **Assign Public Key IP Address** if the subnet does not allow for a public IP address.

    f. If you are creating a private Essbase subnet, enter a **Bastion Subnet CIDR** to assign to the subnet for the bastion host.

    g. [Optional] Provision a load balancer if you want to add an extra layer of security. In Oracle Cloud Infrastructure, select **Provision Load Balancer**, and specify the load balancer shape and subnets.

11. In **Database Configuration**, select from the following options and then perform the configuration tasks:

    Database options:

    - If you plan to use the Oracle Autonomous Database deployed automatically by the stack, you must provide the password that you encrypted using KMS.
    - If you plan to use an existing Oracle Autonomous database, select **Use Existing Database**, specify the compartment (in which Autonomous Transaction Processing was created), and provide the Autonomous Database password used when you created the service, which you encrypted using KMS.
    - To use an existing Oracle Cloud Infrastructure Database System for the internal Essbase repository, select the option **Database System** for Database Type, and specify the compartment and database details. The database must be accessible to the created compute node. If the database has a private IP, use the existing network option where the network is set up, to allow for traffic

between the subnet that hosts the compute node and the subnet that hosts the database. See Bare Metal and Virtual Machine Database Systems.

Database configuration tasks:

a. Enter a database admin user password.

b. Select the database license or accept the default.

c. Click **Next**.

12. On the Review page, review the information that you provided, and click **Create**. The Job Information tab in Oracle Resource Manager shows the status until the job finishes and the stack is created.
13. Check for any log errors. If you have any, see Troubleshoot Deployment Errors.
14. From the Review page, the value for **essbase_url** is used in the browser to access Essbase. The **essbase_node_public_ip** is for accessing SSH.
15. After you deploy the stack, now complete the post-deployment tasks, including update your created Identity Cloud Service application, test connectivity to Essbase, and others.

You can modify the created resources and configure variables later. Logs are created that can be forwarded to Oracle Support, if necessary for troubleshooting. After deployment, you're ready to assign users to roles and permissions in the Essbase web interface. You can also perform additional network and security configuration.

Reviewing or Collecting Output After Deployment

If you didn't keep a record of all of the deployment output, an Oracle Cloud Infrastructure administrator can collect them from the Variables page or the Application Information of the Oracle Resource Manager, as well as the client configuration details of the Identity Cloud Service confidential application.

- **Viewing the Deployment**
  Log into Oracle Cloud Infrastructure console, go to Resource Manager for your compartment, and view the details for the Essbase stack you created. From there, if you click on the apply job, you can see the deployment log and output details. If you deployed a bastion host, the outputs include a **bastion_host_public_ip**, and there is no **essbase_node_public_ip**. If you selected to use a load balancer, its public IP is in the **essbase_url**.
- **Viewing the Variables**
  In addition to using the log to find and record deployment details, you can also view most of them in the Variables page or the Application Information page of the Resource Manager. For example, if you deployed a bastion host, then **create_private_subnet** is `true`. If you selected to use a load balancer, **create_load_balancer** is `true`.
- **Viewing the Confidential Application Configuration**
  To locate the client secret, which is masked in Resource Manager, an Identity Cloud Service Administrator can go to the Identity Cloud Service Console, select the confidential application, and view its configuration.

Deploy for Version 19.3.0.3.4

Deploy Oracle Essbase from Oracle Cloud Marketplace.

As the Oracle Cloud Infrastructure administrator, you use Oracle Cloud Infrastructure to set up Essbase. Oracle Cloud Marketplace uses Oracle Resource Manager to provision the network, compute instances, Autonomous Transaction Processing database for storing Essbase metadata, and Load Balancer.

During this process, you'll need to provide other administrator user IDs. Review Administrator Access Requirements to understand what these administrator accounts can do.

1. Read prerequisites and requirements that you need to know or do before deployment. See Before You Begin with Oracle Essbase.
2. Sign into Oracle Cloud Infrastructure console as the Oracle Cloud Infrastructure administrator.
3. From the navigation menu, select **Marketplace**.
4. On Oracle Marketplace page,
   a. In the title bar, select or accept the region from which to run the deployment.
   b. In the Category dropdown menu, select **Database Management**.
   c. Under All Applications, select Oracle Essbase.
   d. Select the stack version, or accept the default.
   e. From the dropdown menu, select the target **Compartment** that you created for Essbase, in which to create the stack instance.
   f. Select the check box to indicate you accept the Oracle Standard Terms and Restrictions.
   g. Click **Launch Stack**.
5. In **Stack Information**, on the Create Stack page.
   a. Enter a stack name, description, and any other stack information as necessary.
   b. Click **Next**.
6. In **General Settings**, on the Configure Variables page, you configure variables for the infrastructure resources that the stack creates.
   a. [Optional] Enter **Stack Display Name** value to identify your stack deployment for all generated resources, for example `essbase_<userid>`. Provide a meaningful stack display name. This name is used as a dimension for filtering Essbase metrics that correspond to components in this stack. If not entered, the display name is generated.

      The target compartment you previously selected is shown.
   b. Enter values for **Vault Encryption Key OCID** and **Vault Crypto Endpoint** for encrypting credentials during provisioning.
   c. [Optional] Enter **Notification Topic OCID**, to which messages are published.
7. In **Essbase Instance**:
   a. Select an **Essbase Availability Domain** in which to create the Essbase compute instance.

b. Select the **Essbase Instance Shape** for the Essbase compute instance.

c. Enter the **Data Volume Size** or accept the default. The minimum value is 256GB.

d. Paste the value of the **SSH Public Key** that you created, to access the Essbase compute instance.

e. In the **Essbase System Admin User Name** field, enter an Essbase administrator user name and password - you can optionally use the Identity Cloud Service user name. It provides an additional way to log in to Essbase, and is also the administrator used to Access the WebLogic Console on which Essbase runs. If you don't enter an Identity Cloud Service user in this field, you must provide one in the **IDCS Essbase Admin User** field later in the stack definition, in the **Security Configuration** section. If you enter an Identity Cloud Service user in this field, the Identity Cloud Service System Administrator User ID is optional in the **Security Configuration** section.

f. [Optional] Select **Enable Monitoring** to support publishing of metrics to the Oracle Cloud Infrastructure Monitoring Service.

8. In **Security Configuration**:

   a. Select **IDCS** for use with your production instances. To set up security and access, you integrate Essbase with Identity Cloud Service as part of the stack deployment. The WebLogic Embedded LDAP option isn't recommended or supported for production instances.

   b. Enter the **IDCS Instance GUID**, **IDCS Application Client ID**, and **IDCS Application Client Secret** values, which you recorded as pre-deployment requirements, after you created a confidential Identity Cloud Service Application.

   c. Enter **IDCS Essbase Admin User** value. This can't be the same user ID as the Essbase administrator. Additionally, this ID must already exist in the Identity Cloud Service tenancy. If you don't provide this user ID during stack creation, or if it's mapping to the initial Essbase administrator doesn't done correctly, you can later use the Identity Cloud Service REST API to create this user and link it to Essbase. See REST API for Oracle Identity Cloud Service.

