Contents

Preface

Audience vi
Documentation Accessibility vi
Related Documents vii
Conventions vii

1 Get Started with Administration

About Oracle Analytics Cloud 1-1
Typical Workflow for Administrators 1-1
Before You Begin With Oracle Analytics Cloud - Classic 1-3
How to Begin With Oracle Analytics Cloud - Classic 1-4
How to Access Oracle Analytics Cloud - Classic 1-4
About Users and Roles 1-4
Top Tasks 1-5

2 Set Up Services

Typical Workflow to Set Up a Service 2-1
Before You Create a Service 2-1
Create a Service 2-5
Migrate to Oracle Analytics Cloud - Classic from Other Environments 2-10
Migrate LDAP-Based Services to Oracle Identity Cloud Service 2-11
Migrate BI Content and Users 2-11
  Create a New Service with Oracle Identity Cloud Service Enabled 2-11
  Export Content (BI Services) 2-11
  Import Content (BI Services) 2-13
Migrate Essbase Applications and Users 2-14

3 Manage Services

Typical Tasks to Manage a Service 3-1
View and Manage Services 3-2
Monitor Services 3-2
  About Oracle Analytics Cloud - Classic Metrics 3-2
  Run a Health Check 3-3
Delete a Service 3-3
Start, Stop and Restart Services 3-3
Back Up a Service 3-4
  Schedule Regular Backups 3-4
  Back Up a Service On Demand 3-4
  Disable and Enable Backups 3-5
Restore a Service 3-5
Patch and Roll Back 3-6
  Apply the Latest Patch to BI Services 3-6
    Before You Patch a BI Service 3-7
    Apply the Latest Patch to a BI Service 3-8
    After You Patch a BI Service 3-9
  Apply the Latest Patch to Essbase Services 3-9
    Patch Essbase Services from 17.3.3 and Earlier 3-9
  Roll Back a Patch to an Earlier Version 3-11
Scale Services 3-12
  Scale Compute Shape 3-12
  Scale Storage 3-13
  Scale a Cluster 3-13

4 Manage Service Access and Security

Manage SSH Access 4-1
Control Access to Service Components 4-1
Manage Access Rules 4-3
Assign Users to Application Roles with Oracle Identity Cloud Service 4-3
  About Application Role Assignment with Oracle Identity Cloud Service 4-3
  Grant Application Roles with Oracle Identity Cloud Service 4-4
Replace the Self-Signed Certificate for Secure HTTP Access 4-5
Redirect HTTP Traffic to HTTPS 4-6
Connect with EssNet over HTTP 4-6
Manage Credentials 4-6
  Update the Database Password for an Essbase Service 4-6
  Update the Database Password for a BI Service 4-7
  Update WebLogic Administrator Passwords for a BI Service 4-7
  Update Cloud Storage Passwords 4-7
Deploy Oracle Analytics Cloud - Classic on an IP Network 4-7
Frequently Asked Questions

Top FAQs for Administration and Configuration 5-2

Troubleshoot

Scripts for Administration Tasks

Run Administration Scripts A-3
Change the WebLogic Administrator Password (BI Service Script) A-4
Export Users and Roles to CSV Files (BI Service Script) A-5
Import Users and Roles from a CSV File (BI Service Script) A-6
Update or Delete Users and Roles from Embedded LDAP (BI Service Script) A-7
Create a Public Container for Sharing Content (BI Service Script) A-9
Export and Import Data Sets (BI Service Script) A-10
Update Database Credentials (BI Service Script) A-11
Gather Diagnostic Logs into a ZIP File (BI Service Script) A-12
Get Status Information (BI Service Script) A-13
Stop and Start Component Processes (BI Service Script) A-13
Register SSL Private Keys with the HTTP Proxy for a Nonmetered Service (BI Service Script) A-14
Redirect HTTP Calls to HTTPS (BI Service Script) A-16
Enable Database Storage for User Group Memberships for a Nonmetered Service (BI Service Script) A-17
Migrate Essbase Applications and Users A-18
Gather Diagnostic Logs into a ZIP File (Essbase Service Script) A-19
Update Database Credentials (Essbase Service Script) A-20
Preface

Learn how to create and manage services.

Topics:

• Audience
• Documentation Accessibility
• Related Documents
• Conventions

Audience

*Administering Oracle Analytics Cloud - Classic* is intended for business intelligence analysts and administrators who use Oracle Analytics Cloud:

• **Administrators** manage access to Oracle Analytics Cloud and perform other administrative duties such as backing up and restoring information for others.

• **Analysts** load and model data and create reports for consumers. Data integration options range from self-service import to operational ETL updates. Analysts can select interactive visualizations and create advanced calculations to reveal insights in the data.

• **Consumers** customize dashboard pages and work with their favorite reports. Dashboards allow consumers to quickly analyze and manage activity across their system.

Documentation Accessibility


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](http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info) or visit [http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs](http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs) if you are hearing impaired.
Related Documents

These related Oracle resources provide more information.

- Oracle Public Cloud http://cloud.oracle.com
- Getting Started with Oracle Cloud
- Managing and Monitoring Oracle Cloud
- Getting Started with Oracle Analytics Cloud
- Visualizing Data and Building Reports in Oracle Analytics Cloud
- Preparing Data in Oracle Analytics Cloud
- Using Oracle Analytics Cloud - Essbase
- Command Line Interface Reference
- Using Oracle Database Cloud Service

Conventions

Conventions used in this document are described in this topic.

Text Conventions

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

Videos and Images

Your company can use skins and styles to customize the look of the Oracle Analytics Cloud, 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.
Get Started with Administration

Let’s explore Oracle Analytics Cloud - Classic and what you need to know to get started with administration.

Topics:
• About Oracle Analytics Cloud
• Typical Workflow for Administrators
• Before You Begin With Oracle Analytics Cloud - Classic
• How to Begin With Oracle Analytics Cloud - Classic
• How to Access Oracle Analytics Cloud - Classic
• About Users and Roles
• Top Tasks

About Oracle Analytics Cloud

Oracle Analytics Cloud is a scalable and secure public cloud service that provides capabilities to explore and perform collaborative analytics for you, your workgroup, and your enterprise.

With Oracle Analytics Cloud - Classic deployed on Oracle Cloud Infrastructure Compute Classic, you get flexible service management capabilities including fast setup, easy scaling and patching, and automated lifecycle management with standards-based REST APIs.

For information about editions and features available, see Getting Started with Oracle Analytics Cloud.

Typical Workflow for Administrators

If you are new to Oracle Analytics Cloud - Classic, use the tasks in this topic as a guide.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscribe to Oracle Analytics Cloud - Classic</td>
<td>Provide your information, and subscribe to Oracle Analytics Cloud - Classic. Other Oracle Cloud services are also required: Oracle Cloud Infrastructure Object Storage Classic, Oracle Database Cloud Service.</td>
<td>Before You Begin With Oracle Analytics Cloud - Classic</td>
</tr>
</tbody>
</table>

Set up prerequisite services
<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set up the storage service</td>
<td>Select a storage replication policy (only required if your cloud account was created before March 2018) and make a note of the REST URL endpoint for your storage service.</td>
<td>Select a Replication Policy for Your Account Using the Web Console Find the REST Endpoint URL for Your Cloud Storage Account</td>
</tr>
<tr>
<td>Set up a cloud database service</td>
<td>Oracle Analytics Cloud - Classic needs a cloud database deployment to store various schemas and data and you can use the same database to store your own data if you want. Oracle Analytics Cloud - Classic requires the database to be Oracle Database 12c Release 1, Oracle Database 12c Release 2, or Oracle Database 11g Release 2 and deployed in the same region and availability domain as Oracle Analytics Cloud - Classic.</td>
<td>Create a Customized Database Deployment</td>
</tr>
<tr>
<td>Create a SSH key pair</td>
<td>(Optional) Create SSH public and private key pairs to secure access to your Oracle Analytics Cloud - Classic deployment.</td>
<td>Manage SSH Access</td>
</tr>
<tr>
<td>Create a service</td>
<td>Create a service with one or more Oracle Analytics Cloud components.</td>
<td>Create a Service</td>
</tr>
<tr>
<td>Enable network access</td>
<td>Permit access to network services associated with your Oracle Analytics Cloud - Classic deployments.</td>
<td>Control Access to Service Components</td>
</tr>
<tr>
<td>Add and manage users and roles</td>
<td>Create accounts for your users and assign them appropriate privileges.</td>
<td>About Users and Roles</td>
</tr>
<tr>
<td>Migrate data and content</td>
<td>Move data from on-premises or other cloud services to Oracle Analytics Cloud - Classic.</td>
<td>Migrate to Oracle Analytics Cloud - Classic from Other Environments</td>
</tr>
<tr>
<td>Monitor service instances</td>
<td>Check on the day-to-day operation of Oracle Analytics Cloud - Classic, monitor performance, and review important notifications.</td>
<td>Monitor Services</td>
</tr>
<tr>
<td>Patch a service</td>
<td>Apply a patch or roll back a patch.</td>
<td>Patch and Roll Back</td>
</tr>
<tr>
<td>Back up a service</td>
<td>Take regular backups in case you need to restore earlier content.</td>
<td>Back Up a Service On Demand</td>
</tr>
<tr>
<td>Scale a service</td>
<td>Scale various aspects of your service environment up (or down) as demands change: storage, compute shape, compute nodes.</td>
<td>Scale Services</td>
</tr>
</tbody>
</table>
Before You Begin With Oracle Analytics Cloud - Classic

You must have a subscription for Oracle Analytics Cloud - Classic and several other services, including Oracle Cloud Infrastructure Compute Classic, Oracle Database Cloud Service, and Oracle Cloud Infrastructure Object Storage Classic.

If you subscribe through Oracle Universal Credits you automatically have access to all the required services.

- **Oracle Cloud Infrastructure Compute Classic**
  Oracle Analytics Cloud - Classic uses block storage in Oracle Cloud Infrastructure Compute Classic to store binary files and logs. See How to Begin with Compute Classic Subscriptions in Using Oracle Cloud Infrastructure Compute Classic.

- **Oracle Database Cloud Service**
  You need Oracle Database Cloud Service to store various schemas and data associated with Oracle Analytics Cloud - Classic. Oracle Analytics Cloud - Classic supports Oracle Database 11g Release 2 and Oracle Database 12c Release 1 and Release 2. See How to Begin with Database Cloud Service Subscriptions in Administering Oracle Database Cloud Service.

  **Note:**
  Oracle Analytics Cloud - Classic doesn't support Oracle Database 18c, non-UTF databases, or Real Application Clusters (RAC) databases.

- **Oracle Cloud Infrastructure Object Storage Classic**
  Oracle Analytics Cloud - Classic uses Oracle Cloud Infrastructure Object Storage Classic containers to store analytics data sets and backups. See How to Begin with Oracle Cloud Infrastructure Object Storage Classic in Using Oracle Cloud Infrastructure Object Storage Classic.

- **Oracle Identity Cloud Service**
  This service is available through Oracle Universal Credits. Foundation is automatically provided when you subscribe to Oracle Analytics Cloud - Classic through Oracle Universal Credits. Some additional features are available with basic and Standard Editions. See About Oracle Identity Cloud Service Pricing Tiers and Features in Administering Oracle Identity Cloud Service.

  - **Oracle Cloud Infrastructure Load Balancing Classic**

- **Oracle Big Data Cloud**
  (Optional) Oracle Analytics Cloud - Classic can integrate with Oracle Big Data Cloud. If you have a big data service that you want to associate with Oracle Analytics Cloud - Classic, check everything is set up correctly.
How to Begin With Oracle Analytics Cloud - Classic

As an administrator, your job is to set up Oracle Analytics Cloud - Classic for others to use.

1. Sign up for a free credit promotion or purchase a subscription to Oracle Analytics Cloud - Classic.
   See Request and Manage Free Oracle Cloud Promotions or Buy an Oracle Cloud Subscription in Getting Started with Oracle Cloud.

   See How to Access Oracle Analytics Cloud - Classic.

3. Set up a service, with one or more components.
   See Create a Service.

4. Learn about user accounts and roles. Create accounts for your users and assign them appropriate privileges and roles.
   See About Users and Roles.

How to Access Oracle Analytics Cloud - Classic

You can access service created with Oracle Analytics Cloud - Classic in several different ways. You can click the My Services URL link in your welcome email or sign in from Oracle Cloud My Services.

To access Oracle Analytics Cloud - Classic through My Services:

1. Sign in to Oracle Cloud and navigate to the My Services Dashboard.

2. Click Navigation in the top corner of My Services, and then click Oracle Analytics Cloud - Classic.
   When you access Oracle Analytics Cloud - Classic for the first time, you see a Welcome page.

3. Click Services or Go to Console.
   A Create Service option and a list of existing services is displayed on the Services page.

4. To access an existing service, click the menu for the service, and then select Open Analytics Cloud URL.

About Users and Roles

One of the first jobs you do after setting up a service with Oracle Analytics Cloud - Classic is to add user accounts for everyone you expect to use the service and assign them to suitable roles.
The way you do this depends on the Oracle Analytics Cloud - Classic option you plan to deploy and the identity management system you plan to use.

<table>
<thead>
<tr>
<th>Oracle Analytics Cloud - Classic Option</th>
<th>Adding Users and Assigning Roles</th>
<th>Book</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Self-Service Data Visualization, Preparation and Smart Discovery</td>
<td>Manage What Users Can See and Do</td>
<td>Preparing Data in Oracle Analytics Cloud</td>
</tr>
<tr>
<td>• Enterprise Data Models</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Collaborative Data Collection, Scenarios and What-if Analysis</td>
<td>Manage Users and Roles</td>
<td>Using Oracle Analytics Cloud - Essbase</td>
</tr>
</tbody>
</table>

Top Tasks

If you’re an administrator for Oracle Analytics Cloud - Classic, here are some of your top tasks.

Topics

• Create a Service
• Migrate to Oracle Analytics Cloud - Classic from Other Environments
• Monitor Services
• Start, Stop and Restart Services
• Back Up a Service On Demand
• Patch and Roll Back
• Manage Service Access and Security
Set Up Services

You must be an administrator to create and set up services with Oracle Analytics Cloud - Classic. If you have existing applications and data that you want to analyze with Oracle Analytics Cloud - Classic, you might want to migrate that content before everyone gets started.

Topics:

• Typical Workflow to Set Up a Service
• Before You Create a Service
• Create a Service
• Migrate to Oracle Analytics Cloud - Classic from Other Environments
• Migrate LDAP-Based Services to Oracle Identity Cloud Service

Typical Workflow to Set Up a Service

If you’re creating a service with Oracle Analytics Cloud - Classic for the first time, follow these tasks as a guide.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sign up for a free credit promotion or purchase a subscription.</td>
<td>Provide your information, and sign up for a free trial or purchase a subscription to Oracle Analytics Cloud - Classic and several other required services.</td>
<td>Before You Begin With Oracle Analytics Cloud - Classic</td>
</tr>
<tr>
<td>Determine your service requirements</td>
<td>Plan your service. Think about what you want before you start.</td>
<td>Before You Create a Service</td>
</tr>
<tr>
<td>Create a service</td>
<td>Create a new service with one or more components.</td>
<td>Create a Service</td>
</tr>
<tr>
<td>Enable network access</td>
<td>Permit access to network services associated with your Oracle Analytics Cloud - Classic deployments.</td>
<td>Control Access to Service Components</td>
</tr>
<tr>
<td>Migrate content</td>
<td>Leverage your existing content in Oracle Analytics Cloud - Classic.</td>
<td>Migrate to Oracle Analytics Cloud - Classic from Other Environments</td>
</tr>
</tbody>
</table>

Before You Create a Service

Take some time to plan your Oracle Analytics Cloud - Classic service before you create it. Think about the questions outlined here and decide what you want to do, before you start.

• Check you're subscribed or have access to all the required services
  – Oracle Cloud Infrastructure Compute Classic
– Oracle Database Cloud Service
– Oracle Cloud Infrastructure Object Storage Classic
– Oracle Identity Cloud Service (Oracle Universal Credits required)
  * Oracle Cloud Infrastructure Load Balancing Classic

Additional services:
– Oracle Big Data Cloud (required for Essbase Edition)

See Before You Begin With Oracle Analytics Cloud - Classic.

• **Which edition do you want to use?**
  – Standard Edition
  – Essbase Edition
  – Enterprise Edition

You need the Enterprise Edition if you want to offer enterprise modeling and reporting features available in Oracle Analytics Cloud - Classic. See Standard, Essbase and Enterprise Editions in Getting Started with Oracle Analytics Cloud.

• **How do you want metered usage to be billed?**
  – Hourly
  – Monthly

Oracle recommends hourly billing, if you expect to stop services frequently within a month, for example in development or test environments. If you intend to use services throughout the month, monthly billing is more suitable.

You won’t be asked about hourly or monthly billing if you have a nonmetered subscription or subscribe to Oracle’s Universal Credits program.

• **Which compute shape do you think you’ll need?**

Oracle Analytics Cloud - Classic offers a set of compute shapes that are optimized for different scenarios. Choose from a set of all-purpose and memory-intensive shapes. The larger the compute shape, the greater the processing power. For more information about the compute shapes and considerations for selecting the shape that is right for your environment, see About Shapes in Using Oracle Cloud Infrastructure Compute Classic.

All-purpose compute shapes include:
– OC4: 2 OCPUs and 15 GB memory
– OC5: 4 OCPUs and 30 GB memory
– OC6: 8 OCPUs and 60 GB memory
– OC7: 16 OCPUs and 120 GB memory
– OC8: 24 OCPUs and 180 GB memory
– OC9: 32 OCPUs and 240 GB memory

Memory-intensive compute shapes include:
– OC1M: 1 OCPUs and 15 GB memory
– OC2M: 2 OCPU and 30 GB memory
– OC3M: 4 OCPUs and 60 GB memory
– OC4M: 8 OCPUs and 120 GB memory
– OC5M: 16 OCPUs and 240 GB memory

You can change the compute shape after creating the service, if the needs of your business change.

• **Which identity management system can I use?**

  – **Oracle Identity Cloud Service**
    
    Use Oracle Identity Cloud Service if you subscribe to Oracle Analytics Cloud - Classic through Oracle Universal Credits. Oracle Identity Cloud Service Foundation is automatically provided with your subscription.
    
    If you want to use single sign-on with Oracle Identity Cloud Service, you need Oracle Cloud Infrastructure Load Balancing Classic.

  – **WebLogic Embedded LDAP Server**
    
    Use WebLogic Embedded LDAP Server if you have a traditional metered or nonmetered subscription to Oracle Analytics Cloud - Classic. When you create your service, you must provide credentials for the Oracle Analytics Cloud administrator:
    
    * User name must start with a letter and can contain up to 25 characters.
    * Passwords must be at least 8 characters and contain at least one non-alphabetic character. Only these special characters are allowed: underscore _, hyphen -, pound sign #, open bracket (, close bracket )

    **Note:**
    
    If you use the embedded LDAP server:
    
    * You can’t scale out your service.
    * You can’t associate your service with Oracle Big Data Cloud.

• **What name do you want to for this service?**

  – Must contain between 1 and 50 characters.
  – Must start with an ASCII letter: a to z or A to Z.
  – Must contain only ASCII letters or numbers.
  – Must not contain any other special characters.
  – Must be unique within the identity domain.

• **Which Database Cloud Service do you want the service to use?**

  Oracle Analytics Cloud - Classic uses a Database Cloud Service to store various Oracle Analytics Cloud - Classic schemas and data. If your Database Cloud Service isn’t set up, you must do that first. See Create a Customized Database Deployment in *Administering Oracle Database Cloud Service*.

  Oracle Analytics Cloud - Classic doesn't support Oracle Database 18c, non-UTF databases, or Real Application Clusters (RAC) databases.

  When you create services with Oracle Analytics Cloud - Classic, you must specify the cloud database you want to use and other information about the database.
– **Database Administrator User Name** must be SYS or another user with SYSDBA privileges.

– **Database Administrator Password** must not start with a number or a special character, or contain the @ character. Only these special characters are allowed: $ # _

– **PDB** or **SID** associated with the database. For Oracle 12c databases, the name of the pluggable database (PDB). For Oracle 11g databases, the SID associated with the database.

– **Region** and **Availability Domain** on Oracle Cloud Infrastructure Compute Classic in which the database is deployed.

– **IP Network** in which the database is deployed, if specified.

  * Is the load balancer associated with the IP network public or private?

**Do you want to create your own public/private key pair for SSH access?**

You can ask the Create Service wizard to create a public/private key pair for you, or you can create one beforehand, using a standard SSH key generation tool such as OpenSSH, and upload or paste its public key value.

**Which storage container do you want to use for analytics data sets and backups?**

You can create the container beforehand or ask the Create Service wizard to create a container for you. Either way, you need to provide some information.

  – Name and URL of the container.

    Container names support UTF-8 characters. Some special characters aren’t allowed: /, ', "`, `<, and >.

  – User name and password of a user, defined in My Services, with storage administration permissions and read/write access to the container.

    Oracle Cloud Infrastructure Object Storage Classic user names must be between 2 to 50 characters and only contain letters and numbers.

If you want to create the container yourself, ensure that the container is empty and dedicated to a single Oracle Analytics Cloud - Classic service. See Create Containers in *Using Oracle Cloud Infrastructure Object Storage Classic*.

If you haven’t done so already, you must set an appropriate replication policy for your storage service. You must do this before you set up Oracle Database Cloud Service or Oracle Analytics Cloud - Classic.

**Do you want to integrate Oracle Analytics Cloud - Classic with Oracle Big Data Cloud?**

Subscribers to Oracle Big Data Cloud can analyze their big data in Oracle Analytics Cloud - Classic. Enter connection details as you create your service, if you want to enable Single-Sign On (SSO) between Oracle Analytics Cloud - Classic and your Oracle Big Data Cloud service. You need to know:

  – Name of your Oracle Big Data Cloud.

  – Administrator password for Oracle Big Data Cloud.

To use this feature:

  – **Billing**: Oracle Universal Credits

- **Service**: Self-Service Data Visualization, Preparation and Smart Discovery or Enterprise Data Models
- **Identity management**: Oracle Identity Cloud Service
- **Oracle Big Data Cloud**: Version 2.1 or later

- **Do you want to scale out your service from the start?**

  By default, services are deployed with a single *analytics server* (or compute node). You can increase the number of analytics servers available to your service, up to a maximum of 10, to meet your specific performance requirements. If you’re not sure, you don’t have to decide now. You can always scale out your service later on if your service requires additional resources.

  If you want to scale out, you need Oracle Cloud Infrastructure Load Balancing Classic.

  To use this feature:
  - **Billing**: Oracle Universal Credits
  - **Service**: Self-Service Data Visualization, Preparation and Smart Discovery or Enterprise Data Models
  - **Identity management**: Oracle Identity Cloud Service

**Create a Service**

Use My Services to create a service with Oracle Analytics Cloud - Classic.

1. Sign in to My Services, and click **Dashboard**.
2. Go to the **Analytics Classic** tile, click the **Action Menu** and select **Open Service Console**.

   If a Welcome page displays, click **Go to Console**.
3. Click **Create Instance**.
4. On the Instance page, enter a unique name for the service, and a description.

5. Enter an email address where you would like a service creation notification and other service-related information to be sent.

6. Select the region where you want to deploy the service and whether you want to use a custom IP network.

   You must deploy Oracle Analytics Cloud - Classic in the same region and availability domain as the database service that you set up to store Oracle Analytics Cloud - Classic schemas.

   The database service you want to use doesn't have to be deployed on the same IP network as Oracle Analytics Cloud - Classic. If you decide to deploy Oracle Database Cloud Service and Oracle Analytics Cloud - Classic on different IP networks, you must remember to create an IP network exchange that enables communication between the two IP networks.

   a. Select the same Region and Availability Domain as the database service you set up for Oracle Analytics Cloud - Classic.

   b. (Optional) If the database you set up for Oracle Analytics Cloud - Classic is deployed on an IP network, select the name of that network from the IP Network list.

      If you want to deploy Oracle Analytics Cloud - Classic on a different IP network, ensure that the IP network you select has access to the database through an IP network exchange.

   c. (Optional) Select Assign Public IP if you want any node created for this service to have a public IP address. If you scale out your service in the future, those added nodes are assigned public IP addresses. When you select this option, you see options for reserving IP addresses on the next page.

      If you deselect this option, none of the nodes associated with this service can have public IP addresses.

      This option is available only if you select an IP network.

7. Click Edit to specify the SSH Public Key to use for authentication when using an SSH client to connect to a compute node that is associated with your service.

   a. If you have an existing public key, click Browse to select the file that contains the public key or select Key Value and paste its value, and then click Enter. If you paste in the value, make sure the value doesn’t contain line breaks or end with a line break.

   b. To generate a new public and private key pair, click Create a New Key, and then click Enter.

      Click Download to save the public and private key pair locally, and then click Done. You can use the private key to connect to a compute node that is associated with this service.

     You can change the public key value for your service when it’s up and running whenever you want.

8. For License Type, select whether you want to use your on-premises license with Oracle Analytics Cloud - Classic (and to be charged the Bring Your Own License rate) or subscribe to a new license for Oracle Analytics Cloud - Classic.


10. (Traditional metered subscriptions only). Select a frequency for metered billing.
• **Hourly**—Pay only for the number of hours used during your billing period.

• **Monthly**—Pay one price for the full month irrespective of the number of hours used.

  For services that start in the middle of a month, the price is prorated. You pay only for the partial month from the start date.

You can’t switch from hourly to monthly or from monthly to hourly billing after you’ve created the service. If you expect to stop services frequently within a month, for example in development or test environments, you might select hourly billing. If you intend to use services throughout the month, select monthly billing.

11. Click **Next**.

12. In the Identity Management section, specify how user accounts are managed for this service.

   • **Select Enable IDCS and Load Balancer** to use Oracle Identity Cloud Service. Always use this if you subscribe to Oracle Analytics Cloud - Classic through Oracle Universal Credits. Oracle Identity Cloud Service Foundation is automatically provided if you subscribe to Oracle Analytics Cloud - Classic through Oracle Universal Credits.

   If you enable Oracle Identity Cloud Service and chose to deploy Oracle Analytics Cloud - Classic on an IP network (in the previous screen), you must specify whether the load balancer associated with your selected IP network is public or private.

   – **Select Public Load Balancer** if the load balancer on the IP network is public, that is, accepts traffic from the internet.

   – **Deselect Public Load Balancer** if the IP network uses a private load balancer. Private load balancers are only visible within your virtual cloud network (VCN).

   If you’re not sure contact your network management team.

   • **Deselect Enable IDCS and Load Balancer** to use the WebLogic embedded LDAP server. Always use this if you subscribe to Oracle Analytics Cloud - Classic through a traditional metered or unmetered subscription.

   In the Service Administrator section, enter a user name and password for the WebLogic embedded LDAP server administrator.

13. In the Options section, select the type of service you want to create.

   a. Select the features you want to offer.

      • **Self-Service Data Visualization, Preparation and Smart Discovery**

      • **Enterprise Data Models — BI**

      • **Collaborative Data Collection, Scenarios and What-if Analysis — Essbase**

      Select only one type of service. If you select **Enterprise Data Models**, you automatically get **Self-Service Data Visualization, Preparation and Smart Discovery**. If you need help to decide, see Features of Oracle Analytics Cloud in *Getting Started with Oracle Analytics Cloud*.

   b. Select a size and shape for the compute node.
If you’re not sure about your final requirements, select the minimum OCPUs as you can scale up later if required.

c. Enter the usable storage or accept the default.

**Total Storage on Disk** is the default system and data storage the service uses.

d. (Optional) Click the Plus icon if you want to allocate specific IP addresses to the nodes created for this service.

IP addresses are assigned automatically, by default.

14. In the Cloud Storage Configuration section, specify the container where you want to store any analytics data sets that users upload, and backups for this service.

a. Enter the REST endpoint URL for the container you want to use.

• If you specify the name of an existing container, you must ensure the container is empty and used only by this service.

• If you want to create a container with the name that you specify here, you must select the check box **Create Analytics Storage Container**.

Use the format:

https://domain-storage.oraclecloud.com/v1/Storage-domain/ContainerName

For example: https://example-storage.oraclecloud.com/v1/Storage-example/myoacstoragecontainer

To find the REST endpoint URL, go to the **Storage Classic** tile on your My Services dashboard, click the **Action Menu** and select **View Details**. The **REST Endpoint** value for your storage service is displayed under **Additional Information**. Copy the REST endpoint and append this value with a forward slash and the name of the container you want to use, for example: <Rest Endpoint value>/<ContainerName>

b. Enter the user name and password of a user with read and write access to Oracle Cloud Infrastructure Object Storage Classic.

c. Optional: If the container you specified doesn’t exist yet, select **Create a Cloud Storage Container**.

15. Optional: Define a public storage container so users can share their data visualizations.

You don’t have to define a public container now. You can set up a public container later when your service is up and running. After you define the container, users will see the menu option that enables them to share their data visualizations.