9. In **Database Configuration**, select from the following options and then perform the configuration tasks:

   Database options:

   - If you plan to use the Oracle Autonomous Database deployed automatically by the stack, you must provide the password that you encrypted using Vault.
   - If you plan to use an existing Oracle Autonomous database, select **Use Existing Database**, enter the Autonomous Database password used when you created the service, which you encrypted using Vault. Specify the compartment in which Autonomous Transaction Processing was created.
   - To use an existing Oracle Cloud Infrastructure Database System for the internal Essbase repository, select the option **Database System** for Database Type, and specify the compartment and database details. The database must be accessible to the created compute node. If the database has a private IP, use the existing network option where the network is set up, to allow for traffic between the subnet that hosts the compute node and the subnet that hosts the database. See Bare Metal and Virtual Machine Database Systems.

   Database configuration tasks:

a. Enter a database administrator user password. This is the Vault encrypted password.

b. Select the database license or accept the default.

c. Click **Next**.

10. In **Network Configuration**:

    a. If you chose **Use Existing Network**, select the name of the existing virtual cloud network. You can still create a new instance of the Autonomous Transaction Processing database.

    b. If you want to create a new virtual cloud network, enter a **Virtual Network CIDR** value to assign the VCN. See Overview of Networking.

    c. Select the target network compartment, virtual network, and application subnet.

    d. If you want to create a private Essbase subnet, enter an **Application Network CIDR** to assign to the subnet for the target Essbase compute node.

    e. Select a subnet strategy: use an existing public subnet or select **Create a Private Essbase Subnet** for the Essbase node, and then create the bastion subnet and select its shape.

    f. [Optional] Select **Public Essbase Node Visibility** to enable a public IP address for the Essbase instance. If selected, the subnet provided must allow for public IP address.

11. In **Load Balancer Configuration**:

    a. Select **Provision Load Balancer** to provision it in Oracle Cloud Infrastructure with a demo certificate. This is not recommended for production workloads.

    b. Select **Public Load Balancer Visibility** to enable a public IP address for the Load Balancer, and to add an extra layer of security. Select a load balancer shape.

12. In **Bastion Configuration** (shown if Public Essbase Node Visibility is not set):

    a. Select **Provision Bastion** to enable the creation of a bastion host.

    b. Select a **Bastion Availability Domain** to provide the target availability domain of the bastion host.

    c. Select a **Bastion Instance Shape**. You must have the capacity of the target shape in the given availability domain for the bastion compute instance to be created successfully. Your bastion shape value doesn't need to match the compute node shape.

13. On the Review page, review the information that you provided, and click **Create**. The Job Information tab in Oracle Resource Manager shows the status until the job finishes and the stack is created.

14. Check for any log errors. If necessary, see Troubleshoot Deployment Errors.

15. On the Review page, the value for **essbase_url** is used in the browser to access Essbase. The **essbase_node_public_ip** is for accessing SSH.

16. After you complete deployment, then complete the post-deployment tasks, including: modifying your created Identity Cloud Service application, testing connectivity to Essbase, and the other listed tasks.

You can modify the created resources and configure variables later. Logs are created that can be forwarded to Oracle Support, if necessary for troubleshooting. After

deployment, you're ready to assign users to roles and permissions in the Essbase web interface. You can also perform additional network and security configuration.

Reviewing or Collecting Output After Deployment

If you didn't keep a record of all of the deployment output, an Oracle Cloud Infrastructure administrator can collect them from the Variables page or Application Information of the Oracle Resource Manager, as well as in the client configuration details of the Identity Cloud Service confidential application.

- **Viewing the Deployment**
  Log into Oracle Cloud Infrastructure console, go to Resource Manager for your compartment, and view the details for the Essbase stack you created. From there, if you click on the apply job, you can see the deployment log and output details. If you deployed a bastion host, the outputs include a **bastion_host_public_ip** and there isn't an **essbase_node_public_ip**. If you selected to use a load balancer, its public IP is in the **essbase_url**.
- **Viewing the Variables**
  In addition to using the log to find and record deployment details, you can also view most of them in the Variables page or the Application Information page of the Resource Manager. For example, if you deployed a bastion host, then **create_private_subnet** is `true`. If you selected to use a load balancer, **create_load_balancer** is `true`.
- **Viewing the Confidential Application Configuration**
  To locate the client secret, which is masked in Resource Manager, an Identity Cloud Service Administrator can go to the Identity Cloud Service Console, select the confidential application, and view its configuration.

Complete Post-Deployment Tasks

After you deploy Oracle Essbase on Oracle Cloud Infrastructure using Marketplace, complete the following tasks.

- Modify the Confidential Identity Cloud Service Application
- Set Up the SSL Certificate
- Secure Your Network
- Migrate Users and Groups from Oracle Analytics Cloud
- Complete System Hardening and Cleanup Tasks
- Troubleshoot Deployment Errors

Modify the Confidential Identity Cloud Service Application

After deploying the Essbase stack from Oracle Cloud Marketplace, update your confidential Identity Cloud Service application with the correct Essbase URLs.

1. Log in to Identity Cloud Service as the identity domain administrator. To get to the Identity Cloud Service console from Oracle Cloud Infrastructure, click **Identity**, then **Federation**, and click on the URL link next to Oracle Identity Cloud Service Console.
2. In the Identity Cloud Service console, expand the Navigation Drawer icon, and then click **Applications**.

3. Locate and select your confidential application.
4. Select **Configuration** and expand **Client Configuration**.
5. Update the Essbase **Redirect URL** to reflect the actual Essbase URL.

   ```
   https://192.0.2.1/essbase/redirect_uri
   ```

   If you deployed a load balancer, include the port number:

   ```
   https://192.0.2.1:443/essbase/redirect_uri
   ```

   Note that if you deployed a load balancer, the IP in the Essbase URL will be for the load balancer.
6. Update the Essbase **Post Logout Redirect URL** to reflect the **essbase_url**. For example:

   ```
   https://192.0.2.1/essbase/jet/logout.html
   ```

7. Scroll up and save the updated confidential application.

Set Up the SSL Certificate

After you deploy the Essbase stack, Oracle highly recommends that you update the SSL certificate, using the Oracle Cloud Infrastructure console or APIs, to one that has been signed with a trusted certificate authority.

For information on setting up a trusted certificate authority, see Managing SSL Certificates.

If you select to provision the Oracle Cloud Infrastructure Load Balancer during the Essbase stack provisioning process, the Load Balancer is configured with a demo certificate you can use for SSL access. The demo certificate is self-signed.

When you use a self-signed certificate, including the provided demo certificate, you must perform additional configuration to enable the use of partitions, as well as Essbase C- and Java-based clients. MaxL is a C-based client. You also need to ignore hostname verification on the WebLogic part of the Essbase stack. **Caution**: use of self-signed certificates should be only temporary, until you can obtain a trusted CA certificate.

Steps for Using Partitions with Self-Signed Certificates

When you use a self-signed certificate, you must perform additional configuration and also disable peer certificate verification, to enable the use of partitions.

1. Access the Essbase node using SSH, as described in Access Oracle Essbase Using SSH.
2. Change to oracle user.

   ```
   sudo su - oracle
   ```

3. Open `essbase.cfg` for editing.

   ```
   vi /u01/config/domains/essbase_domain/config/fmwconfig/essconfig/
   essbase/essbase.cfg
   ```

4. Add the following variable to the bottom of the file.

   ```
   env:API_DISABLE_PEER_VERIFICATION 1
   ```

Steps for Using MaxL with Self-Signed Certificates

1. When you use a self-signed certificate, you must perform configurations to enable the use of MaxL.
   - Either use **MaxL** client, following the instructions in Manage Essbase Using the MaxL Client.
   - OR use **MaxL** on the server, using the startMAXLsh file at the following path on the server:

     ```
     /u01/config/domains/essbase_domain/esstools/bin
     ```

2. In order to use self-signed certificate, peer verification should be disabled, by setting the environment variable API_DISABLE_PEER_VERIFICATION=1.
   - In Linux, edit the MaxL startup script (startMAXL.sh) and add the following line:

     ```
     export API_DISABLE_PEER_VERIFICATION=1
     ```

   - In Windows, edit start maxl script (startMAXL.bat) and add the following line:

     ```
     set API_DISABLE_PEER_VERIFICATION=1
     ```

Steps for Using Java-based Clients with Self-Signed Certificates

When you use a self-signed certificate and a Java client, you must configure your Java client.

1. From an external host:
   a. When Load Balancer was configured:
      Download the certificate provided with the Oracle Cloud Infrastructure Load Balancer.

      ```
      echo -n | openssl s_client -connect <LOAD BALANCER IP>:443 | sed
      -ne  '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > /tmp/lbr.cert
      ```

   b. When Load Balancer wasn't configured:
      Download the certificate as follows.

      ```
      echo /p' > /tmp/lbr.cert
      ```

2. Import the certificate to the Java keystore. For example, if you're working from the Essbase node, and assuming you downloaded the certificate to `/tmp/lbr.cert` on the Essbase server,

a. Log in as user **opc**. Access the Essbase node using SSH.

b. Run commands to add `lbr.cert` to the keystore. For example (your path details may differ):

```
sudo /usr/java/default/bin/keytool -import -alias mysert -
file /tmp/lbr.cert -keystore /usr/java/default/jre/lib/security/
cacerts -storepass new2mepass
     Trust this certificate? [no]: yes
     Certificate was added to keystore
```

3. Restart the Java process, if the Java client is WebLogic.
4. Stop and restart the Essbase stack instance.
5. Set up WebLogic to ignore hostname verification, as described in the next section.

Steps for Configuring WebLogic for Use with Self-Signed Certificates

If you decide to use a self-signed certificate, you must set up the WebLogic component of the Essbase stack to ignore hostname verifications.

1. Access the Essbase node using SSH.
2. Change to oracle user.

```
sudo su - oracle
```

3. Open the `setDomainEnv.sh` file for editing.

```
vi /u01/config/domains/essbase_domain/bin/setDomainEnv.sh
```

4. Add the following line to the `JAVA_OPTIONS="${JAVA_OPTIONS}"` string:

```
-Dweblogic.security.SSL.ignoreHostnameVerification=true
```

When you're finished, it should look like this:

```
JAVA_OPTIONS="${JAVA_OPTIONS} -
Dweblogic.security.SSL.ignoreHostnameVerification=true"
```

5. Save the file.
6. Stop and restart the Essbase stack instance.

Secure Your Network

After you deploy the Essbase stack on Oracle Cloud Infrastructure, take steps to secure your network.

See Ways to Secure Your Network.

Migrate Users and Groups from Oracle Analytics Cloud

Before you migrate to Oracle Cloud Infrastructure, you must migrate your users and groups from Oracle Analytics Cloud.

The way you migrate depends on whether you're using Oracle Identity Cloud Service or an embedded WebLogic LDAP server. If you subscribe to Oracle Analytics Cloud through Universal Credits, you manage users in Oracle Identity Cloud Service. If you subscribe to Oracle Analytics Cloud through a traditional metered or unmetered subscription, you might be using an embedded WebLogic LDAP server.

Migrate Users And Groups from Oracle Identity Cloud Service

Migrate Users and Groups from Embedded WebLogic LDAP Server

Migrate Users And Groups from Oracle Identity Cloud Service

There are options for migrating users and groups from Oracle Identity Cloud Service.

- Use export and import features in Oracle Identity Cloud Service to migrate users and roles from an identity domain on Oracle Cloud Infrastructure Classic to another identity domain on Oracle Cloud Infrastructure. See Manage Oracle Identity Cloud Service Users or Manage Oracle Identity Cloud Service Groups
- The Essbase Migration Utility offers an option to migrate users and groups from Oracle Identity Cloud Service in your source environment at the same time as you migrate your Essbase cloud applications.

Migrate Users and Groups from Embedded WebLogic LDAP Server

Process bulk export of files with multiple users and roles, for LDAP identity mode.

1. Log into Oracle Analytics Cloud - Essbase as a Service Administrator, **server_admin**.
2. On the Applications page, click **Security**.
3. On the Security page, on the **Users** tab, click **Export**.
4. Save the `.csv` file to a local directory.
5. You can open the `.csv` file in Excel to view the exported user data. Note that passwords are not exported, so that the column does not contain values. You can enter a password in this column, to assign an initial user password for users imported from this file.
6. Modify CSV format (columns) to match the format that Oracle Identity Cloud Service can import. Sample CSV format can be found in the Oracle Identity Cloud Service user import dialog.
7. Import users into Oracle Identity Cloud Service. For more details, see Import a Batch of Users into a Cloud Account with Identity Cloud Service.

   CLI tool using LCM handles the migrating of roles, if the same set of users exist in the new Oracle Identity Cloud Service environment on Marketplace.

   Use the Migration Utility to migrate users and groups from the source embedded WebLogic LDAP at the same time as you migrate your Essbase cloud applications. See Migrate Cloud Service Applications Using Migration Utility.

Complete System Hardening and Cleanup Tasks

After you deploy Oracle Essbase on Oracle Cloud Infrastructure using Marketplace, complete the following tasks for security.

Change Database Administrator Password

If you created an Autonomous Transaction Processing database or Oracle Cloud Infrastructure database during creation of the Essbase stack, Oracle highly recommends that you update the database administrator password, using the Oracle Cloud Infrastructure console. This password isn't used during the normal run time of the Essbase stack, but it may need to be provided for maintenance tasks. Afterward, delete the stack without running the destroy action.

Secure Your Network

See Ways to Secure Your Network.