> **Note:**

This step doesn’t apply when you select the option **Collaborative Data Collection, Scenarios and What-if Analysis — Essbase**.

a. Select **Configure storage container for sharing data**.

b. Enter the **Shared Storage Container URL**.
Specify the container you want to use to share content. The container must be set up as a public container, that is, a container with global read access. Use the REST endpoint URL format:

https://domain.storage.oraclecloud.com/v1/Storage-domain/
ContainerName

For example: https://example.storage.oraclecloud.com/v1/Storage-example/mypubliccontainer

To find the REST endpoint URL for the storage container, go to the Storage Classic tile on your My Services dashboard, click the Action Menu and select View Details. The REST Endpoint value for the service is displayed under Additional Information. Copy the REST endpoint and append this value with a forward slash and the name of the public container you want to use, for example: <Rest Endpoint value>/<PublicContainerName>

c. Enter the user name and password of a user with read and write access to the public container.

d. If the container you specified doesn't exist yet, select Create Shared Storage Container.

16. In the Database section, select the database cloud service where you want Oracle Analytics Cloud - Classic to store its schemas and data.

a. Select the name of the database you want to use.

b. For PDB/SID, enter the name of the pluggable database (PDB) or SID associated with the database.

For Oracle 12c databases, provide the name of the pluggable database. For Oracle 11g databases, provide the SID.

> Note:

Oracle Analytics Cloud - Classic doesn't support Oracle Database 18c, non-UTF databases, or Real Application Clusters (RAC) databases.

c. For Database Administrator Username, enter SYS or another user with SYSDBA privileges, and then enter the password for this administrator.

17. Optional: In the Associations section, select Big Data Cloud Service if you want to integrate Oracle Analytics Cloud - Classic with an existing big data service. Select the name of the service you want to connect to and the administrator password for that big data service.

This option is available only with Essbase Edition and Enterprise Edition, if you select the Oracle Analytics Cloud option Self-Service Data Visualization, Preparation and Smart Discovery or Enterprise Data Models, and enable Oracle Identity Cloud Service (Enable IDCS and Load Balancer).

18. Optional: In the Service Administrator section, increase the Number of Analytics Servers, if required. The default value is 1.

You don't have to scale out now if you're not sure. You can scale out (and scale in) at any time.

This option is available only if you select the Oracle Analytics Cloud option Self-Service Data Visualization, Preparation and Smart Discovery or Enterprise
Data Models, and if you enable Oracle Identity Cloud Service (Enable IDCS and Load Balancer).

19. Click Next.

20. Verify the information you provided, and then click Create.

It takes 45–60 minutes to create the service. When the service is ready, a notification email is sent to the email address that you nominated earlier. To check the current status, go to the Oracle Analytics Cloud - Classic dashboard and check for status messages under Create and Delete History.

Oracle Analytics Cloud - Classic makes two attempts to create the service. If service creation fails after the second attempt, log files are copied to the storage container that you nominated for the service. To find out what went wrong, go to the Storage Classic page in My Services, locate the container, and open the service_provisioning folder. Expand the ZIP file and look for any issues recorded in the logs.

- For BI and Data Visualization services, look at setupBICS.log.
- For Essbase services, look at continue-service-start-essbase.log.

Migrate to Oracle Analytics Cloud - Classic from Other Environments

You can migrate content from other cloud and on-premises environments to Oracle Analytics Cloud - Classic.

<table>
<thead>
<tr>
<th>Migrate From…</th>
<th>More Information</th>
</tr>
</thead>
</table>
| Oracle Analytics Cloud - Classic deployed on Oracle Cloud Infrastructure Classic | • **BI Enterprise and Data Visualization services**: See Migrate Oracle Analytics Cloud Using Snapshots in Preparing Data in Oracle Analytics Cloud.  
• **Essbase services**: See Migrate Cloud Service Applications in Using Oracle Analytics Cloud - Essbase. |
| Oracle Analytics Cloud deployed on Oracle Cloud Infrastructure | • **BI Enterprise and Data Visualization services**: See Migrate Oracle Analytics Cloud Using Snapshots in Preparing Data in Oracle Analytics Cloud.  
• **Essbase services**: See Migrate Cloud Service Applications in Using Oracle Analytics Cloud - Essbase. |
| Oracle BI Enterprise Edition 12c | • **BI Enterprise services**  
Migrate data models, dashboards and analyses, and application roles. See Migrate Snapshots from Oracle BI Enterprise Edition in Preparing Data in Oracle Analytics Cloud.  
Migrate data models. See Migrate Data Models from Oracle BI Enterprise Edition in Preparing Data in Oracle Analytics Cloud.  
Migrate catalog objects, such as dashboards and analyses. See Migrate Catalog Content from Oracle BI Enterprise Edition in Visualizing Data and Building Reports in Oracle Analytics Cloud. |
| Oracle BI Enterprise Edition 11g | • **BI Enterprise services**: See Migrate Oracle BI Enterprise Edition 11g in Preparing Data in Oracle Analytics Cloud. |
Migrate LDAP-Based Services to Oracle Identity Cloud Service

You can use Oracle Identity Cloud Service if you subscribe to Oracle Analytics Cloud - Classic using Oracle Universal Credits. If you have an existing service that uses WebLogic embedded LDAP server for identity management, you can use various export and import utilities to migrate your artifacts to another Oracle Analytics Cloud - Classic environment that uses Oracle Identity Cloud Service.

Topics:

- Migrate BI Content and Users
- Migrate Essbase Applications and Users

Migrate BI Content and Users

If you have Oracle Analytics Cloud - Classic services that use the WebLogic embedded LDAP server, you can export everything (including data visualizations, reports, dashboards, user information, and so on) and import them to a new environment enabled with Oracle Identity Cloud Service (IDCS).

Steps

- Create a New Service with Oracle Identity Cloud Service Enabled
- Export Content from the Service using Embedded LDAP Server
- Import Content to the New Service using IDCS

Create a New Service with Oracle Identity Cloud Service Enabled

Oracle Identity Cloud Service Foundation is automatically provided when you subscribe to Oracle Analytics Cloud - Classic through Oracle Universal Credits. Creating a service that integrates with Oracle Identity Cloud Service is easy. When you create the service, you select the option Enable IDCS and Load Balancer.

Note:

Oracle Identity Cloud Service is only available through Oracle Universal Credits.

Export Content (BI Services)

Start your migration to Oracle Identity Cloud Service by exporting everything from the source service to your local file system. First you upload the migration scripts, and
then you export snapshots, data sets, users, and groups. The source service must use an embedded WebLogic LDAP server.

- Export snapshots of your environment.
- Export users and groups.

To export content from the source service:

1. Export a snapshot of your environment:
   a. Sign in to the source service.
   b. Click Console, and then click Service Administration.
   c. Click Manage Snapshots, and then click Create Snapshot.
      Name the snapshot Final snapshot before migration or something similar.
   d. Select the content you want to include, Everything or Custom.
      - **Everything** - Include everything about your environment in the snapshot.
      - **Custom** - Select only the content types you want to save in the snapshot. Deselect any items that you don't want.
   e. Download this final snapshot to your local file system. Select the snapshot, click Snapshot Actions menu, and then click Download.
   f. Enter and confirm a password for the snapshot.
      The password must contain at least 8 characters. Don’t forget this password. You'll be asked for this password when you upload the snapshot on the target service.
   g. Download any other snapshots you want to migrate or keep on your local file system.

2. Export users and groups. Run the `wls_ldap_csv_exporter` script:

   ```bash
   $ /bi/app/public/bin/wls_ldap_csv_exporter -u weblogic_admin_user -c oracle_common_folder_path -D output_dir
   ```

   Typically, `oracle_common_folder_path` is the folder `/bi/app/fmw/oracle_common`.

   This script creates two CSV files, one CSV file contains users and the other contains groups. There is also a log file, which describes any invalid or incompatible records that Oracle Identity Cloud Service won’t understand.
   - Everyone has a default password.
   - Oracle Identity Cloud Service doesn't support group memberships, that is, where a group is member of another group. Such records are discarded from the group CSV file and mentioned in the log file.
   - Oracle Identity Cloud Service requires several mandatory parameters for users: User ID, Last Name, First Name, Password, Work Email. Oracle Identity Cloud Service won't import user records if parameters are missing.

3. Prepare both CSV files for Oracle Identity Cloud Service. Make sure the CSV files contain all the information Oracle Identity Cloud Service requires.
   a. Review the log file for information about invalid or incomplete records.
   b. Review the users CSV file, and ensure the information is complete.
c. Repeat for the groups CSV file.

Import Content (BI Services)

After exporting all your content from a service that uses the embedded LDAP, you use migration scripts to import the content on the target service. The target service must be set up to use Oracle Identity Cloud Service.

• Import snapshots of the source service
• Import users and groups

To import your content:

1. Upload snapshots of the source service:
   a. Sign in to the target service.
   b. Click Console, and then click Service Administration.
   c. Click Manage Snapshots, click the Page menu, and then select Upload Snapshot.
   d. Use Select to navigate to the folder where you downloaded snapshots for migration.
   e. Select the final snapshot that you took before migration.
   f. Enter the snapshot password, and click OK.
      You'll see a snapshot named Final snapshot before migration or something similar.
   g. Upload any other snapshots that you exported and want to keep on the target service.

2. Restore the most recent snapshot:
   a. Select the final snapshot, click the Actions menu, and then click Restore.
   b. Select the Restore option you want.
      For example, you may not want to include application roles if you're restoring a snapshot taken from a pre-production service, to a production service. Pre-production roles often have different members to the production service. If so, select Custom and deselect Application Roles before you restore.
      • Replace Content Snapshot Only - Restore only the content inside the snapshot. Any content types that are missing from the snapshot remain unchanged.
      • Replace Everything - Overwrite all your existing content. Replace your existing content with the content included in this snapshot (listed in the description field). Any content types not included in the snapshot, excluding file-based data sets, plug-ins and extensions, are removed and restored with default values.
      • Custom - Select only the content types you want to restore. You can restore with content saved inside the snapshot or restore your content with default settings. If you don't want to restore everything, deselect all the items you want to keep.
   c. Click Restore, and then Yes to continue.
The time it takes to restore your system depends on the size of your snapshot. After the restore completes, you might need to wait a few more minutes for the restored content to refresh through your system.

d. Sign out.

3. Import users from the CSV file you exported earlier:
   a. In Oracle Identity Cloud Service console, click **Users**, then **Import**.
   b. Click **Browse** to locate the CSV file that contains user account information.
   c. Click **Import**.

   See Import User Accounts in *Administering Oracle Identity Cloud Service*.

4. Import groups from the CSV file you exported earlier.
   a. In Oracle Identity Cloud Service console, click **Groups**, then **Import**.
   b. Click **Browse** to locate the CSV file that contains group account information.
   c. Click **Import**.

   See Import User Accounts in *Administering Oracle Identity Cloud Service*.

5. Sign in to the target service.

6. Activate scheduled deliveries (if any).
   a. Click **Console**, and then click **Service Administration**.
   b. Click **Monitor Deliveries**, click the **Actions** menu, and then click **Restore Deliveries**.
   c. To activate a delivery, select **Enable Delivery** from the Actions menu.

   See Restore and Enable Delivery Schedules.

7. Verify everything migrated as you expected.

---

**Migrate Essbase Applications and Users**

You can migrate applications and users from Oracle Analytics Cloud – Essbase services from v17.3.3 (or earlier) to the latest version, using scripts.

You can use the scripts in this section to import Essbase applications, users and groups when you install a new Essbase service version.

**Prerequisites**

---

**Note:**

- Oracle Identity Cloud Service (IDCS) requires that user fields aren’t empty. If you’re enabling IDCS, then in your existing Essbase services and prior to migrating your data, open the Security tab and ensure that all user data fields (including ID, name, email, and role) contain values and aren’t empty.

- When you export applications, the target file is overwritten. If you want to save the previous version of an LCM exported application, rename it or run the export script with another file name.
Before you migrate applications and users, copy the following scripts from the older Essbase service version to the latest version, at the same file location. You can check first whether they already exist on the new host:

- /u01/app/oracle/tools/acss/BI/esscs_tools/lcm/esscs_lcm.py
- /u01/app/oracle/tools/acss/BI/esscs_tools/lcm/idcs_users.py
- /u01/app/oracle/tools/acss/BI/esscs_tools/lcm/ldap_users.py
- /u01/app/oracle/tools/acss/BI/esscs_tools/lcm/user_group.py
- /u01/app/oracle/tools/acss/BI/esscs_tools/public/essbase_export.sh
- /u01/app/oracle/tools/acss/BI/esscs_tools/public/essbase_import.sh

**Export Script Location**

/bi/app/public/bin

To run the export script, see Run Administration Scripts.

**Export Syntax**

```
essbase_export.sh filename
```

Where:

- **filename**: Full path to the tar archive file that stores all Essbase applications, CSV files of users and groups, and files of settings.

**Import Script Location**

/bi/app/public/bin

To run the import script, see Run Administration Scripts.

**Import Syntax**

```
essbase_import.sh filename
```

Where:

- **filename**: Name of the tar created by the export script.
Manage Services

When Oracle Analytics Cloud is up and running, you can monitor and manage the services you’ve created through Oracle Cloud My Services.

Topics:
- View and Manage Services
- Monitor Services
- Delete a Service
- Start, Stop and Restart Services
- Back Up a Service
- Restore a Service
- Patch and Roll Back
- Scale Services

Typical Tasks to Manage a Service

Here are the common tasks you will perform as Oracle Analytics Cloud - Classic administrator.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>View and manage services</td>
<td>Access all your services you created with Oracle Analytics Cloud - Classic from My Services.</td>
<td>View and Manage Services</td>
</tr>
<tr>
<td>Monitor services</td>
<td>Check on the day-to-day operation of Oracle Analytics Cloud - Classic, monitor performance, and review important metrics and notifications.</td>
<td>Monitor Services</td>
</tr>
<tr>
<td>Delete a service</td>
<td>Delete services you don't need anymore to free up resources.</td>
<td>Delete a Service</td>
</tr>
<tr>
<td>Start, stop and restart cloud services</td>
<td>Stop services to temporarily prevent access. Start or restart services whenever you want.</td>
<td>Start, Stop and Restart Services</td>
</tr>
<tr>
<td>Back up a service</td>
<td>Take regular backups in case you need to restore earlier content.</td>
<td>Back Up a Service On Demand</td>
</tr>
<tr>
<td>Restore a service</td>
<td>Restore your service from a backup.</td>
<td>Restore a Service</td>
</tr>
<tr>
<td>Patch a service</td>
<td>Apply a patch or roll back a patch.</td>
<td>Patch and Roll Back</td>
</tr>
<tr>
<td>Scale service resources</td>
<td>Change the shape, CPU allocation, storage, and add nodes to meet new demands.</td>
<td>Scale Services</td>
</tr>
</tbody>
</table>
View and Manage Services

You can view information about services and perform various administration tasks Oracle Analytics Cloud - Classic from My Services.