Delete SSH Provisioning Key

> **Note:**
>
> This section, Delete SSH provisioning key, is no longer relevant as of version 19.3.0.3.4.

Optional. During creation of the Essbase stack, Oracle Resource Manager creates an SSH public-private key pair to support execution of commands during the provisioning process. Once provisioning is complete, you can delete this SSH provisioning key on both the bastion (if provisioned) and the Essbase compute node. To delete it, remove the public key from the /home/opc/.ssh/authorized_keys file. Then, delete the stack without running the destroy action.

Remove Vault

Delete any vault or key (formerly prefixed by KMS) that you created during Essbase stack provisioning, in Encrypt Values Using Vault.

Delete Stack

(Optional) Once the Essbase stack is created, you can delete the stack without running the destroy action. This helps to declutter the Oracle Resource Manager interface, and deletes the state, which contains encrypted values of sensitive content.

See Delete the Stack.

Troubleshoot Deployment Errors

When you deploy the Oracle Essbase stack, you may encounter some of the following errors in the log displayed in the Oracle Resource Manager console.

Error Code	Message / More Information
ESSPROV-00000	Unknown error occurred.

Error Code	Message / More Information
ESSPROV-00001	Essbase System Admin username should be alphanumeric and length should be between 5 and 128 characters.
ESSPROV-00002	Essbase System Admin password should start with a letter and length should be between 8 and 30 characters, and should contain at least one number, and optionally, any number of the special characters ($ # _). For example, Ach1z0#d.
ESSPROV-00003	Database Admin password should start with a letter and length should be between 12 and 30 characters, and should contain at least one number, and at least one of the special characters ($ # _). For example, BEstr0ng_#12. See Complete System Hardening and Cleanup Tasks.
ESSPROV-00005	Missing value for IDCS Application Client ID. See Create a Confidential Identity Cloud Service Application.
ESSPROV-00006	Missing value for IDCS Application Client Secret. See Create a Confidential Identity Cloud Service Application.
ESSPROV-00007	Missing value for IDCS Instance GUID. See Create a Confidential Identity Cloud Service Application.
ESSPROV-10001	Permission denied accessing the target autonomous database. There may be a mismatch in the target dynamic policies for the compute instance. See Set Up Policies.
ESSPROV-10002	Permission denied downloading the wallet for the target autonomous database. There may be a mismatch in the target dynamic policies for the compute instance. See Set Up Policies.
ESSPROV-10003	Permission denied decrypting the target encrypted value with the given encryption key. There may be a mismatch in the target dynamic policies for the compute instance. See Set Up Policies.
ESSPROV-10010	Unable to validate the given IDCS Client ID and/or IDCS Client Secret.
ESSPROV-10011	Unable to connect to the IDCS endpoint. Validate that the IDCS Tenant GUID is valid.

3

Migrate Your Essbase Instances to Oracle Cloud Infrastructure

When your target environment is ready, migrate your Essbase applications to Oracle Cloud Infrastructure.

Prepare to Migrate Cloud Service Applications and Users

Migrate Cloud Service Applications

Prepare to Migrate Cloud Service Applications and Users

Here are some considerations and requirements when migrating cloud service applications from Oracle Analytics Cloud - Essbase.

You can use the Essbase command-line tool (CLI) to migrate your source application and artifacts across Oracle Analytics Cloud - Essbase deployments and releases. This is used to migrate applications one-at-a-time.

You can use Migration Utility tool to migrate multiple applications, artifacts, and users at one time, across Essbase cloud services.

- If you're migrating across Essbase cloud deployments and releases, from v17.3.3 (or earlier), use the scripts for migrating to Essbase. See Scripts for Administration Tasks. This also applies to export and import of provisioned application roles and scripts.
- Restoring an application or database from a prior backup, after the application or database was re-created using LCM import, isn't supported.
- Global variables, email configuration settings, and file scanner settings must be set on the target instance before using any of the migration tools.
- Oracle Identity Cloud Service roles aren't supported in Essbase.
- After migration from Oracle Analytics Cloud - Essbase, Identity Cloud Service provisioning doesn't continue to be honored. However, Essbase server/application level role assignments are migrated.
- All Identity Cloud Service users and groups listed in the Security provisioning page in the Essbase web interface can be provisioned with one of the Essbase roles: User, Power User, and Service Administrator.
- Migration Utility can migrate users and groups from embedded LDAP (or from Identity Cloud Service) to Identity Cloud Service in addition to all Essbase applications.
- If you're migrating users and groups from an LDAP source to an Essbase instance, Identity Cloud Service doesn't support nested groups. Therefore, group associations to other parent groups, from an LDAP source instance, aren't migrated to Identity Cloud Service targets, when using Migration Utility.

- Any users or groups that exist with the same name in the target environment as in the source environment, aren't updated in the target.
- To run Essbase CLI or Migration Utility, use the Identity Cloud Service user that you provisioned to be the initial Essbase Service Administrator during the Essbase deployment and setup.
- When you run Migration utility for SSL connection, include the host (-Dhttps.proxyHost) and port (-Dhttps.proxyPort) proxy settings in the command line.

The required user roles are as follows:

- For exporting: Application manager for the application created. In addition, the following roles can use LCM utility and CLI tool: Service Administrator for all applications; Power User for all applications created by the Power User.
- For importing: Power User or Service Administrator, for creating new applications during import. If you use the Power User role, then the target applications are owned by the Power User used in the migration.

Migrate Cloud Service Applications

You can migrate applications and cubes from cloud service instances to Essbase 19c. Learn how to prepare for migration, and review some use cases for migrating.

You can use the Command-Line Interface (CLI) tool to migrate your source application and artifacts from cloud deployments and releases. This is used to migrate applications one-at-a-time.

You can use the Migration Utility tool to migrate multiple applications, artifacts, users, and groups at one time, from Oracle Analytics Cloud – Essbase.

- Migrated Cloud Service Artifacts
- Migrate Cloud Service Applications Using CLI Tool
- Migrate Cloud Service Applications Using Migration Utility

Migrated Cloud Service Artifacts

The following table describes which global, application-level, and cube-level Essbase artifacts you can migrate between cloud service instances.

Artifact	Supported For Oracle Analytics Cloud migration	Exceptions/Comments
Application and cube metadata	yes	Application metadata includes application type and settings. Cube metadata includes cube properties and settings.
Application-level configuration files	yes	If these files exist, they're migrated.
Calculation scripts	yes	Application- and cube-level calculations are migrated.

Artifact	Supported For Oracle Analytics Cloud migration	Exceptions/Comments
Catalog server	no	Files listed under Files in the web interface under Applications/<appname> are migrated. Other files stored under Shared/Users folders aren't migrated. You can manually download them in the web interface and restore them.
Connections and Datasources	yes	Using Migration Utility, system- and application-level connections and Datasources are migrated. Using CLI tool, connections and Datasources created at the application level are migrated. With both tools, you must include the following argument in `lcmexport` operations: `-include-server-level` (or its abbreviation `-isl`).
Data	yes	To be migrated, data must be in the cube directory on the cloud instance.
Disk volumes	NA	Disk volume definitions aren't applicable to Essbase cloud instances.
Drill through definitions	yes	Drill through definitions are migrated.
Excel workbooks and files	yes	Excel workbooks and files are migrated.
Filters	yes	Cube-level and user-created filters are migrated.
Global variables	yes	-
Layouts	yes	Cube-level layouts are migrated.
Linked Reporting Objects (LROs)	yes	LROs are included for backward compatibility with migrated on-premises applications.
Location aliases	yes	Location aliases are migrated with the cube.
Log files	no	Log files aren't migrated.
Named queries	yes	Cube-level named queries are migrated.
Outlines and formulas	yes	Formulas containing @XREF aren't migrated.

Artifact	Supported For Oracle Analytics Cloud migration	Exceptions/Comments
Partitions	yes	Replicated and transparent partitions are migrated. Only partition definitions from the target cube are exported to the file system.
Report scripts	yes	Application- and cube-level report scripts are migrated. The scripts are included for backward compatibility with migrated on-premises applications.
Rule files, text files, .csv files	yes	Application-and cube-level files are migrated.
Scenarios	yes	If a cube is scenario-enabled and has a Sandbox dimension, the related scenarios are migrated.
Substitution variables	yes	Application- and cube-level substitution variables are migrated. If you have global (server)-level substitution variables, you must convert them to application-level variables prior to migration, or recreate them in the Console after migration.
Users and groups	-	Users and groups are migrated using Migration Utility; they aren't migrated when using CLI tool.
User roles	yes	User roles can be migrated only from one Essbase cloud instance to another.
Wallet files	yes	Wallet files are migrated for the specified application.

Migrate Cloud Service Applications Using CLI Tool

You can use Command-Line Interface (CLI) tool to migrate a source application and artifacts across Essbase cloud deployments and releases. The tool is used to migrate applications one-at-a-time.

The standard migration workflow using the Essbase command line tool (CLI) is as follows:

1. Download the CLI tool. See Download and Use the Command-Line Interface.
2. Use the CLI lcmexport command to export individual applications one-by-one from source to a zip file. See LcmExport: Back Up Cube Files
3. Use the CLI lcmimport command to import each individual application from a zip file to Oracle Essbase. See LcmImport: Restore Cube Files

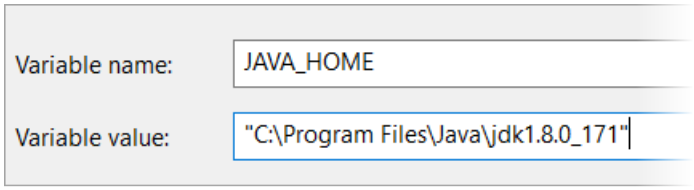
Use the following workflow when the source deployment is from Oracle Analytics Cloud (either Oracle Cloud Infrastructure or Oracle Cloud Infrastructure Classic) using Oracle Identity Cloud Service Federated Security.

1. Create a new Identity Cloud Service application. See Create a Confidential Identity Cloud Service Application.
2. Configure your Identity Cloud Service instance to point to the same external security provider used in Oracle Analytics Cloud.
3. Download the CLI tool, and using the lcmexport command, export individual applications one-by-one from source to a zip file. Specify the **-isl** option to include server level roles.
4. Manually re-create, in the new Identity Cloud Service instance, any non-federated users (Identity Cloud Service local users) that you had in the source instance. This is necessary if you want to use tools like CLI, MaxL, or REST API.
5. Using the CLI lcmimport command, import each individual application from a zip file to Oracle Essbase.

When partitions exist in the source between a source application or database, and a target application or database, only partitions from the target are exported to the file system. When partitions exist between cubes being migrated, you must import the data source before the data target. Otherwise, partition definitions may not be restored.

Download and Use the Command-Line Interface

1. If it is not already installed, download and install Java SE Development Kit 8 from Oracle Technology Network.
2. Set the JAVA_HOME environment variable on your system to point to the JDK installation folder. If the installation path has any spaces, enclose the path in quotation marks.



3. In the Essbase web interface, click **Console**.
4. In the Console, go to **Desktop Tools** and expand **Command Line Tools**.
5. Click **Download**

   next to the utility labeled **Command-line Tool.**
6. Download `cli.zip` to a local drive. For best results, choose a path that has no spaces; for example, `C:\Oracle`.
7. Uncompress `cli.zip`, and see the extracted files under the `cli` folder.
8. To issue commands interactively,
   a. Navigate to the CLI folder containing the shell script, `esscs.bat` or `esscs.sh`.

b. Set the proxy and launch the CLI:

For Windows:

```
set HTTPS_PROXY=www-proxy.example.com:80
esscs.bat login -u MyAdmin -p mypass7YG -url https://192.0.2.1/
essbase
```

For Linux:

```
export HTTPS_PROXY=www-proxy.example.com:80
esscs.sh login -u MyAdmin -p mypass7YG -url https://192.0.2.1/
essbase
```

For more examples and details, see the CLI `login` command topic in the *Using Oracle Essbase* documentation.

If the CLI was installed correctly, a list of supported commands is displayed.

9. To execute multiple CLI commands, add them to any shell script and execute it.

In any script you run that contains CLI commands, Oracle recommends you include the following directive before the CLI login statement:
For Windows:

```
set ESSCLI_ID=%USERNAME%_%random%
```

For Linux:

```
export ESSCLI_ID=`whoami`_$PPID
```

This helps store session information and prevent execution errors when multiple scripts are run concurrently.

Selective and Ordered Import of Artifacts

You can control import of Essbase artifacts using a selection list text file, using the CLI tool.

A selection list text file contains a list of all artifacts in the exported zip that are grouped by section. You can generate the file during export using lcmexport command. At the end of the file is an IMPORT section that contains the list of artifact entries to be imported.

You can edit the file and delete, or comment, the rows of artifacts that you want to skip in the import, using lcmimport command. You provide the text file as an argument in lcmimport operation. You can also control the order of import.

Sample selection list text file

```
@Provisions
/Sample/Provisions/CalcAssociation.csv

@Databases/Basic/Calc_scripts
/Sample/Databases/Basic/Calc scripts/Default Calc
```

```
/Sample/Databases/Basic/Calc scripts/CalcAll.csc

# ------------IMPORT-----------------
import @Provisions
import @Databases/Basic/Calc_scripts
# ------------IMPORT----------------
```

How to use this feature

- During export with the CLI tool, you can specify in the lcmexport command, the optional argument `-gal,–generateartifactlist` to generate a text file containing a list of exported artifacts.
- To skip a complete category of files, such as .rul files, comment the corresponding IMPORT section at the end of the text file.
- To skip specific files, delete or comment those entries in the text file.
- To control the import order, rearrange the entries under any specific category into the order that you prefer them to be imported. Files are then imported in the order listed under that category. During import, specify this file using `-al,-artifactlist`.
- Note that the lcmimport command has an `-overwrite` option.
  - If `–overwrite` is true, the import operation recreates the entire application. It only imports the artifacts or files that are listed in the text file.
  - If `–overwrite` is false, the import operation imports just the artifacts or files that aren't commented in the text file. It doesn't impact other artifacts already present in the target application.