2. Click the navigation menu, and then select **Analytics Classic**.
3. Click a service instance to view additional properties and perform various actions on that service.
4. Click the **Manage this instance** icon or the page tabs to explore all the options available.

Monitor Services

You can use Oracle Analytics Cloud - Classic metrics to monitor the performance of your services.

Topics:

- **About Oracle Analytics Cloud - Classic Metrics**
- **Run a Health Check**

About Oracle Analytics Cloud - Classic Metrics

You'll find status and performance information for Oracle Analytics Cloud - Classic in My Services.

**Instance Metrics**

On the **Instances** tab for Oracle Analytics Cloud - Classic, you'll find a summary of metrics for the service instances, including the number of CPUs, memory used, storage used, and more.

You can also see metrics on the Services tab per service instance: subscription billing type, product version, service instance creation date, number of CPUs, and memory and storage sizes.

If you click the service instance name, you can see detailed service instance metrics, public IP addresses, resources, load balancer details, associated services, and operation messages.

- The Instance Overview pane displays a variety of component, storage, and resource details, including the infrastructure of the database, storage and backup services that supports this service instance are displayed. When you expand Associations, you can also see Database Cloud Service details and status.
- The Administration pane displays the quantity of storage cloud volumes and backup volumes used, backup and restore history, and available patches.

**Activity Metrics**

On the **Activity** tab, you can view recent lifecycle management activities performed for a service, during a specified time range.
Run a Health Check

Monitoring information is updated automatically. You can also run a health check to update the display of monitoring information at any time.

1. In the My Services dashboard, navigate to Analytics Classic.
2. On the Overview pane, click the **Display monitoring information** icon to update the information displayed.
3. In the Resources section, click the **View Healthcheck Details** icon. Healthcheck details are displayed.

Delete a Service

You can delete services you created but don't need anymore.

1. In the My Services dashboard, navigate to Analytics Classic.
2. Click the **Manage the service** icon for the service you want to delete.
3. Select **Delete**, enter your database administration credentials, and then click **Delete** again to confirm.
   
   Select **Force service deletion** if you want to delete a service, regardless of whether there are processes running and any other warnings and messages you might see.

   **Note:**

   The **Force service deletion** option doesn't delete the schemas created for the service in Oracle Database Cloud Service. This is the cloud database you specified when you created the service. You must manually delete these schemas.

Start, Stop and Restart Services

You can start, stop and restart service from the Oracle Analytics Cloud - Classic dashboard. in My Services

1. In the My Services dashboard, navigate to Analytics Classic.
2. Select **Manage the service** for service you want to start, stop or restart.
3. Select the action you want to perform.
   
   • Select **Start** to start the service.
   • Select **Stop** to stop the service.
   • Select **Restart** to restart the service.

   Alternatively, click the icon for **Start Service**, **Stop Service**, or **Restart Service** on the Overview pane.
Back Up a Service

Back up Oracle Analytics Cloud - Classic regularly so you can restore your service if something goes wrong.

Topics:
- Schedule Regular Backups
- Back Up a Service On Demand
- Disable and Enable Backups

Schedule Regular Backups

You can schedule regular backups for your service. Service backups are saved to your cloud storage, and contain all the artifacts required to restore your service.

1. In the My Services dashboard, navigate to Analytics Classic.
2. Click the name of the service you want to schedule backups for.
3. Click Administration.
4. The Backup tab shows your current cloud storage and backup storage usage, available backups, and restore history.
5. Click Manage backups for this instance, and then click Configure Backups.
6. Set up a suitable schedule for weekly backups. For Full Backup, set the day and time you want weekly backups to start.
   By default, the first backup starts 12 hours after you create the service (to the nearest five-minute interval). For example, if you create a service at 1:01 PM on a Monday, weekly backups are initiated at 1:00 AM on Tuesdays.
7. Set up a suitable schedule for daily backups. For Incremental Backup, set the time you want daily backups to start.
   Incremental backups are initiated every day except the day when full backups are initiated. For example, if you create a service at 1:01 PM on a Monday, by default, incremental backups are initiated at 1:00 AM every day except Tuesdays.
   For Oracle Analytics Cloud - Classic, the content included in full and incremental backups is exactly the same.
8. Optional. Change the length of time that backups are stored.
   a. Click Manage backups for this instance.
   b. Select Configure Backups.
   c. In the Set new retention period to field, specify the number of days you want to keep backups.

Back Up a Service On Demand

You can back up your service whenever you want. Service backups are saved to your cloud storage and contain all the artifacts required to restore your service.
1. In the My Services dashboard, navigate to Analytics Classic.

2. Click the name of the service you want to back up.

3. Click **Administration**.

   The Backup tab shows your current cloud storage and backup storage usage, available backups, and restore history.

4. Click **Manage backups for this instance**️, and then click **Backup Now**.

   When completed successfully, details about your on-demand backup are displayed.

5. Optional. Change the length of time that backups are stored.
   
   a. Click **Manage backups for this instance**️
   
   b. Select **Configure Backups**.
   
   c. In the **Set new retention period to** field, specify the number of days you want to keep backups.

### Disable and Enable Backups

If no one is using your service, you can temporarily disable backups using the Oracle Analytics Cloud - Classic CLI command `update-backup-config`. When you disable backups, you can't take an on-demand backup and scheduled backups are canceled. All your existing backups are preserved in case you need them.

1. Run the CLI command `psm analytics update-backup-config`.

   For help with that command, run the command with the `-h` option. See Use the Command Line Interface in *PaaS Service Manager Command Line Interface Reference*.

2. To disable backups, set the `backups` parameter to **DISABLE**.

   For example: "backups":"DISABLE"

3. To enable backups, set the `backups` parameter to **ENABLE**.

   For example: "backups":"ENABLE"

   See analytics update-backup-config in *PaaS Service Manager Command Line Interface Reference*.

### Restore a Service

You can restore your service from a backup.

The service backup must be from the same Oracle Analytics Cloud - Classic version as the service you want to restore.

> **Note:**

If you scaled-out your service and a node fails during the restore process, then you must scale-in the failed node, complete the restoration, and then scale-out the node again.
1. In the My Services dashboard, navigate to Analytics Classic.
2. Click the name of the service you want to restore.
3. On the Services tab, select Administration.
   You can see the quantity of cloud storage and backup used, as well as monitor available backups and restore history.
4. Click the Manage this service icon for the backup you want to restore, and click Restore.
5. Enter some notes to remind yourself why you're restoring the service, and click Restore.
   When the restore process completes, you see the details of the last successful restore process in the Restore History section.

If your service uses the WebLogic embedded LDAP server and you recently changed the administrator password, your backups might not contain the latest password. If this is the case when you restore your service, the administrator password reverts to the password in the backup.

**Patch and Roll Back**

A text notification is displayed on the Oracle Analytics Cloud - Classic dashboard when patches become available. You can view and apply patches for individual services. You can also see what patches have been applied, and roll back to an earlier patch.

**Topics:**
- Apply the Latest Patch to BI Services
- Apply the Latest Patch to Essbase Services
- Roll Back a Patch to an Earlier Version

**Apply the Latest Patch to BI Services**

The latest patch is 105.1.0.x. Check these FAQs to see whether or not you need apply this patch.

My Service Uses Oracle WebLogic Embedded LDAP Server. After Patching My Service Can I Use Oracle Identity Cloud Service?

No. If your service uses Oracle WebLogic Embedded LDAP Server for identity management, your service continues to use the same LDAP server after you apply the latest patch.

You can use Oracle Identity Cloud Service if you subscribe to Oracle Analytics Cloud - Classic through Oracle Universal Credits. Oracle Identity Cloud Service Foundation is automatically provided with your subscription. If you do subscribe through Oracle Universal Credits and have existing services that use Oracle WebLogic Embedded LDAP Server, Oracle recommends that you create a brand new service enabled with Oracle Identity Cloud Service and migrate your users and content to the new service. See Migrate BI Content and Users.
Can I Use the Pixel-Perfect Reporting (Oracle BI Publisher) Feature After Patching My Service?

In most cases, Yes. If you have a traditional metered subscription, applying this patch doesn’t expose features for pixel-perfect reporting in your existing service. In this case, you must create a new service with the option Enterprise Data Models, and migrate any information that you want to keep from your existing service. See Create a Service and Migrate BI Content and Users.

Several Patches Are Available. Which Patch Do I Apply?

Check the table to see whether you need apply the latest patch. If you do, you must perform important tasks both before and after you apply the patch.

<table>
<thead>
<tr>
<th>Your Current Version</th>
<th>Apply Patch?</th>
<th>Patch Version</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.4.5 to 18.3.3</td>
<td>Yes</td>
<td>105.1.0.x</td>
<td>Apply the latest patch.</td>
</tr>
<tr>
<td>105.1.0.x</td>
<td>No</td>
<td>-</td>
<td>You have the latest version.</td>
</tr>
</tbody>
</table>

Topics:
- Before You Patch a BI Service
- Apply the Latest Patch to a BI Service
- After You Patch a BI Service

Before You Patch a BI Service

Before you patch a BI service to the latest version, you must complete some prerequisite steps.

1. Always take a snapshot of your service before you apply a patch.
   a. Sign in to Oracle Analytics Cloud, and navigate to Console.
   b. Click Service Administration, then Manage Snapshots.
   c. Click Create Snapshot.
   d. Enter a short description, for example: Before Patch 105.1.0.x 1st January 2019.

2. Sign in to My Services.

3. Verify that you have enough resources before you apply the patch.
   Oracle recommends 230 GB, that is, 130 GB latency, and 100 GB data.
   If required, scale up the compute shape or add more storage.

4. In My Services, back up the database associated with your service.
   a. Open the Database dashboard and navigate to the database cloud service.
      If you need to confirm the exact database service, open the Oracle Analytics Cloud - Classic dashboard and navigate to your service where its database information is displayed.
   b. Back up the database. Click the Administration tile, then Back up Now.
5. Restart your service before you patch. If you made any changes or customizations on the compute node associated with your service you must restart your service before you patch.

6. Sign in to your service to verify that your service up and running, and ready to be patched.

Now you're ready to patch your BI service.

Apply the Latest Patch to a BI Service

Patches for your service are rolled out periodically. Oracle recommends that you apply the most recent patches promptly. Delaying patches could cause your service to be unsupported for future patching and upgrade. Before you patch, you can run a precheck to identify potential problems, such as insufficient disk space storage.

Most patching operations are rolling operations, so your service continues to function with very little interruption during the patch process. The patching operation shuts down one node at a time and applies the patch. After a node is patched, it's automatically restarted. The load balancer automatically detects that a node is down and doesn't send requests to that node. The other nodes process requests without interruption. The patching operation continues patching nodes until all nodes are patched. For example, if you have a two-node cluster, one node keeps running while the other is being patched.

1. Complete the prerequisite before you patch steps.

2. Sign in to My Services, click Dashboard, and navigate to Analytics Classic.

3. Click the name of the service you want to patch.

4. On the Services tab, select Administration.

   On the Patching tab, you can view available patches, run a patch, and view patch installation and rollback history.

   Patches are cumulative, that is, the latest patch includes all the updates included in previous patches. The latest patch is 105.1.0.x

5. To check a patch before running it, click the Manage this service icon for the patch, and click Precheck.

   Upon completion, click Precheck summary link to view ramifications or possible conflicts due to running the patch.

6. If required, correct the database administrator (DBA) credentials for the database.

   If you changed the DBA credentials after setting up the service or after the last patch, the precheck fails with a message telling you that the stored credentials are incorrect.

   a. Connect to the compute node for your service using the ssh utility:

      $ ssh -i private-key-file-location opc@node-ip-address

   b. Change to the oracle user.

      sudo su oracle

   c. Run the script /bi/app/public/bin/store_dba_credentials.

      When prompted, enter the database administrator user name 'SYS as SYSDBA' and then enter the password for the SYS user. For example:
store_dba_credentials 'SYS as SYSDBA' 'mydbadminpassword'

d. Exit the compute node.

It's important that you log out from your ssh session.

7. To apply a patch, click the Manage this service icon for the patch you want to apply, and click Patch.

Upon successful completion, a notification is displayed. The completed patch is listed in the Patch and Rollback History section.

8. If the patch succeeds, complete the postpatch steps.

9. If the patch fails, your service remains at the previous version.

After You Patch a BI Service

After patching a BI service to the latest release you must restore the settings and snapshots that you saved earlier.

1. Sign in to your service, and click Console.

2. Activate scheduled deliveries (if any).
   a. In Console, click Service Administration, then Monitor Deliveries.
   b. Click Restore Jobs.
   c. To activate a delivery, select Enable Delivery from the Actions menu.

See Restore and Enable Delivery Schedules.

Apply the Latest Patch to Essbase Services

Check the table to see whether you need to apply this patch or create a new Essbase service, and migrate your existing data using scripts.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>17.3.3 and earlier</td>
<td>No</td>
<td>-</td>
<td>Create a new service and migrate content from your existing service. See Patch Essbase Services from 17.3.3 and Earlier.</td>
</tr>
<tr>
<td>17.3.5 to 18.3.3 - 69</td>
<td>Yes</td>
<td>105.1.0.x</td>
<td>Apply the latest patch.</td>
</tr>
<tr>
<td>105.1.0.x</td>
<td>No</td>
<td>-</td>
<td>You have the latest version.</td>
</tr>
</tbody>
</table>

Patch Essbase Services from 17.3.3 and Earlier

If your Essbase service is patched to 17.3.3 (or earlier) and you want to upgrade to the latest version, you can't apply the patch through My Services. Instead, you must
create a new (latest) Essbase service, and migrate data from your existing service using scripts.

**Note:**

If you're enabling Oracle Identity Cloud Service (IDCS), then in your existing Essbase service, open the Security tab and ensure that all user data fields (including ID, name, email, and role) contain values and aren't empty. IDCS requires that user fields aren't empty. Enter values in all fields as necessary.