Sample use cases

- **Import only the data from exported zip**
  You have an exported zip of Sample app and want to just import the data from Sample/Basic.
  - In the text file generated during lcmexport, comment all the import entries, except "import @Databases/Basic".
  - Also comment "/Sample/Databases/Basic/Basic outline" under "@Databases/Basic", just to import data alone.
  - Note that `-overwrite` option is not valid for this use case (“data only” import). The reason is that during import, LCM will drop the entire application and import it as blank. Then, only data is attempted to be imported, without the outline, therefore making the application invalid.
- **Import outline only**
  You want to update the Sample.Basic cube with just the outline from the exported zip.
  - In the IMPORT section at the end of the text file, comment all entries except "import @Databases/Basic".
  - Also comment "/Sample/Databases/Basic/Data" under "@Databases/Basic", just to import the outline.
- **Import single cube for an application with multiple cubes**
  Sample application has three cubes named Basic, Basic1, Basic2, and you want to just import Basic.

- In the IMPORT section at the end of the text file, comment all entries except "Basic" cube (import @Databases/Basic, import @Databases/Basic/Xml_files, etc.).
- Without the -overwrite option, it imports or overrides only the Basic cube, whereas other cubes (Basic1, Basic2) in that application, remain as they are without any impact.
- With the -overwrite option, it drops and recreates the application, with just the Basic cube.

LcmExport: Back Up Cube Files

This CLI command backs up cube artifacts to a Lifecycle Management (LCM) `.zip` file. To do this, you need at least Application Manager permission.

Syntax

```
lcmExport [-verbose] -application appname [-zipfilename filename] [-
localDirectory path] [-threads threadscount] [-skipdata] [-overwrite]
[-generateartifactlist] [-include-server-level]
```

Option	Abbreviation	Description
-verbose	-v	Optional. Show extended descriptions
-application	-a	Name of application to back up
-zipfilename	-z	Optional. Name of compressed file to hold backup files
-localdirectory	-ld	Optional. A local directory path
-threads	-T	Optional. Number of threads to spawn if using parallel export. Minimum: 10
-skipdata	-skip	Optional. Do not include data in the backup
-overwrite	-o	Optional. Overwrite existing backup file
-generateartifactlist	-gal	Optional. Generate a text file containing a complete list of the exported artifacts. You can use this text file to manage the import of artifacts. For example, you can rearrange the order of artifacts in the list to control the order in which they are imported. You can skip importing some artifacts by removing or commenting out items in the list.
-include-server-level	-isl	Optional. Include globally defined connections and Datasources as part of the export

Notes

This command, like other CLI commands, can be used from outside the Essbase machine, whereas the LCM utility must be run on the Essbase machine.

Example

```
esscs lcmExport -v -a Sample -z Sample.zip -ld c:/temp -skip -o -gal
-isl
```

LcmImport: Restore Cube Files

This CLI command restores cube artifacts from a Lifecycle Management (LCM) `.zip` file. To do this, you must be the power user who created the application, or a service administrator.

Syntax

`lcmImport [-verbose] -zipfilename` *`filename`* `[-overwrite] [-targetappName` *`targetApplicationName`*`] [-artifactlist` *`artifactList`*`]`

Option	Abbreviation	Description
-verbose	-v	Optional. Show extended descriptions
-zipfilename	-z	Name of compressed file containing backup files
-overwrite	-o	Optional. Recreate the target application.
-targetappName	-ta	Optional. Target application name, if you want it to be different from the source name.

-artifactlist	-al	Optional. Name of the file containing the list of artifacts to import. This file can be generated from lcmexport. To skip artifacts, comment out or delete entries from the list. For example, to skip importing audit records, comment out that line, as shown:
		
		`# ------------IMPORT-----------------`
		`import @Provisions`
		`import @Databases/Basic`
		`#import @Databases/Basic/Audit`
		`import @Databases/Basic/Text_files`
		`import @Databases/Basic/Xml_files`
		`import @Databases/Basic/Calc_scripts`
		`import @Databases/Basic/`
		`Open_XML_Excel_files`
		`import @Databases/Basic/`
		`ScenarioManagement`
		`import @Databases/Basic/Provisions`
		`import @Databases/Basic/Rule_files`
		
		To control import order, rearrange the `import` entries in the text file.
		If –overwrite is used, the import operation deletes and recreates the entire application, importing only the artifacts present in the list. If –overwrite is not used, the import operation includes the artifacts specified in the list, without impacting any other artifacts already present in the target application.

Notes

- This command, like other CLI commands, can be used from outside the Essbase machine, whereas the LCM utility must be run within the Essbase machine.

- When partitions exist between cubes being migrated, you must import the data source before the data target. Otherwise, partition definitions may not be restored.

Example

```
esscs lcmImport -z C:/Sample/Sample.zip -o -al C:/Sample/Sample.txt
```

Migrate Cloud Service Applications Using Migration Utility

You can use Migration Utility to migrate source applications and elements from Oracle Analytics Cloud - Essbase deployments and releases to Essbase 19c. The utility migrates multiple applications at one time. It also migrates artifacts, rules, users and groups.

As an Essbase Service Administrator user, you can use Migration Utility to migrate an entire instance (all applications, users and groups, and other artifacts) from one cloud instance to another in a single process. Note that the Essbase Command-line tool (CLI) commands, lcmimport and lcmexport, require you to migrate applications one-at-a-time, and do not migrate users and groups.

Here are some use cases for migrating with Migration Utility.

- Use this utility if you want to migrate users on Oracle Cloud Infrastructure Classic to Oracle Identity Cloud Service on Oracle Cloud Infrastructure, at the same time that you migrate your cloud service application.
- WebLogic LDAP users can migrate the users from LDAP in the source to Identity Cloud Service in the target.
- Use this utility for basic deployments that aren't customized. If your deployment includes customizations, such as custom Single Sign On solutions, use CLI tool instead of Migration Utility.
- When the source deployment is from
  - Oracle Analytics Cloud - on Oracle Cloud Infrastructure, using Identity Cloud Service Native Security, or
  - Oracle Analytics Cloud - on Oracle Cloud Infrastructure Classic, using Identity Cloud Service Native Security, or
  - Oracle Analytics Cloud - on Oracle Cloud Infrastructure Classic, using Embedded LDAP

  then before using the Migration utility steps below to export, first create a new Identity Cloud Service application. Also, before using the Migration Utility steps below to import, change the host and Identity Cloud Service details in `import.properties` to point to the target Essbase 19c instance.

To migrate cloud service applications and users using Migration Utility

1. Before you use the utility, if you haven't already, patch your source Essbase instance to the latest version. You download the utility from the target Essbase 19c instance.
2. If it isn't already installed, download and install Java SE Development Kit (JDK) 8 from Oracle Technology Network.
3. Set the JAVA_HOME environment variable name on your system to point to the JDK installation folder. If the installation path contains any spaces, enclose

the path in the variable value, within quotation marks, for example, `"C:\Program Files\Java\jdk1.8.0_171"`.

4. Sign in to the target Essbase, and navigate to the Console tab.
5. In the Console, go to Desktop Tools, and expand Command Line Tools.
6. Click **Download** next to **Migration Utility**.
7. Download `migrationTools.zip` to a local drive. For best results, choose a path that has no spaces, for example, `C:\Oracle`.
8. Extract `migrationTools.zip`, and see the extracted files (properties, jar, and readme) in the `migrationTools` folder.
9. Before you run the import or export commands provided with Migration Utility, you must edit the properties files.
    a. Edit the properties strings in the `export.properties` file:
        - userName - Essbase administrator user name.
        - password - Essbase administrator password.
        - host - Essbase host or IP address.
        - port - Essbase port. Enter the value of 80 for LDAP source. Otherwise, accept the default value of 443 (SSL/TLS) for Identity Cloud Service source.
        - proxy - proxy server URL.
        - skiprole - import of roles from Oracle Analytics Cloud - Essbase is skipped. Value must be left empty or true.
    b. Edit the properties strings in `import.properties` file:
        - userName - Essbase administrator user name.
        - password - Essbase administrator password.
        - host - Essbase host or IP address.
        - port - Essbase HTTP listening port. Default value 443 (SSL/TLS).
        - userPassword - Initial password assigned for all new users.
        - proxy - proxy server URL (optional)
    c. Edit Identity Cloud Service information in `import.properties` to obtain values from the Service Console for Oracle Identity Cloud Service for the following:
        - idcsHost - Identity Cloud Service host
        - idcsTenant - Identity Cloud Service tenant
        - clientId - Client identifier for OAuth authorization
        - clientSecret - Client secret for OAuth authorization
        - appId - Application identifier

        From the Oracle Cloud Infrastructure console, click the left navigation icon. Under **Governance and Administration**, select **Identity**, and **Federation**.

        You should see OracleIdentityCloudService as an Identity Provider. Here you will find the **Oracle Identity Cloud Service Console** url. For example, `https://`

`idcs-170644901bf04406ae7180bd3d995ce6.identity.oraclecloud.com/ui/v1/adminconsole/`. In this url, **idcsHost** is `identity.oraclecloud.com`.

idcsTenant is `idcs-170644901bf04406ae7180bd3d995ce6`.

For **clientId**, and **clientSecret**, see values recorded from the deployment steps for Essbase 19c.

For **appId**, navigate to the client application from the Oracle Identity Cloud Service Console, click the left navigation icon, and select **Applications**. Search for the client application and select the application. On the target landing page, capture the URL from the browser address bar. It should look like this: **https://idcs-170644901bf04406ae7180bd3d995ce6.identity.oraclecloud.com/ui/v1/adminconsole/?root=apps&app=79692ac19e9e451ebe1bf9eceec3b483**. From this URL, look for the `app` parameter. This provides the **appId**. For the above example, **appId** is `79692ac19e9e451ebe1bf9eceec3b483`.

10. To run Migration Utility, use the following java command to export all applications, users, and groups from the Essbase source instance catalog to a tar file.

```
java -jar -Dhttps.proxyHost=<proxy-url> -Dhttps.proxyPort=<nn>
      migrationTools.jar export export.properties <new_tar_file>
```

for example:

```
 e.g. java –jar -Dhttps.proxyHost=www-proxy-abcdef.example.com
      -Dhttps.proxyPort=80 migrationTools.jar import
import.properties 115ldap.tar.gz
```

11. After you export from the source instance, use the following java command to import the data tar file to the target instance.

```
java -jar -Dhttps.proxyHost=<proxy-url> -Dhttps.proxyPort=<nn>
      migrationTools.jar import import.properties
<existing_tar_file>
```

12. After you run the import, the data is stored in the Essbase catalog of the target instance. If any exported applications already exist on the target, they aren't overwritten.

4

Complete the Post-Migration Tasks

After successfully migrating your Essbase content, test your instance thoroughly, and then perform cleanup.

Test the Migrated Essbase Instance

Clean Up Infrastructure and Platform Resources in Oracle Analytics Cloud - Essbase Classic (Customer Managed)

Clean Up Infrastructure and Platform Resources in Oracle Analytics Cloud - Essbase (Oracle Managed)

Test the Migrated Essbase Instance

After migrating your instance to Oracle Cloud Infrastructure, test thoroughly to ensure it's production-ready.

Essbase post-migration tasks:

- If you have any artifacts in LCM that are not supported for migration, they can be manually migrated.
- Test that the migrated data loads and dimension builds work as expected.
- Run a Smart View report to check connectivity and data.
- After the results look OK, scan the application logs for errors, warnings, and suspicious messages.

Clean Up Infrastructure and Platform Resources in Oracle Analytics Cloud - Essbase Classic (Customer Managed)

After testing your Essbase instance on Oracle Cloud Infrastructure you can delete the source Oracle Analytics Cloud – Essbase instance and other supporting resources in Oracle Cloud Infrastructure Classic such as IP reservations, the associated cloud database, cloud storage, and so on. Remove these resources from Oracle Cloud Infrastructure Classic to avoid costs for services that you no longer use.

1. Delete the Oracle Analytics Cloud – Essbase instance.
    a. Sign in to your Oracle Cloud account, and navigate to the **Analytics Classic** page.
    b. Click **Manage this instance**  for the instance you migrated, and then select **Delete**.
    c. When prompted for confirmation, click **Delete**.
2. Delete IP reservations that you created for the service.
    a. Click **IP Reservations**.

b. Click **Delete** for the IP reservation.

c. When prompted for confirmation, click **OK**.

3. Delete the Oracle Database Cloud Service service instance associated with the Oracle Analytics Cloud – Essbase instance.

   Don't delete a database if it's still used by other services.

   a. Navigate to the **Database Classic** page.

   b. Click **Manage this instance** for the database instance, and then select **Delete**.

   c. When prompted for confirmation, click **Delete**.

4. Delete any object storage containers that you created in Oracle Cloud Infrastructure Classic to support your source Oracle Analytics Cloud – Essbase instances.

   Don't delete a container if it's still used by other services.

   a. Navigate to the **Storage Classic** page.

   b. Click the delete icon for the container.

   c. When prompted for confirmation, click **OK**.

Clean Up Infrastructure and Platform Resources in Oracle Analytics Cloud - Essbase (Oracle Managed)

For Oracle Cloud Infrastructure (Oracle Managed) instances, after testing your Essbase instance on Oracle Cloud Infrastructure you can delete the source Oracle Analytics Cloud – Essbase (Oracle Managed) instance and other supporting resources in Oracle Cloud Infrastructure Classic. Remove these resources from Oracle Cloud Infrastructure Classic to avoid costs for services that you no longer use.