1. Export Essbase applications and users from your service (17.3.3 or earlier) and save them locally.
   a. Connect to the service using Secure Shell (SSH) client software.
   b. Check the required migration script exists at this location:
      
      `/u01/app/oracle/tools/acss/BI/esscs_tools/lcm/esscs_lcm.py`

   **Note:**

   If the scripts aren't available, you must create a new Essbase service and copy the following scripts from the new service to this location:
   
   - `/u01/app/oracle/tools/acss/BI/esscs_tools/lcm/esscs_lcm.py`
   - `/u01/app/oracle/tools/acss/BI/esscs_tools/lcm/idcs_users.py`
   - `/u01/app/oracle/tools/acss/BI/esscs_tools/lcm/ldap_users.py`
   - `/u01/app/oracle/tools/acss/BI/esscs_tools/lcm/user_group.py`
   - `/u01/app/oracle/tools/acss/BI/esscs_tools/public/essbase_export.sh`
   - `/u01/app/oracle/tools/acss/BI/esscs_tools/public/essbase_import.sh`

   Stop your existing service before you create a new one. Copy the scripts, stop the new service, and then restart the existing service to perform the export.

   c. Export your content to a file:
      
      i. Change to the oracle user.
      ii. Go to the export scripts location: `cd /bi/app/public/bin`
      iii. Run the export script:

      ```
      essbase_export.sh filename
      ```
2. Stop your existing Essbase service.

Oracle recommends stopping the existing Essbase service so you don't incur multiple CPU costs when you create a new service in the next step. A stopped service still requires disk space so you need a quota for additional disk space for the new service.

⚠️ Caution:

Oracle doesn't recommend that you delete your Essbase service until you've migrated your data to the new service. When you delete a service, all your data is deleted and it isn't recoverable. If you decide to delete the service because you don't have quota for additional disk space or for some other reason, you risk losing all your data.

3. Create a new Essbase service.

4. Import content from the exported file:
   a. Connect to the new service using SSH client software.
   b. Copy the exported `tar` file to the new service.
   c. Change the user to `oracle`.
   d. Go to the import script location: `cd /bi/app/public/bin`
   e. Run the import script:

```
   essbase_import.sh filename
```

Where:

`filename` Full path to the previously copied `tar` archive file that contains all your Essbase applications, CSV files of users and groups, and files of settings.

Roll Back a Patch to an Earlier Version

If you experience issues after applying a patch, you can roll back to the previous version.

For rollback to work certain aspects of your environment must be the same before and after the rollback.

- The database password before and after the rollback must be exactly the same. If you changed the database password between the patches, you must change it back before rolling back.
- The topology of your service before and after the rollback must be exactly the same. Rollback fails if you scaled your environment in or out between the patches.

1. In the My Services dashboard, navigate to Analytics Classic.
2. Click the name of the service you want to roll back.
3. On the Services tab, select Administration.
   On the Patching tab, expand the Patch and Rollback History accordion.

4. To roll back a patch, click the Manage this service icon for the patch, click Rollback and then confirm that you want to start the rollback.
   A message notifies you when the rollback has completed.

Scale Services

If a service you deployed with Oracle Analytics Cloud - Classic is performing poorly or
is running out of storage, you can scale the compute shape of the node or the storage
attached to the node. You can also add one or more nodes to a cluster; that is, scale
out your service in response to changes in the load.

Topics:
- Scale Compute Shape
- Scale Storage
- Scale a Cluster

Scale Compute Shape

If a cloud service is performing poorly or is running out of storage, you can scale the
compute shape allocated to the service. To save costs, or if your workload is reduced,
you might scale down. For example, changing the compute shape from OC5 to OC4
reduces by 50%, the capacity of the node and the amount of RAM allocated.

All-purpose compute shapes include:
- OC4: 2 OCPUs with 15 GB RAM
- OC5: 4 OCPUs with 30 GB RAM
- OC6: 8 OCPUs with 60 GB RAM
- OC7: 16 OCPUs with 120 GB RAM
- OC8: 24 OCPUs with 180 GB RAM
- OC9: 32 OCPUs with 240 GB RAM

If you want to scale up to one of the higher-memory options, the memory-intensive
compute shapes include:
- OC1M: 1 OCPU with 15 GB RAM
- OC2M: 2 OCPUs with 30 GB RAM
- OC3M: 4 OCPUs with 60 GB RAM
- OC4M: 8 OCPUs with 120 GB RAM
- OC5M: 16 OCPUs with 240 GB RAM

For more information about these compute shapes and considerations for selecting
shapes, see About Machine Images and Shapes in Using Oracle Cloud Infrastructure
Compute Classic.
Expect a temporary unavailability of your service, as it scales up or down. You can check scaling progress by clicking next to your service name and then select View Activity.

1. In the My Services dashboard, navigate to Analytics Classic.
2. Click the name of the service you want to scale.
3. Expand the Resources section, and click Manage this node for the node you want to scale.
4. Click Scale Up/Down.
5. Select a new compute shape to adjust the allocated resources.
6. Click Yes, Scale Up/Down VM.
7. Restart your service if you see this message in the activity log.

Scale Storage

If a cloud service is performing poorly or if relevant disks are running out of space, you can scale the allocated storage. Oracle recommends at least 230 GB, that is, 130 GB latency storage, and 100 GB data storage.

Expect a temporary unavailability of your service as your service scales up or down. You can check scaling progress by clicking next to your service name and then selecting View Activity.

1. In the My Services dashboard, navigate to Analytics Classic.
2. Click the name of the service you want to scale.
3. Expand the Resources section, and click Manage this node for the node you want to scale.
4. Click Add Storage.
5. Select the quantity of storage space to add to the Data and Latency disks, and click Yes, Add Storage. You can see the storage space reflected as part of the total storage value shown in your displayed resources.

Note:

Data disks store configuration and log settings. Latency disks store Essbase applications data.

Scale a Cluster

When you scale out your service, Oracle Analytics Cloud - Classic adds one or more nodes (analytics servers) to the existing cluster. Each service can have as many as 10 nodes. All new nodes have the same compute shape and amount of storage that you allocated when the service was created. For example, if your service started with an
OC3 shape (1 CPU and 7.5 GB RAM) and you decide to scale out, the additional nodes have the same OC3 shape.

**Note:**

To scale a cluster, you must subscribe to Oracle Analytics Cloud - Classic through Oracle Universal Credits and be patched to 17.4.5 or later.

If necessary, you can change the compute shape and add more storage.

Expect your service to be temporarily unavailable while your service scales out or in. You can check scaling progress by clicking next to your service name and then selecting **View Activity**.

1. In the My Services dashboard, navigate to Analytics Classic.
2. Click the name of the service you want to scale.
3. To scale out a service:
   a. Click next to your service name, and select **Scale Out**.
   b. Select the number of nodes (analytics servers) you want to add, and click **Scale Out**.
      If you previously requested and reserved IP addresses, select an IP reservation from the **Select IP Reservation** list.

   New nodes are listed in the Resources pane. You can stop additional nodes if you don't need the extra OCPU right away.

4. To scale in a service:
   a. Click next to the node you want to remove, and select **Remove Node**.
   b. Confirm how you want to scale in:
      • To scale in gracefully, click **Remove Node**.
      • To forcibly scale in, select **Force Remove** and click **Remove Node**.

      If you forcibly scale in, the service removes the node even if the node is unresponsive.
Manage Service Access and Security

By default, Oracle Analytics Cloud - Classic services are accessible only through HTTP, secure protocols like SSL and SSH, and only using specific ports. You can customize the default security configuration to support different access rules and security policies.

Topics:

• Manage SSH Access
• Control Access to Service Components
• Manage Access Rules
• Grant Application Roles with Oracle Identity Cloud Service
• Replace the Self-Signed Certificate for Secure HTTP Access
• Redirect HTTP Traffic to HTTPS
• Connect with EssNet over HTTP
• Manage Credentials
• Deploy Oracle Analytics Cloud - Classic on an IP Network

Manage SSH Access

To make things easy, you view and manage SSH keys for all the services in your Oracle Analytics Cloud - Classic identity domain from the same page.

If you lose the SSH private key used to access a service lost or it gets corrupted, you can add a new public key for that service. Or maybe you need to add a new public key to comply with your organization's new security policies or regulations.

1. In the My Services dashboard, navigate to Analytics Classic.
2. To view or add SSH keys for a particular service, click Manage this service, and then select SSH Access to add or edit SSH keys assigned to that service.
3. To view or add SSH keys for any service in the identity domain, select the SSH Access tab.

A list of services and their current details are displayed.

• Use the Search fields to find services by their name and type.
• View or edit the SSH public keys assigned to the VMs in your service.
• Add a new key for a service by clicking Add New Key.

Control Access to Service Components

You use access rules to control network access to Oracle Analytics Cloud - Classic.
1. In the My Services dashboard, navigate to Analytics Classic.

2. Select **Manage the service** for the service you want to add access rules for.

3. Select **Access Rules**.

4. Click **Create Rule** to set up a new access rule for your service.

5. Enter a unique name for the access rule. The name must begin with a letter, and can contain numbers, hyphens, or underscores. The length can't exceed 50 characters or include the prefix `ora_` or `sys_`.

6. (Optional) Specify a description for the rule.

7. Select or enter a source — the host from which traffic should be allowed.
   - **PUBLIC-INTERNET** — Any host on the internet.
   - **BI_ANALYTIC_SERVER** — Server for Oracle Analytics Cloud - Classic.
   - **DBaaS** — The cloud database you specified when you created the service. If your service instance is configured with more than one database you can select which database to use for the source.
   - **custom** — A custom list of addresses from which traffic is allowed. In the field that is displayed when you select this option, enter a comma-separated list of the subnets (in CIDR format, such as `192.123.42.1/24`) or IPv4 addresses for which you want to permit access.

8. Select or enter a destination for the rule, a service component to which traffic should be allowed. The same options as the previous step are available. The source and the destination must be different.

9. Specify one or more ports through which the source will access the destination. You can specify a single port or a range of ports (such as 7001–8001).
   - 80 – HTTP access to Oracle Analytics Cloud - Classic (closed by default for services using Oracle Identity Cloud Service)
   - 443 – HTTPS access to Oracle Analytics Cloud - Classic (closed by default for services using Oracle Identity Cloud Service)
   - 1521 - Database
   - 10000 – Spark
   - 22 – SSH
   - 5902 – VNC

10. Select the transport protocol (**TCP** or **UDP**) with which the source will access the destination.

11. Click **Create**.

12. To manage access rules on the Access Rules page, click the Menu icon and choose an option.
   - **Enable** — You can enable rules with the rule type USER or DEFAULT. You can't enable a rule if the rule type is SYSTEM.
   - **Disable** — You can disable rules with the rule type USER or DEFAULT. You can't disable a rule if the rule type is SYSTEM.
• **Delete** — You can delete rules with the rule type USER. Rules of type USER can be deleted. You can't delete a rule if the rule type is SYSTEM or USER.

**Manage Access Rules**

There are different types of access rules: user, default, and system. As administrator, you can enable and disable user and default access rules as required. You're allowed to delete only user access rules.

1. In the My Services dashboard, navigate to Oracle Analytics Cloud - Classic
2. Select **Access Rules**.
3. Click the **Actions** icon and select an option.
   - **Enable** — You can enable rules of type USER or DEFAULT. You can't enable rules of type SYSTEM.
   - **Disable** — You can disable rules of type USER or DEFAULT. You can't disable rules of type SYSTEM.
   - **Delete** — You can delete rules of type USER. You can't delete rules of type DEFAULT or SYSTEM.

**Assign Users to Application Roles with Oracle Identity Cloud Service**

As administrator, you can assign users certain permissions in Oracle Analytics Cloud through Oracle Identity Cloud Service.

**Topics**

- About Application Role Assignment with Oracle Identity Cloud Service
- Grant Application Roles with Oracle Identity Cloud Service

**About Application Role Assignment with Oracle Identity Cloud Service**

When you set up an Oracle Analytics Cloud instance, an application dedicated to that instance is automatically created in Oracle Identity Cloud Service.

If you want to, you can assign user permissions through this application.

**Note:**

You don't have to use Oracle Identity Cloud Service. You might prefer to assign user permissions to application roles through the Console. See Configure What Users Can See and Do Using the Console.

The Oracle Identity Cloud Service application for your Oracle Analytics Cloud instance includes several predefined application roles (ServiceAdministrator, ServiceUser, ServiceViewer) that map to a set of predefined application roles in Oracle Analytics Cloud.
To understand more about the predefined Oracle Analytics Cloud application roles, see About Application Roles.

Grant Application Roles with Oracle Identity Cloud Service

As an administrator, you can grant application roles to users with Oracle Identity Cloud Service.

1. In My Services, open the dashboard.
2. Navigate to the Analytics tile, click Action Menu, and then select Open Service Console.
3. On the Instances page, click the name of the instance you want to manage.
4. On the Instance overview page, click Show more, and then click the name of the IDCS Application that is associated with this Oracle Analytics Cloud instance.
5. On the Oracle Identity Cloud Service application page, click **Application Roles**.

6. Select an application role, and click the **Menu** for the specific role.

7. From the menu list, select **Assign Users**.

8. On the Assign Users page, select the users, and click **OK**.

---

**Replace the Self-Signed Certificate for Secure HTTP Access**

This topic does not apply to Oracle Analytics Cloud services using Oracle Identity Cloud Service with Oracle Cloud Infrastructure Load Balancing Classic.

Secure Socket Layer (SSL) is the most commonly used method of securing data sent across the internet and assures visitors that transactions with your application are secure.

When you create a service with Oracle Analytics Cloud - Classic and you choose to use WebLogic embedded LDAP server for identity management (instead of Oracle Identity Cloud Service with a Load Balancer), a self-signed certificate is generated. This certificate is intended to be temporary, so you must replace it with a certificate and key signed by Certificate Authority (CA) that HTTP access from browsers are configured to trust; for example, a commercial CA built into the browser by the browser vendor. The temporary certificate expires one year after service creation.

For production environments, use a CA-issued SSL certificate. For development environments, you can use either a CA-issued or self-signed certificate.

1. Access the SSH client, using a tool such as PUTTY.
2. Enter the host using your private key.

3. For BI and Essbase services, use the script `proxy_register_ssl_private_key`. See Register SSL Private Keys with the HTTP Proxy for a Nonmetered Service (BI Service Script).

Redirect HTTP Traffic to HTTPS

By default, both HTTP and HTTPS access to the Oracle Analytics Cloud URL is enabled. For BI services, you can redirect HTTP traffic to HTTPS using the script `proxy_redirect_http_to_https`.

See Redirect HTTP Calls to HTTPS (BI Service Script) and Run Administration Scripts.

Connect with EssNet over HTTP

You can connect with EssNet from any software using Essbase Runtime Client (RTC) over HTTP protocol without opening ports or performing extensive configuration.

To connect with Agent using Discovery URL, point the server address to the specific endpoint as follows: `https://host/essbase/agent`. This RTC endpoint is a "discovery URL", which automatically selects the connection type and routes clients, whether connecting from inside or outside of the firewall.

When you use RTC, use cURL to connect with HTTP endpoints.

When you use SSL encrypted communication, you must enable the Essbase libcurl library to set up a secure channel. Specify the location of the certificate authority (CA) certificate, or use the default provider. Choose one of the following options.

- `API_CAINFO=CA certificate file path`
- `API_CAPATH=directory path containing CA certificates`

You can download a CA certificate file. One sample source is: `https://curl.haxx.se/docs/caextract.html`.

If you’re using a self-signed certificate, you must add it to the CA certificate file.

Manage Credentials

From time to time you might need to update credentials for services and databases used by Oracle Analytics Cloud - Classic.

You can update passwords for the associated database, cloud storage, and the WebLogic administrator.

Update the Database Password for an Essbase Service

You set the database administrator credentials when you set up your Essbase service.

You can update the password using a script. See Update Database Credentials (Essbase Service Script).
Update the Database Password for a BI Service

You select a cloud database and set the database administrator credentials when you set up Enterprise Business Intelligence and Data Visualization services. If the database administrator password for this Oracle Database Cloud Service changes or expires, you can use the `reset_schema_password` script to update the password that your BI service uses to access its schemas.

See Update Database Credentials (BI Service Script).

Update WebLogic Administrator Passwords for a BI Service

If you have a traditional metered or nonmetered subscription to Oracle Analytics Cloud - Classic, you use WebLogic Embedded LDAP Server for identity management.

You set the WebLogic administrator credentials when you set up your BI service. You can update the password using a script. See Change the WebLogic Administrator Password (BI Service Script)

Update Cloud Storage Passwords

Oracle Analytics Cloud - Classic uses containers in Oracle Cloud Infrastructure Object Storage Classic to store analytics data sets and backups.

Sometimes, you might need to update the credentials Oracle Analytics Cloud - Classic uses to access Oracle Cloud Infrastructure Object Storage Classic. For example, when you try to back up or restore your Oracle Analytics Cloud - Classic service and you receive an access denied error message because the storage credentials are out of sync.

To update the password required to access the storage container:

1. In My Services, navigate to Analytics Classic.
2. Click the name of the service that you need to update.
3. Click Manage this Instance menu icon, and select Instance Credentials.
4. Enter the name of the user with read/write access to Oracle Cloud Infrastructure Object Storage Classic that you specified when you created this service.
5. Enter the updated password for this user.
6. Click Update.
7. Restart your service.

Deploy Oracle Analytics Cloud - Classic on an IP Network

You can deploy Oracle Analytics Cloud - Classic and its associated Oracle Database Cloud Service on an IP network. If you use Oracle Identity Cloud Service with Oracle Analytics Cloud - Classic, you perform all the tasks in this topic. If you use the
embedded LDAP server with Oracle Analytics Cloud - Classic, you don’t need to create the load balancer (you can skip steps 2 and 3).

**Note:**

This topic describes how to deploy Oracle Analytics Cloud - Classic on a basic IP network to help you get started. If your organization has more complex network configuration requirements, work with your networking team to perform all the required configuration. For example, if you have multiple IP networks you must set up an IP network exchange. See Workflows for Using IP Networks in *Using Oracle Cloud Infrastructure Compute Classic*.

To deploy Oracle Analytics Cloud - Classic on an IP network:

1. In My Services, use the Compute Classic console to create an IP network. Note down the name of the IP network. See Create an IP Network in *Using Oracle Cloud Infrastructure Compute Classic*.

2. In the Compute Classic console, create a load balancer for the IP network.
   - **IP Network** — Select the IP network you created in step 1.
   - **Scheme** — Select *Internet Facing* if you want the load balancer to accept traffic from the internet (that is, a public load balancer). Or select *Internal*, if you want the load balancer to accept requests only from the specified IP network.

   Make a note of both settings. When you set up Oracle Analytics Cloud - Classic, you must provide the name of the IP network and specify whether its associated load balancer is public or private. See Create a Load Balancer in *Using Oracle Cloud Infrastructure Compute Classic*.

3. (Oracle Identity Cloud Service only) In My Services, verify that the load balancer you created is available. Check that the Status is *Enabled* and State is *Healthy*. See Verify a Load Balancer Configuration in *Using Oracle Cloud Infrastructure Load Balancing Classic*.

4. In the Oracle Database Cloud Service console, create a custom database deployment on the IP network you created in step 1.

   Oracle Analytics Cloud - Classic uses Oracle Database Cloud Service to store Oracle Analytics Cloud - Classic schemas and data. You must deploy Oracle Analytics Cloud - Classic in the same region and availability domain as the database service.
Note:

Oracle Database Cloud Service doesn’t have to be deployed on the same IP network as Oracle Analytics Cloud - Classic. If you decide to deploy Oracle Database Cloud Service and Oracle Analytics Cloud - Classic on different IP networks, you must create an IP network exchange that enables communication between the two IP networks.

See Create a Customized Database Deployment in Administering Oracle Database Cloud Service.

5. In the Oracle Analytics Cloud - Classic console, create an Oracle Analytics Cloud - Classic instance on the same IP network.
   - **Region** and **Availability Domain** — Select the same region and availability domain where you deployed the database earlier.
   - **IP Network** — Select the name of the IP network you created earlier.
     - **Assign Public IP** — Select this option if you want any node created for this service to have a public IP address.
     - **Public Load Balancer** — Select this option if the load balancer you created for the IP network is **Internet Facing**.
   - **Database Service Name** — Select the database that you created in this IP network.

See Create a Service.

6. In the Oracle Analytics Cloud - Classic console, click the Manage this instance icon, and then click Oracle Analytics Cloud URL to verify that the service is running.
Frequently Asked Questions

This reference provides answers to common questions asked by administrators creating and managing services for Oracle Analytics Cloud - Classic.

Topics:

• What do I use the Service Console in My Services for? Is this the same as the Console I see in the service?
• What is an OCPU?
• How can I determine the right compute size for my initial deployment?
• How do I access my service once it is created?
• Do I need to patch the service on a specific schedule?
• Can I manually update software packages running in my service instance?
• I want to connect to the database where my organization’s analytics data is stored? Do I do this from the Service Console in My Services?
• What network options can I use to manage access into and out from my service?
• How do I configure VPN connectivity for my service to my network?
• Is IPv6 supported?
• How do I get support for Oracle Analytics Cloud?
• Is there a charge for Oracle Support in addition to my subscription fee?
• Do I have direct access to the file system associated with my service?
• My service currently uses the embedded LDAP server for identity management. What's the maximum number of users?
• What do I need to back up?
• What can I use the various backups for?
• How often should I back up?
• How do I find the version of a service instance backup?
• Do I need to back up and restore the actual data associated with my data sets separately?
• Where are backups stored?
• Can I use my database backup to restore user content instead of my Oracle Analytics Cloud - Classic snapshot?
• Is there a specific order that I must follow while restoring?
Top FAQs for Administration and Configuration

The top FAQs for Oracle Analytics Cloud - Classic administration and configuration are identified in this topic.

What do I use the Service Console in My Services for? Is this the same as the Console I see in the service?

- **Service Console** — You use the Service Console in My Services to manage lifecycle tasks such as create, delete, patch, and scale services.

  To access the Service Console, sign in to My Services, open the Dashboard, and navigate to Oracle Analytics Cloud - Classic. If you can't see Oracle Analytics Cloud - Classic, click **Customize Dashboard**, find Oracle Analytics Cloud - Classic and select **Show**.

- **Console** — When you sign in to a particular service, you see a different administrative console where you manage the environment for that service only.

  To access the Console for a service, sign in to the service, open the **Navigator**, and then click **Console**.

What is an OCPU?

An OCPU provides CPU capacity equivalent of one physical core of an Intel Xeon processor with hyper-threading enabled. Each OCPU corresponds to two hardware execution threads, known as vCPU.

How can I determine the right compute size for my initial deployment?

A good starting point is to pick a size that closely matches your on-premises hardware for business intelligence.

For more sizing guidelines, see [http://support.oracle.com](http://support.oracle.com).

How do I access my service once it is created?

It's accessible from My Services. Open the Service Console for Oracle Analytics Cloud - Classic and click the name of the service you want to access. Click the **Manage this service** menu, and then click **Oracle Analytics Cloud URL**.

How do I patch or upgrade my service?

You can patch or upgrade your service from My Services.

Do I need to patch the service on a specific schedule?

No. Patches are delivered through the My Services and you can patch within your organization's preferred schedule.

Can I manually update software packages running in my service instance?

Oracle Analytics Cloud is based on an Oracle Linux image. If required, you may update the packages that are already installed using the `yum update` command. If you want to make any other custom changes to the image, log a service request with Oracle Support to check supportability.
You don't have to log a service request to run any of the approved scripts available under /bi/app/public/bin.

I want to connect to the database where my organization’s analytics data is stored? Do I do this from the Service Console in My Services?

No. You connect to the data you want to analyze within a given service that you created. See How do I access my service once it is created?

What network options can I use to manage access into and out from my service?

By default, you access Oracle Analytics Cloud - Classic through public IPs. If you want to use private IPs, you can configure an IP network and VPN as a Service (VPNaaS). See Deploy Oracle Analytics Cloud on an IP Network and Using Oracle Cloud Infrastructure Compute Classic.

How do I configure VPN connectivity for my service to my network?

VPN is a separate feature from your service and is available to use with some Oracle Cloud services. Contact your Oracle representative for more information.

Is IPv6 supported?

No, not currently.

How do I get support for Oracle Analytics Cloud?

You create a service request in the same way as for on-premises software.

Is there a charge for Oracle Support in addition to my subscription fee?

No. Support is included in your subscription fee.

Do I have direct access to the file system associated with my service?

Yes. You can use the SSH keys, generated at the time of provisioning, to access your service’s file system. However, modifications that you make to the file system might not be saved after you perform routine lifecycle operations, such as patching, and might even prevent you from performing lifecycle operations.

My service currently uses the embedded LDAP server for identity management. What’s the maximum number of users?

The performance of the embedded LDAP server is best with fewer than 10,000 users. If you have more users, use Oracle Identity Cloud Service. See Migrate LDAP-Based Services to Oracle Identity Cloud Service.

Are initialization blocks supported in Oracle Analytics Cloud?

You can use initialization blocks (init blocks) to set session variables but you can’t use them to set users, roles, or groups. If you subscribe to Oracle Analytics Cloud through Universal Credits, USER and ROLE (GROUP) session variables are set in Oracle Identity Cloud Service.

What do I need to back up?

To ensure you can restore Oracle Analytics Cloud - Classic if something goes wrong, you must back up your service and the database associated with your service. If you
deployed Oracle Analytics Cloud - Classic with the data visualization or business intelligence service, then you can also back up the content that users create.

- **Oracle Analytics Cloud - Classic**: You can back up your service from My Services or using the Command Line Interface. See Back Up a Service and psm analytics backup.
  
  To restore your service, see Restore a Service or psm analytics restore.

- **Oracle Analytics Cloud - Classic user content**: (data visualization and business intelligence services only) You can back up the content that users create to a separate file, called a snapshot. User content includes data models and catalog items such as reports, dashboards, data visualization projects, data sets, data flows, security roles, service settings, and more. If something goes wrong with your content or service, then you can revert to the content you saved in a snapshot. Snapshots are also useful if you want to move or share content from one service to another.
  
  To back up user content, see Take a Snapshot.
  
  To restore user content, see Restore from a Snapshot.

**Note:**

For Essbase services, you back up the entire service; you can’t back up only the content.

- **Oracle Database Cloud Service**: Oracle Analytics Cloud - Classic stores various schemas and information in a cloud database that you select when you set up. You can back up this database from My Services.
  
  To back up the database instance, see Create an On-Demand Backup.
  
  To schedule a database instance backup, see Disable and Re-enable Scheduled Backups.
  
  To restore from a database backup, see Recover to Most Recent Backup and Recover to Specific Backup.

**What can I use the various backups for?**

- **Oracle Analytics Cloud - Classic service backup**: Use to recover your service if the virtual machine crashes or your service is corrupted.

- **Oracle Analytics Cloud - Classic user content snapshot**: Use to revert to a prior snapshot that you may have taken as a checkpoint. You can also use snapshots to migrate user content from one Oracle Analytics Cloud - Classic service to another.

- **Oracle Database Cloud Service backup**: Use to recover from a database failure or crash. If the database is entirely dedicated to a single Oracle Analytics Cloud - Classic service, then you can use this backup to recover the content users create in that service.

**How often should I back up?**

- **Oracle Analytics Cloud - Classic service backup**: Schedule weekly full backups and daily incremental backups. In addition, take a full, on-demand backup before
you patch your service or before you make any significant changes to your
service, for example, if you scale up, scale down, and add storage.

- Oracle Analytics Cloud - Classic user content snapshot: Take snapshots before
  making major changes to your content. You can take regular weekly snapshots or
  at your defined frequency based on the rate of change of the business intelligence
  environment and rollback requirements.

- Oracle Database Cloud Service backup: Schedule weekly full backups and daily
  incremental backups. In addition, take a full backup before you patch.

How do I find the version of a service instance backup?

In My Services, backups are listed by the timestamp when the backup was created. If
you compare the timestamp of a particular backup with your service’s patch history,
you can determine the version of the service in that backup.

For example, you create a service on 4/14/2018 with Oracle Analytics Cloud - Classic
version 18.2.1 and take backups on 4/16/2018 and 4/18/2018. On 5/14/2018, you
apply patch version 18.2.3 and take a backup on 5/16/2018. In this case, backups
taken on 4/16/2018 and 4/18/2018 are from service version 18.2.1, whereas the
backup taken on 5/16/2018 is from service version 18.2.3.

Do I need to back up and restore the actual data associated with my data sets
separately?

If you import a snapshot to a different environment, then you must upload or import the
data from data sets again after restoring from a backup.

Where are backups stored?

Backups for Oracle Analytics Cloud - Classic and Oracle Database Cloud Service are
stored on Oracle Cloud Infrastructure Object Storage, in two, separate storage
containers.

- Oracle Analytics Cloud - Classic service backups: When you create a service with
  Oracle Analytics Cloud, you select the container you want to use for backups.

- Oracle Analytics Cloud - Classic user content snapshots: Snapshots are stored in
  the same container as your Oracle Analytics Cloud - Classic service backups.

- Oracle Database Cloud Service backups: When you create a database with
  Oracle Database Cloud Service, you select the container you want to use for
  backups. You can't store database backups in the same container as you store the
  Oracle Analytics Cloud - Classic service backups.