- Delete the Oracle Analytics Cloud – Essbase (Oracle Managed) service instance.

  1. Sign in to your Oracle Cloud account, and navigate to the Oracle Analytics Cloud – Essbase **Service Details** page.

  2. Click **Action Menu** for the instance you migrated, and then select **Delete**.

  3. When prompted for confirmation, click **Delete**.

5

Manage Users and Roles

Essbase integrates with security layers managed by Oracle to create a highly secure environment for the cloud. Service Administrators can assign appropriate user roles and application permissions in Essbase.

About Users and Roles

User Roles and Application Permissions

Provision Application Permissions

About Users and Roles

The following are common use cases for assigning access to users:

- Users can view and access cubes (databases) for which they were assigned access to the related applications.
- Power Users can create enterprise-level cubes and grant other users access to applications for which they have an Application Manager role.
- Service Administrators can assign users at all levels and manage all aspects of the applications, cubes, and users.
- Service Administrators can assign a Database Update role for users who need to update data in a cube.

To provide access to Essbase users, the following steps are required:

- Assign Essbase user role
- Assign Essbase application-level permissions

Access to Essbase is restricted by security, and managed by Oracle Identity Cloud Service. You create users and user groups in the Oracle Identity Cloud Service administration interface.

Oracle Identity Cloud Service doesn't support creating nested groups (assigning a group to a parent group).

User Roles and Application Permissions

Users can work with applications and cubes according to their assigned roles and permissions. Roles and permissions help you manage the business activities users are permitted to perform within an Essbase instance, and the application data that they can access.

User roles are incremental; access granted to lower-level roles is inherited by higher-level roles. For example, Service Administrators, in addition to the access that only they have, inherit the access granted to Power User and User roles. You assign user roles in the Security page (available only to Service Administrators).

Table 5-1 User Roles

User Role	Description
Service Administrator	Full access to administer users, applications, and cubes.
Power User	Ability to create and delete applications and cubes that were created by this user. Ability to be granted access to, and to perform, some administrative tasks in applications and cubes created by others and provisioned to this user.
User	Ability to access any provisioned application, or a cube that has a minimum access permission. This user role has no access to administrative tasks in applications or cubes.

Users can access most Essbase features and functionality only after being assigned an application permission in addition to their user role. Application permissions determine more than simply which users and groups can see an application or cube. They also determine whether the user can view data, update data, or manage the cube or application.

Application permissions can be assigned to users and groups using the Permissions tab within the application inspector (available to Service Administrators, application managers, and some power users).

Table 5-2 Application Permissions

Application Permission	Description
Application Manager	Ability to create, delete, and modify cubes and application settings within the assigned application; assign users to an application; create and delete scenarios, and give permission to run calculation scripts.
Database Manager	Ability to manage cubes, cube elements, locks, and sessions within the assigned application; create and delete scenarios, execute calculation scripts, and assign permissions to run calculation scripts.
Database Update	Ability to read and update data values based on assigned scope. Ability to create and delete scenarios. The permission to execute calculation scripts necessitates write access; however, filters may be assigned with None or Read permission to block access to certain cells.
Database Access	Ability to access scenarios, read data values in all cells, and access specific data and metadata, unless further overridden by filters. Can update values in specific cells, if granted write access to those cells through filters.

Provision Application Permissions

If you're a Service Administrator or Power User, you can provision application access permissions, which are incremental. Upper-level permissions include the privileges of lower-level permissions.

Users can have a unique permission for each application or cube. The permissions, from least privileged to highest, are:

- Database Access
- Database Update
- Database Manager
- Application Manager

1. In the Essbase web interface, on the Applications page, select an application row, and then in the **Actions** menu, select **Inspect**.
2. On the **Permission** tab, use the + to open a menu for selecting users or groups to provision for access to the application.
3. Use the radio buttons to select the appropriate role(s) for the relevant users and groups.
4. Click **Close**.

6

Monitor Essbase Operations

(Optional) You can monitor and set notifications on Essbase operations. This was added in version 19.3.0.3.4.

Topics:

- Monitor Operations and Resources Using Oracle Cloud Infrastructure Monitoring Service
- Get Event Notifications Using Oracle Cloud Infrastructure Notifications Service

Monitor Operations and Resources Using Oracle Cloud Infrastructure Monitoring Service

Oracle Cloud Infrastructure Monitoring service enables you to actively and passively monitor your cloud resources using the Metrics and Alarms features.

> **Note:**
>
> This feature was added for version 19.3.0.3.4.

You use Monitoring service, which collects metrics for Essbase processes and volumes deployed in the stack, to create alarms and triggers related to your CPU, memory, and storage utilization. See Monitoring Overview in Oracle Cloud Infrastructure documentation. You must set the relevant additional policies.

When Monitoring is enabled, the compute instance starts a background process to collect metrics and publish them to the Oracle Cloud Infrastructure Monitoring service using the “oracle_essbase” namespace.

Monitoring queries can be customized and run in the Metrics Explorer, which can be accessed from the Oracle Cloud Infrastructure console, in Monitoring > Metrics Explorer. For information on viewing default metrics and building queries, see Viewing Default Metric Charts and Building Metric Queries in the Oracle Cloud Infrastructure documentation.

For metrics dimensions, various dimensions are provided that can be used to filter the metrics that will be displayed. There are some noteworthy dimensions, including:

- stackDisplayName – corresponds to the name of the stack that was provided on the stack definition page.

The following metrics are also provided.

- Volume – collected for each block volume attached to the compute instance
  - VolumeTotalSize – total size in bytes for a given volume
  - VolumeUsedSize – number of bytes used for a given volume

  - VolumeFreeSize – number of bytes free for a given volume
  - VolumeUsedPercent – percentage of the volume used
- Process – collected for all Essbase processes running on the compute instance
  - CpuUtilization – CPU utilization for a process
  - MemoryUtilization – memory utilization for a process

Get Event Notifications Using Oracle Cloud Infrastructure Notifications Service

Use notifications to get notified when event rules are triggered, or alarms are breached, or to directly publish a message. This feature is optional.

The use of Oracle Cloud Infrastructure Notifications service is optional. This service can be used by subscribers to be notified of life cycle events. Notifications service broadcasts messages to distributed components through a publish-subscribe pattern, delivering secure, highly reliable, low latency, and durable messages, for applications hosted on Oracle Cloud Infrastructure and externally. See Notifications Overview in Oracle Cloud Infrastructure documentation. For information on managing and creating alarms, see Building Metrics and Managing Alarms.

> **Note:**
>
> This feature was added for version 19.3.0.3.4.

> **Note:**
>
> If you don't use Monitoring service, the alternative method to monitor is to ssh into the machine and monitor the essbase-init-log file.

If notifications are enabled, messages are published on the given topic for the following events:

- Compute instance configuration started
- Compute instance configuration completed or failed
- Backup started
- Backup completed or failed