Can I use my database backup to restore user content instead of my Oracle
Analytics Cloud - Classic snapshot?

Yes, but only if the database is dedicated to a single Oracle Analytics Cloud - Classic
service. If you share the database across multiple services or use the database to
store other data, you must use snapshots to recover user content for individual
services.

Before you restore from a database backup, verify that the version of Oracle Analytics
Cloud - Classic you're currently using and the version in the backup are the same.
Is there a specific order that I must follow while restoring?

In the unlikely event you need to restore everything, restore the database first, and then restore Oracle Analytics Cloud - Classic. If you have user content that you must restore from a snapshot, then restore that content last.
Troubleshoot

This topic describes common problems that you might encounter administering services in Oracle Analytics Cloud - Classic and explains how to solve them.

Topics:

• I'm having problems creating a service
• How do I diagnose other issues?
• When do I contact Oracle Support?

I'm having problems creating a service

In My Services, navigate to the Oracle Analytics Cloud - Classic dashboard, open the Service Create and Delete History pane. Click Details to see why provisioning failed. Maybe you have insufficient resources or perhaps you entered an invalid service name? In most cases, you can diagnose the problem from the information provided here.

When you create a service, a diagnostics ZIP file is uploaded to your cloud storage location. If your issue requires further diagnosis, you can examine the log files in this ZIP file.

1. Go to your cloud storage and locate the service_provisioning logs folder. Either:
   • Open the Storage Cloud Service Console and navigate to the container you specified when you created the service.
   • Navigate to a URL similar to: https://storage.oraclecloud.com/v1/<storage domain>

   Provisioning ZIP files are named like this: <service>-bi-1-logs-<timestamp>.zip

   For example:
   • service_provisioning/mybiservice-bi-1-logs-20161018-080743.zip
   • service_provisioning/testbiservice-bi-1-logs-20161026-223639.zip
   • service_provisioning/myessbaseservice-bi-1-logs-20161027-135349.zip

2. Expand the ZIP file and look for issues recorded in the logs.

   For a BI service, look at setupBICS.log.

   For an Essbase service, look at continue-service-start-essbase.log.

3. If you’re still having issues, contact Oracle Support and send them the ZIP file.

How do I diagnose other issues?

Oracle Analytics Cloud - Classic saves logs to several locations:

• /bi/data/logs - Includes provisioning logs for BI services
- /bi/logs - Includes lifecycle operation logs for BI services
- /u01/data/logs/workspace/log - Includes provisioning logs for Essbase services
- /u01/data/logs/var/log - Includes lifecycle operation logs for Essbase services
- /u01/data/logs/ESSBASE - Includes service lifecycle operation logs for Essbase services
- /u01/data/logs - Includes runtime logs for Essbase services

You can use your favorite SSH client to log in to the compute node associated with your service to access these logs.

You can also download and view Essbase logs at the server level and applications level, from the Essbase service. See Download Server and Application Logs in Using Oracle Analytics Cloud - Essbase.

**When do I contact Oracle Support?**

If you encounter a problem with creating or managing Oracle Analytics Cloud - Classic services, contact Oracle Support for assistance, after recording any error messages in the user interface. If necessary, Oracle Support can guide you through collecting any additional diagnostics.
Oracle Analytics Cloud - Classic provides scripts to perform some common administration tasks. Always use the scripts provided. Don't perform any administration tasks manually.

Topics:

- Administration Scripts for Data Visualization and Business Intelligence Services (BI Services)
- Administration Scripts for Essbase Services

To run the scripts, see Run Administration Scripts.

Understanding Customization and Administration

My Services is your primary tool for administering Oracle Analytics Cloud - Classic deployments. In addition, there are some scripts to perform some important administration tasks. There are two types of customization for Oracle Analytics Cloud - Classic deployments:

- **Supported customizations:** Any configuration or functionality change that you make exclusively using Oracle Analytics Cloud scripts available from:
  
  `/bi/app/public/bin`

  The changes you make with these scripts are tested and supported.

  In addition, you may run `yum update` to update existing packages running in your deployment.

- **Unsupported customizations:** Any configuration or functionality change that you make using any other script, installer, or API, using WebLogic Console or Enterprise Manager, or by directly editing files. Such customizations are equivalent to on-premises customizations.
  
  - Custom changes aren't covered by Oracle Support.
  
  - Unsupported customizations can prevent patching and other service lifecycle operations.

Administration Scripts for Data Visualization and Business Intelligence Services (BI Services)

<table>
<thead>
<tr>
<th>Administrative Task</th>
<th>Script Name</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change the WebLogic administrator password for my BI service</td>
<td><code>update_wls_admin_password</code></td>
<td>Change the WebLogic Administrator Password (BI Service Script)</td>
</tr>
<tr>
<td>Import a batch of users or roles from a CSV file</td>
<td><code>import_users_groups_csv</code></td>
<td>Import Users and Roles from a CSV File (BI Service Script)</td>
</tr>
</tbody>
</table>
## Administration Scripts for Essbase Services

<table>
<thead>
<tr>
<th>Administrative Task</th>
<th>Script Name</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export Essbase applications and users from v17.3.x to latest update.</td>
<td>export.sh filename</td>
<td>Migrate Essbase Applications and Users</td>
</tr>
<tr>
<td>Import Essbase applications and users from v17.3.x to latest update.</td>
<td>import.sh filename</td>
<td>Migrate Essbase Applications and Users</td>
</tr>
<tr>
<td>Gather diagnostic logs related to my Essbase service into a ZIP file before contacting Oracle Support</td>
<td>python collect_diagnostic_logs.py</td>
<td>Gather Diagnostic Logs into a ZIP File (Essbase Service Script)</td>
</tr>
<tr>
<td>Enable a nonmetered service to store user group membership information in a database</td>
<td>configure_bi_sql_group_provider</td>
<td>Enable Database Storage for User Group Memberships for a Nonmetered Service (BI Service Script)</td>
</tr>
<tr>
<td>Update the password your Essbase service uses to access its database schemas.</td>
<td>changeRCUPassword.py</td>
<td>Update Database Credentials (Essbase Service Script)</td>
</tr>
</tbody>
</table>
Run Administration Scripts

You must be an Oracle Analytics Cloud - Classic administrator to run the administration scripts. To access a compute node associated with Oracle Analytics Cloud - Classic, you use Secure Shell (SSH) client software to establish a secure connection and log in as the user oracle. Several SSH clients are freely available. This topic describes how to run scripts using the ssh utility, included with UNIX and UNIX-like platforms.

Before you start, you’ll need some connection information:

• The IP address of the compute node
  The IP address of a compute node associated with your Oracle Analytics Cloud - Classic service is displayed in My Services (Overview page for the service). See View and Manage Services.

• The SSH private key file that matches the public key associated with the service.

To connect to a compute node using the ssh utility:

1. Run the utility.

   $ ssh -i private-key-file-location opc@node-ip-address

Where:

• `private-key-file-location` is the path to the SSH private key file that you registered when you created the service.

• `opc` is the operating system user you must connect as. An `opc` user can perform operations that require root access to the compute node, such as running administration scripts. This user can use the `sudo` command to gain root access to the compute node.

• `node-ip-address` is the IP address of the compute node in x.x.x.x format.

2. Change to the oracle user.

   sudo su - oracle

3. Run the Oracle Analytics Cloud - Classic script.

Refer to the documentation for the Secure Shell (SSH) client software for general information.

When using Bash, enclose special characters inside single quotes to preserve the literal value. For example, to specify a new password on the command line, such as `MYNEW$PASSWORD$`, you enter `'MYNEW$PASSWORD$'`. 
Change the WebLogic Administrator Password (BI Service Script)

You set the administrator password for the WebLogic server when you set up your service. If you want to change the password you must always use the script update_wls_admin_password.

---

**Note:**

If you change the administrator password your backups might not contain the latest password. If this is the case and you restore your service, the administrator password reverts to the older password in the backup.

---

**Script Location**

/bi/app/public/bin/update_wls_admin_password

To run the script, see Run Administration Scripts.

**Syntax**

update_wls_admin_password [-h] [LOGLEVEL] [LOGDIR] username 'old_password' 'new_password'

Where:

- **username** Existing WebLogic server administrator username.
- **old_password** Existing WebLogic server administrator password.
- **new_password** New password for the WebLogic server administrator user.

Optional parameters:

- **-h** Shows help for the script and exits.
- **LOGLEVEL** Sets the logging level for standard errors (stderr). The default is INFO. Options:
  - DEBUG
  - INFO
  - WARNING
  - ERROR
  - CRITICAL
  The logging level for messages in the log file is always DEBUG.
- **LOGDIR** Log directory. The default directory is: /var/log/bi
Example

update_wls_admin_password 'weblogic' 'oldpassword' 'newpassword'

Export Users and Roles to CSV Files (BI Service Script)

(Only valid for services using WebLogic embedded LDAP server). To export users and roles, use the script `wls_ldap_csv_exporter`. This script creates two CSV files and a log file. One CSV file contains users and the other contains groups.

Script Location

/bi/app/public/bin/wls_ldap_csv_exporter

To run the script, see Run Administration Scripts.

Syntax

```
wls_ldap_csv_exporter -u weblogic_admin_user
                 -c oracle_common_folder_path
                 -D output_dir
                 [--loglevel LOGLEVEL] [--logdir LOGDIR]
```

Where:

- **u** Sets the administrator user name.
- **c** Sets the `oracle_common` folder path. Typically,

  `/bi/app/fmw/oracle_common`

- **D** Specifies where to export the CSV files.
- **LOGLEVEL** Sets the logging level for standard errors (stderr). The default is `INFO`. Options:
  - DEBUG
  - INFO
  - WARNING
  - ERROR
  - CRITICAL

  The logging level for messages in the log file is always DEBUG.
- **LOGDIR** Log directory. The default directory is: `/var/log/bi`
Examples

wls_ldap_csv_exporter -u weblogic_admin -c /bi/app/fmw/oracle_common -D /myfolder

Import Users and Roles from a CSV File (BI Service Script)

(Only valid for services using WebLogic embedded LDAP server). Rather than add users manually one at a time through the Console, you can add a batch of users from a file. To do this, create a CSV (comma-separated values) file that contains the user data in a fixed format. You can create multiple user roles with member assignments from CSV files too. To import users and roles this way, use the script import_users_groups_csv.

It’s important that the CSV file is formatted correctly. Spaces are not allowed.

<table>
<thead>
<tr>
<th>Import Type</th>
<th>Information Required in the CSV</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td>User ID,Display Name,Password,givenname,lastname,mail</td>
<td>User ID,Display Name,Password,givenname,lastname,mail AGold,Ali Gold,MyPassword1,Alice,Gold,<a href="mailto:alice.gold@example.com">alice.gold@example.com</a> BJones,Brian Jones,MyPassword12,Brian,Jones,<a href="mailto:brian.jones@example.com">brian.jones@example.com</a> JSmith,Johnny Smith,MyPassword1234,John,Smith,<a href="mailto:john.smith@example.com">john.smith@example.com</a> SWasher,Sally Washer,MyPassword12345,Sally,Washer,<a href="mailto:sally.washer@example.com">sally.washer@example.com</a></td>
</tr>
<tr>
<td>Roles</td>
<td>Display Name,Description,User Members One or more User IDs separated by a semicolon.</td>
<td>Display Name,Description,User Members Reviewers,This role includes a group of users who can review reports,Agold;BJones;JSmith Editors,This role defines a group of users who can edit reports,BJones;JSmith</td>
</tr>
</tbody>
</table>

Script Location

/bi/app/public/bin/import_users_groups_csv

To run the script, see Run Administration Scripts.
Syntax

import_users_groups_csv [-h] --admin-user ADMIN_USER
                      --type {users,groups}
                      [--loglevel LOGLEVEL] [--logdir LOGDIR]
filename

Where:

filename Name of the CSV file.

Optional parameters:

- h Shows Help for the script and exits.
- ADMIN_USER Sets the administrator user name.
- users,groups Specifies the type of CSV you want to import.
- LOGLEVEL Sets the logging level for standard errors (stderr). The default is INFO. Options:
  - DEBUG
  - INFO
  - WARNING
  - ERROR
  - CRITICAL
  The logging level for messages in the log file is always DEBUG.
- LOGDIR Log directory. The default directory is: /var/log/bi

Examples

import_users_groups_csv weblogic_admin users allmyusers.csv
import_users_groups_csv weblogic_admin groups allmygroups.csv

Update or Delete Users and Roles from Embedded LDAP
(BI Service Script)

(Only valid for services using WebLogic embedded LDAP server). Rather than updating or deleting users manually one at a time through the Console, you can update or delete a batch of users from a file. To do this, create a CSV (comma-separated values) file that contains the user data in a fixed format. You can update or delete multiple user roles from CSV files too. To modify users and roles this way, use the script update_users_groups.

It’s important that the CSV file is formatted correctly. Spaces aren’t allowed.
<table>
<thead>
<tr>
<th>Type</th>
<th>Information Required in the CSV</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td>User ID,Display Name,Password,givenname,lastname,mail</td>
<td>AGold,Ali Gold,MyPassword1,Alice,Gold,<a href="mailto:alice.gold@example.com">alice.gold@example.com</a> BJones,Brian Jones,MyPassword12,Brian,Jon es,<a href="mailto:brian.jones@example.com">brian.jones@example.com</a> JSmith,Johnnie Smith,MyPassword1234,John,Smith, <a href="mailto:john.smith@example.com">john.smith@example.com</a> SWasher,Sally Washer,MyPassword1235,Sally ,Washer,<a href="mailto:sally.washer@example.com">sally.washer@example.com</a></td>
</tr>
<tr>
<td>Roles</td>
<td>Display Name,Description,User Members</td>
<td>Reviewers,This role includes a group of users who can review reports,Agold;BJones;JSmith Editors,This role defines a group of users who can edit reports,BJones;JSmith</td>
</tr>
</tbody>
</table>

**Script Location**

/bi/app/public/bin/update_users_groups

To run the script, see Run Administration Scripts.

**Syntax**

```
update_users_groups [-h] --admin-user ADMIN_USER
                    --action {update,delete}
                    --type [users,groups] [--loglevel LOGLEVEL] [--logdir LOGDIR]
                    filename
```

Where:

- `filename` Name of the CSV file.

Optional parameters:

- `-h` Shows Help for the script and exits.
- `ADMIN_USER` Sets the administrator user name.
- `update,delete` Specifies whether you want to modify or delete users (or groups) in the CSV file.
• users,groups  Specifies whether the CSV file contains users or groups.

• LOGLEVEL  Sets the logging level for standard errors (stderr). The default is INFO. Options:
  – DEBUG
  – INFO
  – WARNING
  – ERROR
  – CRITICAL

  The logging level for messages in the log file is always DEBUG.

• LOGDIR  Log directory. The default directory is: /var/log/bi

Example

update_users_groups delete removeoldusers.csv

Create a Public Container for Sharing Content (BI Service Script)

You can define a public storage container so that other users can share their content. Use the script configure_public_storage to specify the storage container you want to use.

If you configured a public container when you set up your service, you override the container that you specified when you run this script.

Script Location

/bi/app/public/bin/configure_public_storage

To run the script, see Run Administration Scripts.

Syntax

configure_public_storage user pwd baseurl container [force]

Where:

user - Name of a user with permission to create containers.

pwd - Password for the storage user.

baseurl - Base URL for the storage service. For example: https://storage.oraclecloud.com/v1
  • – https://domain.storage.oraclecloud.com/v1
     For example: https://example.storage.oraclecloud.com/v1
  • – https://Storage-GUID.storage.oraclecloud.com/v1
For example: https://Storage-ab1c23de4456f78g9123456hi7k8j89.storage.oraclecloud.com/v1

container - Name of the storage container you want to create, in the format: storage-identityDomainID/containername

Optional parameters:

force - Override the current public container, if one is designated.

Example


Export and Import Data Sets (BI Service Script)

You can export and import data sets that users have uploaded to Oracle Analytics Cloud - Classic. Use the script migrate_datafiles to export all the data sets in cloud storage to an archive (.zip file) and import them on another service.

Script Location

/bi/app/public/bin/migrate_datafiles

To run the script, see Run Administration Scripts.

Syntax

migrate_datafiles sikey archive action

Where:

sikey - Service key. Always bootstrap.

archive - Full path to the archive you want to create or import. For example /tmp/mydatasets.zip.

action - Either export or import.

Example — Export

$ migrate_datafiles bootstrap /tmp/mydatasets.zip export

Enter encryption password for archive: ENTER_PASSWORD
Confirm encryption password for archive: ENTER_PASSWORD
$ chmod ugo+rw /tmp/dss.zip
Example — Import

If you haven’t done so already, copy the data set archive you want to import the target service, for example mydatasets.zip.

$ migrate_datafiles bootstrap /tmp/mydatasets.zip import
   Enter encryption password for archive: ENTER_PASSWORD
   Confirm encryption password for archive: ENTER_PASSWORD

Update Database Credentials (BI Service Script)

When you create a service with Oracle Analytics Cloud - Classic, various schemas are created and loaded into an associated Oracle Database Cloud Service that you select. If the database administrator password for this Oracle Database Cloud Service changes or expires, you can use the reset_schema_password script to update the password that your BI service uses to access its schemas.

Before you run the command, you must stop BI processes, and then restart them after resetting the password.

1. Connect to the compute node for your service
2. Change to the script folder: /bi/app/public/bin
3. Stop BI processes using the script stop_analytics_suite
4. Update the schema password using the script reset_schema_password
5. Restart BI processes, using the script start_analytics_suite

Script Location

/bi/app/public/bin

To run the script, see Run Administration Scripts.

Syntax

reset_schema_password [-h] [LOGLEVEL] [LOGDIR]

Where:

- `-h` Shows help for the script and exits.
- `LOGLEVEL` Sets the logging level for standard errors (stderr). The default is INFO. Options:
  - `DEBUG`
  - `INFO`
  - `WARNING`
  - `ERROR`
  - `CRITICAL`
  The logging level for messages in the log file is always DEBUG.
- `LOGDIR` Log directory. The default directory is: /var/log/bi
Example

To update the schema password, run all three scripts from /bi/app/public/bin in this order:

> stop_analytics_suite
> reset_schema_password
> start_analytics_suite

Gather Diagnostic Logs into a ZIP File (BI Service Script)

If you're troubleshooting an issue with your service or you need to contact Oracle Support, you can easily collect all available log files into one place. Use the script collect_diagnostic_logs to collect diagnostic data into a ZIP file.

Script Location

/bi/app/public/bin/collect_diagnostic_logs

To run the script, see Run Administration Scripts.

Syntax

collect_diagnostic_logs [-h] [--loglevel LOGLEVEL] [--logdir LOGDIR] filename

Where:

filename Name of the ZIP file you want to generate.

Optional parameters:

- h Shows help for the script and exits.
- LOGLEVEL Sets the logging level for standard errors (stderr). The default is INFO. Options:
  - DEBUG
  - INFO
  - WARNING
  - ERROR
  - CRITICAL
  The logging level for messages in the log file is always DEBUG.
- LOGDIR Log directory. The default directory is: /var/log/bi

Example

collect_diagnostic_logs DiagnosticsForMyService.zip
Get Status Information (BI Service Script)

You can find out the status of your service at any time. Use the script `status` to report whether WebLogic Server and various other BI processes are up and running.

If this script can't respond for some reason, restart the service and try again. See Stop and Start Component Processes (BI Service Script).

Script Location

`/bi/app/public/bin/status`

To run the script, see Run Administration Scripts.

Syntax

```
status [-v]
```

Where:

- v Indicates verbose.

Example

```
>status

/Servers/AdminServer/ListenPort=7001
Accessing admin server using URL t3://xxx:7001

Status of Domain: /bi/domain/fmw/user_projects/domains/bi
NodeManager xxx:9556): RUNNING

Name          Type      Machine        Restart Int Max Restart Status
----------      ------    --------        ------- ------- ------- ------- -------
AdminServer    Server    xxx unknown    unknown unknown RUNNING
bi_server1     Server    m1 unknown    unknown unknown RUNNING
obiccs1        OBICCS    m1 3600 2     RUNNING
obisch1        OBISCH    m1 3600 2     RUNNING
obips1         OBIPS     m1 3600 2     RUNNING
obijh1         OBIJH     m1 3600 2     RUNNING
obis1          OBIS      m1 3600 2     RUNNING
```

Stop and Start Component Processes (BI Service Script)

If you're having issues, you can restart the BI components running on your service rather than the entire service. Restarting BI components is often quicker than restarting the service. When you stop BI processes, anyone who is signed in, is signed out. When you restart, users are prompted to sign in again. Use scripts `stop_analytics_suite` and `start_analytics_suite` to stop and start BI components.

Script Location

`/bi/app/public/bin/stop_analytics_suite`
/bi/app/public/bin/start_analytics_suite

To run the scripts, see Run Administration Scripts.

Syntax — stopPod.py

stop_analytics_suite [-h] [--loglevel LOGLEVEL] [--logdir LOGDIR]

start_analytics_suite [-h] [--loglevel LOGLEVEL] [--logdir LOGDIR]

Optional parameters:

• **h**    Shows help for the script and exits.

• **LOGLEVEL**  Sets the logging level for standard errors (stderr). The default is INFO. Options:
  - DEBUG
  - INFO
  - WARNING
  - ERROR
  - CRITICAL

  The logging level for messages in the log file is always DEBUG.

• **LOGDIR**  Log directory. The default directory is: /var/log/bi

Examples

stop_analytics_suite

start_analytics_suite

Register SSL Private Keys with the HTTP Proxy for a Nonmetered Service (BI Service Script)

If you have a nonmetered subscription for Oracle Analytics Cloud - Classic, you can register your custom SSL certificates to secure HTTPS access to your service. Use the script `proxy_register_ssl_private_key` to register your private key and your Certificate Authority (CA) signed certificate.

When the service is created, a self-signed certificate is generated. The self-signed certificate is intended to be temporary and you must replace it with a new private key and a certificate signed by a CA which your browsers are configured to trust (that is, a commercial CA built into the browser by the browser vendor). The temporary certificate expires after one year.

Before You Run the Script

1. Verify that your private key and SSL certificate files contain the required information.
• Private key and CA signed certificate must use the DNS registered name as the common name (CN).
  – CA signed certificate must also include the CN as the first Subject Alternative Name
• Private key and CA signed certificate files must be in PEM format.
• Private key must not be protected with passphrase.
• Private key permissions must be set to read-only and owned by the oracle user.

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>To test any changes you make to certificates and certificate chains on Windows, you might need to clear your SSL state. From the Control Panel menu, select Internet Options, then Content, then Clear SSL State.</td>
</tr>
</tbody>
</table>

2. If your service uses a DNS registered host name, specify the host name that you want to secure with SSL in servername.conf:

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Each service has a public IP address available on the internet. You can register your own FQDN (Fully Qualified Domain Name) against this public IP address so your service appears in your organization's internet domain. The FQDN must match the CN in the certificate. The FQDN must also be present as Subject Alternative Name in the certificate.</td>
</tr>
</tbody>
</table>

a. Create a file named servername.conf at this location:
   `/bi/data/httpd/conf.d/servername.conf`
b. Set permissions on the file as, owned by the oracle user and readable by everyone.
c. In servername.conf, add a single line:
   ```
   ServerName <DNS name that matches your SSL certificate>
   ```
   For example: ServerName analytics.myexample.com

**Script Location**

`/bi/app/public/bin/proxy_register_ssl_private_key`

To run the script, see Run Administration Scripts.

**Syntax**

```
proxy_register_ssl_private_key [-h] [LOGLEVEL] [LOGDIR] privatekeypath sslcertificatepath
```
Redirect HTTP Calls to HTTPS (BI Service Script)

By default, both HTTP and HTTPS access to the Oracle Analytics Cloud URL is enabled. If you want to redirect all incoming HTTP traffic to HTTPS, you can use the script `proxy_redirect_http_to_https`.

For example, if you currently access the service using http://analytics.mycorp.com/analytics, you are redirected to this URL after running the script https://analytics.mycorp.com/analytics. The browser should confirm the valid certificate.

Script Location

/bi/app/public/bin/proxy_redirect_http_to_https

Syntax

proxy_redirect_http_to_https [-h] [LOGLEVEL] [LOGDIR]

Optional parameters:

• h Shows help for the script and exits.

• LOGLEVEL Sets the logging level for standard errors (stderr). The default is INFO. Options:
  – DEBUG
  – INFO
  – WARNING
  – ERROR
  – CRITICAL

The logging level for messages in the log file is always DEBUG.

Optional parameters:

• LOGDIR Log directory. The default directory is: /var/log/bi
Enable Database Storage for User Group Memberships for a Nonmetered Service (BI Service Script)

If you have a nonmetered subscription for Oracle Analytics Cloud - Classic, you might want to store user group memberships in a database and for your service’s authentication provider to access this information when authenticating a user’s identity. You can use the script `configure_bi_sql_group_provider` to set up the provider and create the tables that you need (GROUPS and GROUPMEMBERS). After you run the script, you must populate the tables with your group and group member (user) information.

Note:
Group memberships that you derive from the SQL provider don’t show up in the Users and Roles page in Oracle Analytics Cloud Console as you might expect but the member assignments work correctly.

These tables are in the Oracle Database Cloud Service you configured for Oracle Analytics Cloud - Classic and in the schema created for your service. Unlike the on-premises equivalent functionality, you can’t change the location of these tables or the SQL that retrieves the results. Instead, you must populate these fixed tables using any supported means for loading database tables.

Script Location

`/bi/app/public/bin/configure_bi_sql_group_provider`

To run the script, see Run Administration Scripts.

Syntax

`configure_bi_sql_group_provider [-h] [LOGLEVEL] [LOGDIR]`
Optional parameters:

- **-h** Shows help for the script and exits.
- **LOGLEVEL** Sets the logging level for standard errors (stderr). The default is INFO. Options:
  - DEBUG
  - INFO
  - WARNING
  - ERROR
  - CRITICAL
  The logging level for messages in the log file is always DEBUG.
- **LOGDIR** Log directory. The default directory is: `/var/log/bi`

Example

`configure_bi_sql_group_provider`

## Migrate Essbase Applications and Users

You can migrate applications and users from Oracle Analytics Cloud – Essbase services from v17.3.3 (or earlier) to the latest version, using scripts.

You can use the scripts in this section to import Essbase applications, users and groups when you install a new Essbase service version.

### Prerequisites

**Note:**

- Oracle Identity Cloud Service (IDCS) requires that user fields aren’t empty. If you’re enabling IDCS, then in your existing Essbase services and prior to migrating your data, open the Security tab and ensure that all user data fields (including ID, name, email, and role) contain values and aren’t empty.
- When you export applications, the target file is overwritten. If you want to save the previous version of an LCM exported application, rename it or run the export script with another file name.

Before you migrate applications and users, copy the following scripts from the older Essbase service version to the latest version, at the same file location. You can check first whether they already exist on the new host:

- `/u01/app/oracle/tools/acss/BI/esscs_tools/lcm/esscs_lcm.py`
- `/u01/app/oracle/tools/acss/BI/esscs_tools/lcm/idcs_users.py`
- `/u01/app/oracle/tools/acss/BI/esscs_tools/lcm/ldap_users.py`
- `/u01/app/oracle/tools/acss/BI/esscs_tools/lcm/user_group.py`
Export Script Location

'/bi/app/public/bin

To run the export script, see Run Administration Scripts.

Export Syntax

essbase_export.sh filename

Where:
filename Full path to the tar archive file that stores all Essbase applications, CSV files of users and groups, and files of settings.

Import Script Location

'/bi/app/public/bin

To run the import script, see Run Administration Scripts.

Import Syntax

essbase_import.sh filename

Where:
filename Name of the tar created by the export script.

Gather Diagnostic Logs into a ZIP File (Essbase Service Script)

If you're troubleshooting an issue with your service or you need to contact Oracle Support, you can easily collect all available log files into one place.

Script Location

'/bi/app/public/bin

To run the script, see Run Administration Scripts.

Syntax

python collect_diagnostic_logs.py [-h] filename

Where:
filename Full path of the ZIP file that you want to generate.

Optional parameter:
Example

python collect_diagnostic_logs.py /tmp/DiagnosticsForEssbaseService

Update Database Credentials (Essbase Service Script)

When you create an Essbase service, various schemas are created and loaded into the Oracle Database Cloud Service that you selected. If the password expires for this Oracle Database Cloud Service, you can use the changeRCUPasswd script to update the password that your Essbase service uses to access the database.

The changeRCUPasswd script changes passwords for:

- Wallet Store stored credentials
- Bootstrap credentials
- WebLogic server data sources
- Oracle database schemas

Script Location

/bi/app/public/bin

To run the script, see Run Administration Scripts.

Syntax

python changeRCUPasswd.py <new_password> <sys db_user> <sys db_password>

Where:

new_password New password for the database.
sys db_user System database user name.
sys db_password System database user password.

Example

python changeRCUPasswd.py xxxxxxxx dsmith ds112233